Université de Montréal

et

Université Panthéon-Assas Paris II

Redefining Personal Information in the Context of the Internet

par

Éloïse Gratton

Faculté de droit

Thèse présentée à la Faculté des études supérieures
en vue de l'obtention du grade de
Docteur en droit de la Faculté de droit de l'Université de Montréal

et

Docteur en droit de l'Université Panthéon-Assas Paris II

Octobre 2012

Université de Montréal

Faculté des études supérieures

Université Panthéon-Assas Paris II

École doctorale Georges Vedel

Droit public interne, science administrative et science politique

Cette thèse intitulée:

Redefining Personal Information in the Context of the Internet

présentée en date du 30 octobre 2012 par:

Éloïse Gratton

a été évaluée par un jury composé des personnes suivantes:

Vincent Gautrais
Professeur titulaire, Université de Montréal
directeur de recherche

Danièle Bourcier
Responsable du groupe “Droit gouvernance et technologies” au CERSA
directrice de recherche

Karim Benyekhlef
Professeur titulaire, Université de Montréal
membre du jury

Gilles Guglielmi
Professeur, Université Panthéon-Assas Paris 2
membre du jury

Ian Kerr
Professeur titulaire, Université d’Ottawa
rapporteur externe

Francis Rousseaux
Professeur, Université de Reims
rapporteur externe

Université de Montréal

et

Université Panthéon-Assas Paris II

Redefining Personal Information in the Context of the Internet

par

Éloïse Gratton

Faculté de droit

Thèse présentée à la Faculté des études supérieures
en vue de l'obtention du grade de
Docteur en droit de la Faculté de droit de l'Université de Montréal

et

Docteur en droit de l'Université Panthéon-Assas Paris II

Octobre 2012

RÉSUMÉ

Résumé: Vers la fin des années soixante, face à l'importance grandissante de l'utilisation des ordinateurs par les organisations, une définition englobante de la notion de donnée personnelle a été incorporée dans les lois en matière de protection de données personnelles (« LPDPs »). Avec Internet et la circulation accrue de nouvelles données (adresse IP, données de géolocalisation, etc.), il y a lieu de s'interroger quant à l'adéquation entre cette définition et cette réalité.

Aussi, si la notion de *donnée personnelle,* définie comme étant « une donnée concernant un individu identifiable » est toujours applicable à un tel contexte révolutionnaire, il n'en demeure pas moins qu'il importe de trouver des principes interprétatifs qui puissent intégrer ces changements factuels. La présente thèse vise à proposer une interprétation tenant compte de l'objectif recherché par les LPDPs, à savoir protéger les individus contre les risques de **dommage** découlant de la **collecte**, de l'**utilisation** ou de la **divulgation** de leurs données.

Alors que la **collecte** et la **divulgation** des données entraîneront surtout un risque de dommage de nature subjective (la collecte, un sentiment d'être sous observation et la divulgation, un sentiment d'embarras et d'humiliation), l'**utilisation** de ces données causera davantage un dommage objectif (dommage de nature financière, physique ou discriminatoire). La thèse propose plusieurs critères qui devraient être pris en compte pour évaluer ce risque de dommage ; elle servira de guide afin de déterminer quelles données doivent être qualifiées de *personnelles*, et fera en sorte que les LPDPs soient le plus efficaces possibles dans un contexte de développements technologiques grandissants.

Mots clés: définition, renseignements personnels, données personnelles, protection, vie privée, Internet, risque de dommage, but des lois en matière de protection de données personnelles, interpretation.

ABSTRACT

Abstract: In the late sixties, with the growing use of computers by organizations, a very broad definition of *personal information* as "information about an identifiable individual" was elaborated and has been incorporated in data protection laws ("DPLs"). In more recent days, with the Internet and the circulation of new types of information (IP addresses, location information, etc), the efficiency of this definition may be challenged.

This thesis aims at proposing a new way of interpreting *personal information*. Instead of using a literal interpretation, an interpretation which takes into account the purpose behind DPLs will be proposed, in order to ensure that DPLs do what they are supposed to do: address or avoid the ***risk of harm*** to individuals triggered by organizations handling their personal information.

While the **collection** or **disclosure** of information may trigger a more subjective kind of harm (the collection, a feeling of being observed and the disclosure, embarrassment and humiliation), the **use** of information will trigger a more objective kind of harm (financial, physical, discrimination, etc.). Various criteria useful in order to evaluate this *risk of harm* will be proposed. The thesis aims at providing a guide that may be used in order to determine whether certain information should qualify as *personal information*. It will provide for a useful framework under which DPLs remain efficient in light of modern technologies and the Internet.

Key words: definition of *personal information*, data protection, privacy, Internet, risk of harm, purpose of data protection laws, interpretation.

LIST OF ABBREVIATIONS

Alberta DPL:	*Personal Information Protection Act* (Alberta)
ALRC:	Australian Law Reform Commission
APEC:	Asia-Pacific Economic Cooperation, a vehicle for promoting open trade and practical economic cooperation in the Asia-Pacific Region
Article 29 Working Party:	A group made up of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisor and the EC.
B.C.:	British Columbia
B.C. DPL:	*Personal Information Protection Act* (British Columbia)
B.U. L. Rev.:	Boston University Law Review
CA :	Cour d'appel
CAI (or C.A.I.):	Commission d'Accès à l'Information du Québec
Cal. L. Rev.:	California Law Review
Can. Crim. L. Rev.	Canadian Criminal Law Review
Canadian Charter:	Canadian Charter of Rights and Freedoms, PART I OF THE CONSTITUTION ACT, 1982
CCTV:	Closed Circuit Television
C.c.Q:	Civil Code of Quebec
C. de D. :	Cahiers de Droit
CIPPIC:	Canadian Internet Policy and Public Interest Clinic
CJLT:	Canadian Journal of Law and Technology
CNIL:	Commission Nationale de l'Informatique et des Libertés (France)
Colum. L. Rev.:	Columbia Law Review
Comité consultatif:	Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

Conn. L. Rev.:	Connecticut Law Review
Convention 108:	Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
COPPA:	Children's Online Privacy Protection Act
CPO:	Chief Privacy Officer
C.Q.:	Cour du Québec
C.S.:	Cour supérieure
Directive 95/46/EC:	Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data
Directive 2002/58/EC:	Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector
Directive 2006/24/EC:	Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic
DPI:	Deep Packet Inspection
DPLs:	Data protection laws
Drake L. Rev.:	Drake Law Review
FC:	Federal Court
Ga. L. Rev.:	Georgia Law Review
EC:	European Commission
EU:	European Union
FIPs:	Fair Information Practices
Fla. St. U. L. Rev.:	Florida State University Law Review
French DPL:	Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
FCC:	Federal Communication Commission
FTC :	Federal Trade Commission

Geo. L.J.:	Georgetown Law Journal
GLBA:	Gramm-Leach-Bliley Act
GPS:	Global Positioning System
Harv. C.R.-C.L. L. Rev.:	Harvard Civil Rights-Civil Liberties Law Review
Harv. J.L. & Tech.:	Harvard Journal of Law & Technology
Harv. L. Rev.:	Harvard Law Review
Hastings Const. L.Q.:	Hastings Constitutional Law Quaterly
Hastings L.J.:	Hastings Law Review
IAB:	Internet Advertising Bureau of Canada
IC:	Industry Canada
Ind. L. Rev.:	Indiana Law Review
Iowa L. Rev.:	Iowa Law Review
IP:	Internet Protocol
ISP:	Internet Service Provider
IVHS:	Intelligent Vehicle Highway Systems
J.O.:	Journal Officiel
L.C.:	Lois du Canada
L.Q.:	Lois du Québec
L.R.C.:	Lois révisées du Canada
L.R.Q.:	Lois refondues du Québec
LAN:	Local Area Network
Lindop Report:	The Report of the Committee on Data Protection drafted by Norman Lindop (U.K., 1978)
Manitoba L.J.:	Manitoba Law Journal
Mich. Telecomm. Tech. L. Rev.:	Michigan Telecommunications & Technology Law Review
Minn. L. Rev.:	Minnesota Law Review

Nat'l L.J.:	National Law Journal
Nordic Conference:	The 1967 Nordic Conference on the Right of Privacy
Nova L. Rev.:	Nova Law Review
NW. U. L. Rev.:	Northwestern University Law Review
N.Y.U. J. Legis. & Publ. Pol'y:	New York University Journal of Legislation & Public Policy
N.Y.U.L. Rev.:	New York University Law Review
OECD:	Organization for Economic Cooperation and Development
OECD Guidelines:	OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980)
OFT:	Office of Fair Trading (U.K.)
OPC:	Office of the Privacy Commissioner
OPCC:	Office of the Privacy Commissioner of Canada
OSN:	Online Social Network
PC:	Personal computers
Penn. St. L. Rev.:	Penn State Law Review
PIAC:	Public Interest Advocacy Centre
PII:	Personally Identifiable Information
PIPEDA:	Personal Information Protection and Electronic Documents Act (Canada)
Quebec Charter:	Charter of Human Rights and Freedoms (Quebec)
Quebec DPL:	An Act Respecting the Protection of Personal Information in the Private Sector (Quebec)
Quebec public sector DPL:	An Act respecting Access to documents held by public bodies and the Protection of personal information (Quebec)
Recommendation 509:	Recommendation 509 of 31 January 1968, on human rights and modern scientific and technological developments (Europe)

RFID:	Radio Frequency Identification
R.J.T. :	Revue juridique Thémis
San Diego L. Rev.:	San Diego Law Review
Stan. L. Rev.:	Stanford Law Review
UCLA L. Rev.:	UCLA Law Review
U.K.:	United Kingdom
U. Kan. L. Rev.:	University of Kansas Law Review
U. Pitt. L. Rev.:	University of Pittsburgh Law Review
UPPs:	Unified Privacy Principles
U.S.:	Unites States
Vand. L. Rev.:	Vanderbilt Law Review
Vill. L. Rev.:	Villanova Law Review
Wash. U. L.Q.:	Washington University Law Quaterly
Resolution (73) 22:	Committee of Ministers, Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector (Council of Europe)
Resolution (74) 29:	Committee of Ministers, Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector (Council of Europe)
Rich. J.L. & Tech.:	Richmond Journal of Law & Technology
Stan. L. Rev.:	Stanford Law Review
T.A.:	Décisions du tribunal d'arbitrage
Yale L.J.:	Yale Law Journal

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

I am grateful to many people in Canada and France. It is difficult to overstate my gratitude to my Ph.D. co-supervisors, Dr. Vincent Gautrais, *professeur titulaire* and *titulaire de la Chaire de l'Université de Montréal en droit de la sécurité et des affaires électroniques*, University of Montreal and Dr. Danièle Bourcier, *directrice de recherche au Centre National de la Recherche Scientifique*, member of the *Centre d'Études et de Recherches Scientifique* and of the *Centre d'Études et de Recherches en Sciences Administratives Politiques* (CERSA) of the University of Panthéon Assas (Paris II) and of the *Centre National de la Recherche Scientifique*, affiliated to the *École Doctorale de droit public, science politique et science administrative* of the University of Panthéon-Assas (Paris II). Throughout my thesis-writing period, Vincent Gautrais provided encouragement, thoughtful guidance, sound advice, good company, and lots of good ideas. Your unfailing enthusiasm and support from the earliest days of this project have been extremely reassuring. Danièle Bourcier was abundantly helpful and offered invaluable assistance, continued encouragement, support, guidance, and invaluable suggestions during this work. I would also like to convey my sincere thanks to the Law Faculties of Université de Montréal and Université de Panthéon Assas for their support. Many thanks also to la Fondation J.A. De Sève and la Fondation Monique Ouellette for their very useful and encouraging financial support.

I am also grateful for the ongoing support of the partners and colleagues at McMillan. They provide me with a challenging, stimulating and friendly working environment and have never questioned my ability to complete this project. I wish to express my love and gratitude to my beloved family; for its understanding through the duration of this project.

To all these people and the many I may have forgotten, thank you and I truly share this project with you.

LIST OF GRAPHIC(S)

See the graphic summarizing the proposed approach at p. 247.

INTRODUCTION

"We are in the midst of an information revolution, and we are only beginning to understand its implications."[1]

Privacy is no doubt essential for individuals as well as for the society in general and protecting privacy has always been seen as an important, sometimes even as a fundamental right.[2] Privacy is also indispensable for the protection of other rights, including freedom of speech and freedom of association.

The concern for the protection of privacy is relatively recent, in the sense that it has been stimulated by the growing pressures exerted by modern industrial society upon daily life.[3] Various definitions of *privacy* have been adopted since the late nineteenth century, illustrating an evolving concept. More precisely, there have been three different attempts at theorizing privacy.

A first step emerged when U.S. Judge Cooley defined privacy quite simply as "the right to be let alone".[4] This was followed by the landmark 1890 article that Samuel Warren ("Warren") and Louis D. Brandeis ("Brandeis") published in the Harvard Law Review, entitled "The Right To Privacy".[5] These authors were defending privacy against the threat of instantaneous photography in the popular press.[6] A second step in theorizing

---

[1] See Michel Serres, "Les nouvelles technologies : révolution culturelle et cognitive", online conference: <http://interstices.info/jcms/c_33030/les-nouvelles-technologies-revolution-culturelle-et-cognitive?portal=j_97&printView=true>, cited in Vincent Gautrais & Pierre Trudel, *Circulation des Renseignements Personnels et Web 2.0* (Montréal: Éditions Thémis, 2010) at 9: "Nous sommes face à une révolution. Une révolution de l'ampleur de laquelle nous n'avons peut-être pas totalement conscience."; See also Daniel J. Solove, "Privacy and Power: Computer Databases and Metaphors for Information Privacy" (2001) 53 Stan. L. Rev. 1393 at 1394 [Solove, "Privacy"]: "We are in the midst of an information revolution, and we are only beginning to understand its implications."

[2] See section 2.2.1.4.3(b)(i) entitled "Protecting Privacy is Important" which elaborates on this issue.

[3] The density of urban housing, the consequent difficulty of escaping from the prying eyes of neighbours, the ubiquity of commercial advertising and the increasing intrusiveness of social surveys, polls and market research are a few factors which have contributed to the conceptualization of the right to privacy. See Home Office, Lord Chancellor's Office, Scottish Office (Chairman The Rt. Hon, Kenneth Younger), *Report of the Committee on Privacy*, presented to Parliament by the Secretary of State for the Home Department, the Lord High Chancellor and the Secretary of State for Scotland by Command of Her Majesty, July 1972, at 6, para. 20 [*Report of the Committee on Privacy*].

[4] *Ibid*. at 327-28, Appendix K, Definitions of Privacy, c. 4.

[5] Samuel Warren & Louis Brandeis, "The Right to Privacy" (1890) 4:5 Harvard Law Review 193.

[6] James Waldo, Herbert S. Lin & Lynette I. Millett, eds., Committee on Privacy in the Information Age, National Research Council, *Engaging Privacy and Information Technology in a Digital Age* (Washington, US: The National Academies Press, 2007) at 20.

privacy took place in the late forties, upon the General Assembly of the United Nations adopting in 1948 the Universal Declaration of Human Rights in order to ensure that the atrocities that took place during the Second World War would not be repeated.[7] Privacy was then conceptualized as "the respect for one's private and family life, his home and his correspondence".

A third step in theorizing privacy came in the late 1960s and early 1970s, motivated, once again, by technological threats to privacy. With the development of automated data banks and the growing use of computers in the private and public sector, privacy was at that point conceptualized as having individuals "in control over their personal information".[8] The principles of Fair Information Practices ("FIPs") were elaborated during this period and have been incorporated in data protection laws ("DPLs") adopted in various jurisdictions around the world ever since. Under these DPLs, individuals have certain rights including the right to be informed of what personal information is collected about them, the use and the disclosure that will be made of their information, and have the right to consent to such data handling activities. Organizations handling personal information have certain obligations such as protecting the information using appropriate security methods, ensuring that the information used and disclosed is accurate, and granting access to the information that they are handling to the individuals to which the information pertains.

Personal information is defined similarly in various national DPLs (such as in France and Canada) as "information relating to an identified or identifiable individual".[9] This definition (or very similar definitions) have been included in transnational policy instruments such as in the 1980 *Convention for the Protection of Individuals with*

---

[7] *Universal Declaration of Human Rights*, G.A. res. 217(III), U.N.G.A.O.R., 3d Sess., Supp. No. 13, U.N. Doc A/810, (1948) 71 [*Universal Declaration of Human Rights*]. See preamble, second paragraph. Soon after, the Council of Europe, founded in 1949 and based in Strasbourg, adopted its own Convention for the Protection of Human Rights and Fundamental Freedoms. *European Convention for the Protection of Human Rights and Fundamental Freedoms,* 4 November 1950, 213 U.N.T.S. 221, E.T.S. 5, second paragraph of the Introductory section: "Considering the Universal Declaration of Human Rights proclaimed by the General Assembly of the United Nations on 10th December 1948". *Ibid*. art. 8.

[8] See section 1.1.2 entitled "Control over Personal Information and Fair Information Practices" which elaborates on this issue.

[9] See section 1.1.3 entitled "Definition of Personal Information: Origin and Background" which elaborates on this issue.

regard to Automatic Processing of Personal Data[10] ("Convention 108"), the 1981 *Guidelines for the protection of privacy and transborder flows of personal data*[11] ("OECD Guidelines"), and more recently, in the Asia-Pacific Economic Cooperation (or "APEC") Privacy Framework[12] ("APEC Privacy Framework"). Going back in time, we can note that identical or at least similar definitions of personal information were in fact used in the resolutions leading to the elaboration of the Convention 108 dating back to the early seventies.[13] This illustrates that a similar definition of *personal information* was already elaborated at that time, and has not been modified since.

The circumstances have changed fundamentally since privacy was conceptualized as "individuals in control of their personal information" over forty years ago. Individuals constantly give off personal information. The Internet now reaches billions of people around the world and serves as a virtual marketplace for products, information, and ideas. The fluidity of personal information collections has increased as the scope and goals of such data continuously evolve. New types of data and collection tools have emerged in cyberspace and are being used by private and public sector organizations for various purposes.[14] Online business models are increasingly based on the notion of greater customization and various online products and services are offered for free as they may be partially supported by advertising revenue.[15] Many online or mobile

---

[10] Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, E.T.S. 108 (1981) at art. 2 (a) [Convention 108]: "*personal data* means 'any information relating to an identified or identifiable individual'".

[11] The OECD was created in 1960, which brings together the governments of countries committed to democracy and the market economy from around the world. OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Paris: OECD Publications, 1980) at art. 1 b) [OECD, *Guidelines*]: *personal data* means "any information relating to an identified or identifiable individual".

[12] APEC was established in 1989 to further enhance economic growth and prosperity, is the premier forum for facilitating economic growth, cooperation, trade and investment in the Asia-Pacific region. APEC, *Privacy framework*, *supra* note 363 at art. 9 states: "Personal information means any information about an identified or identifiable individual."

[13] Council of Europe, Committee of Ministers, 26 September 1973, 224th meeting of the Ministers' Deputies, *Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector* [Council of Europe, *Resolution (73) 22*]; Council of Europe, Committee of Ministers, 20 September 1974, 236th meeting of the Ministers' Deputies, *Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector* [Council of Europe, *Resolution (74) 29*]. In each resolution, personal information was defined very broadly as "information relating to individuals (physical persons)".

[14] See section 1.2.2 entitled "New Types of Information and Collection Tools" and section 1.2.4 entitled "New Uses of Information" which elaborate on this issue.

[15] See section 1.2.4.1 entitled "New Business Models (Customization and Sponsored Services)" which elaborates on this issue.

service providers wish to use analytic solutions in order to improve their websites, products or services.[16] The second generation of the Internet makes possible greater interaction and connectedness among online users and individuals are becoming increasingly involved in managing their own data through online social networks ("OSNs").[17] There are also recent technological developments triggering the emergence of new identification tools, which allow for easier identification of individuals.[18] The power and scope of the activity of aggregating and correlating information have increased along with Internet technologies, and new algorithms are being developed that allow extraction of information from a sea of collected data.[19] Data-mining techniques and capabilities are reaching new levels of sophistication, and the convergence of different technologies now makes it possible for organizations to collect information that are of far more personal nature than before.[20]

In this context, I maintain that it is reasonable to wonder if the FIPs (or the DPLs) still provide for a proper legal framework. Because it is possible to interpret almost any data as *personal information* (any data can in one way or another be related to some individual) the question arises as to how much data should be considered as *personal information*. I maintain that when using a literal interpretation of the definition of *personal information*, many negative outcomes may occur. First, DPLs may be protecting all *personal information*, regardless of whether this information may be harmful to individuals or is worthy of protection. This encourages a potentially **over-inclusive** and burdensome framework, triggering a system under which organizations and industry players will incur additional costs for complying with DPLs, which have nothing to do with the protection of individuals. With the rise in popularity of

---

[16] See Eloïse Gratton, "Personalization, Analytics, and Sponsored Services: The Challenges of Applying PIPEDA to Online Tracking and Profiling Activities" (2010) 8 CJLT 299 [Gratton, "Personalization"].

[17] See section 1.2.1.2 entitled "New Ways of Using the Internet: Web 2.0" which elaborates on this issue.

[18] See section 1.2.3 entitled "New Identifying Methods" which elaborates on this issue.

[19] *Id.*, See also Waldo, Lin & Millet, *supra* note 6 at 2.

[20] See section 1.2.3 entitled "New Identifying Methods" which elaborates on this issue. See also Conseil de l'Europe, Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, *Rapport sur l'application des principes de protection des données aux réseaux mondiaux de télécommunications. L'autodétermination informationnelle à l'ère de l'Internet : Éléments sur la réflexion sur la Convention no 108 destinés au travail futur du Comité consultatif*, Strasbourg, 18 novembre 2004, at 24 [Conseil de l'Europe, *L'autodétermination informationnelle*].

cloud computing where organizations are storing all the data generated by users of cloud services,[21] this may lead to a large undertaking and an economic burden.

The definition of *personal information*, if interpreted using a strict literal method, may prove to be **under-inclusive**. It may not cover certain information which, "on their own", do not qualify as such. It may also not govern certain profiles falling outside of the scope of the definition, although these profiles are otherwise used or disclosed, creating some type of privacy or other harm to the individuals behind the profiles.

Using a literal interpretation of the notion of *personal information* may also create various **uncertainties**, especially in light of new types of data and collection tools which have recently emerged. Also, due to the fact that with recent technological developments, with unlimited resources and efforts, any information can be linked to an individual, more guidance is required in order to determine whether illegal means should be taken into account when determining if certain information is *personal*; what kind of resources (cost, efforts, etc.) should be used in assesssing whether a certain piece of information qualifies as *personal*; at what point is data *anonymized*; and whether the data should be evaluated "alone" or in "correlation" with other data available when assessing if certain information is *personal*. Also, when dealing with new types of data, it is not always clear if information identifying a device or an object qualifies as *personal data*; when a device is used by a group, at what point is it identifiable to an individual; and how accurate must the link be, between an individual and a piece of information, in order to qualify as "identifying" an individual.

A literal interpretation of the notion of *personal information* may also be **obsolete** in certain situations for instance if profile data is used to take a decision which has an impact on an individual behind the profile, although this individual is not "identified" (by name and address for example). I also maintain that pre-determined categories of so called "sensitive" information which focuses strictly on the nature of the information without taking into account the context of their availability may be obsolete.

---

[21] See Miranda Mowbray, "The Fog over the Grimpen Mire: Cloud Computing and the Law" (2009) 6:1 *SCRIPTed* 129 at 134; Randal C. Picker, "Competition and Privacy in Web 2.0 and the Cloud" (26 June 2008) at 3, online: SSRN <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1151985>.

At the time that the FIPs were initially elaborated in the early 1970s, their main purpose was to address specific concerns pertaining to computerized databases. The best way to deal with these data protection issues was deemed to be having individuals in control of their information.[22] Forty years later, that selfsame concept is still one of the most predominant theories of privacy and the basis for DPLs around the world.[23] While many issues with this theory still remain, a new approach in interpreting the notion of *personal information* may go a long way in dispelling them. This new approach is necessary in order for DPLs to be and remain effective in the future.

The definition of *personal information* was drafted in broad terms and it was meant to be flexible in part to survive technological advancements. I will propose a new method of interpreting the notion of *personal information*, taking into account the ultimate purpose behind the adoption of DPLs in order will ensure that only data that were meant to be covered by DPLs will in fact be covered.

In the context of proposing a new interpretation to the definition of *personal information*, the idea is to aim for a level of generality which corresponds with the highest level goal that the lawmakers wished to achieve. I will demonstrate how the ultimate purpose of DPLs is broader than protecting the privacy rights of individuals, as it is to protect individuals against the *risk of harm* that may result from the collection, use or disclosure of their information. Likewise, with the proposed approach, only data that may present such *risk of harm* to individuals would be protected. I argue that in certain cases, the *harm* will take place at the point of *collection* while in other cases, at the point where the data will be *used* or even *disclosed*. I will also elaborate on the fact that while with the activities of collection and disclosure, the risk of harm is of subjective nature, at the point which the information is used, this risk is usually of an objective nature. The *risk of harm* approach applied to the definition will reflect this and protect data only at the time that it presents such risk or in light of the importance or extent of such risk or harm.

---

[22] See section 1.1.2 entitled “Control over Personal Information and Fair Information Practices” which elaborates on this issue.

[23] See also Daniel J. Solove, “Conceptualizing Privacy” (2002) 90 Cal. L. Rev. 1087 at 1109 [Solove, “Conceptualizing”].

The proposed approach will have **various benefits**. For instance, it will provide for a more optimal protection, in the sense that data presenting no such risk of harm will flow freely. Therefore, for those entities that handle data presenting no palpable risk, many needless undertakings will be averted and no undue financial burden will be imposed. Another benefit with the proposed approach will be the elaboration of a badly needed flexible framework in the context of modern data protection issues; which is the best way to address both over-inclusive and under-inclusive outcomes of DPLs. It may also provide for a guide when there is uncertainty surrounding the qualification of certain information, or when there are provisions in DPLs providing for some type of subjectivity.[24] For instance, certain DPLs have some type of "reasonable" or "legitimacy" tests.[25] Using the proposed approach may assist organizations to determine if they are acting in compliance with these "reasonableness", "legitimacy", or "fairness" tests. For instance, if a certain data handling activity creates no or very low *risk of harm* for the individuals, then the organization could "reasonably" take the position that their activities are in fact reasonable, legitimate and fair.

The proposed approach would be useful in making sure that new types of data and unique identifiers linked to people or objects and not just basic biographical data are covered if they present a *risk of harm*, in making sure that two pieces data which, once correlated, present a *risk of harm* will be covered, in providing guidance in order to set guidelines assessing the sensitivity of certain data and in order to make sure that certain data, although they may not "identify" an individual, may still be covered if they are harmful to an individual.

Lastly, DPLs generally provide that individuals be told who is collecting their data and the purpose of such collection to enable them to decide whether to release control of all or part of such data. While the goal of this thesis is not to re-open and challenge the notion of privacy as "control" and the FIPs (but rather, to test-drive the current data protection legal framework, assess its viability in light of recent technological developments and propose a new guide for interpreting the notion of *personal information*), I argue that an interpretation which focuses on the *risk of harm* would

[24] See section 2.2.1.3.2(a) entitled "DPLs Already Subjective on Various Issues" which elaborates on the type of subjectivity found in DPLs.

[25] See section 2.2.1.3.2(a)(i) entitled "Reasonableness or Legitimacy " which elaborates on this issue.

have the result of reducing the burden of the notification obligation. Given that individuals may be overloaded with information in quantities that they cannot realistically be expected to process or comprehend, obtaining adequate consent from individuals may be impossible in many cases.[26] While transparency of data processing would remain a fundamental principle, notification would be required only in cases of the presence of *risk or harm*. This may translate in a website privacy policy potentially becoming a one paragraph user-friendly statement outlining, for example, the fact that the website may sell the profile information collected to third parties.

The approach proposed in this thesis aims at assisting lawmakers, policymakers, privacy commissioners, courts, organizations handling personal information and individuals assessing whether certain information should be governed by the relevant DPL, depending on whether the data handling activity at stake creates a *risk of harm* for the individual to which the data pertains. I maintain that this will provide for a useful framework under which DPLs remain efficient in light of modern technologies.

In the preliminary section, I will provide an overview of the historical perspective of laws protecting privacy and discuss the evolution of the notion of privacy as well as the conception of privacy as "control over personal information" (and the FIPs). Then, I will elaborate on the changes which have recently taken place at the technological level, such as an increase in the volume of data available and data exchanges, the emergence of new types of data and collection tools, new identifying methods, new uses, and an increased availability of information.

Section 2 is divided into two sections. In section 2.1, I will deconstruct the notion of privacy as "control over personal information", which is the basis of DPLs around the world. More specifically, I will demonstrate how, over forty years after the elaboration of the principles of FIPs incorporated in DPLs, it is time to go back to the drawing board. I will illustrate how, in the context of new Internet technologies, the concept of "control over personal information" is challenged since under this conception, privacy is viewed as an absolute right, ignoring the importance of the data flow for the society as well as over countervailing values such as free speech and freedom of information. I will also discuss how the "notice and choice" approach is challenged with the current volume of

[26] See section 2.1.1.2 entitled "Notice and Choice Approach Challenged" which elaborates on this issue.

data collections and vagueness of privacy policies, the increase in the volume of players involved, the dynamic aspect of privacy policies and business models, and due to the fact that with technology becoming increasingly sophisticated, individuals may have a hard time understanding what kind of information is being collected about them and how their information will in fact be used. I will also elaborate on how a literal interpretation of the definition of *personal information* (the object of protection of the DPLs) is no longer workable, as it has the outcome of triggering an over-inclusive outcome in certain situations, an under-inclusive effect in others, how it may create uncertainty as to which data qualifies as *personal information* and may even in some cases provide for an obsolete framework. In light of this, I will explain, in section 2.2, the reasoning behind the proposed approach in reconstructing the definition of *personal information*. To do so, I will be presenting the proposed approach to interpreting the definition of *personal information*, under which the ultimate purpose behind DPLs should be taken into account. I will provide an overview of the limits and benefits of this approach as well. I will then demonstrate what is the ultimate purpose of DPLs: to protect individuals against a *risk of harm* triggered by organizations collecting, using and disclosing their information.

In section 3, I will elaborate on the fact that this risk of harm may in certain cases be more subjective and may relate to a breach of privacy while in other cases, this harm may be more objective in nature and have much less to do with privacy. More specifically, I will demonstrate how this harm is different depending on the data handling activity at stake. I will detail what kind of harm, problems or concerns DPLs were attempting to address, by analyzing the purpose or goal of each activity which is regulated by DPLs: the collection, the disclosure, and the use of personal information. Section 3 will therefore offer a way forward, proposing a decision-tree test useful when deciding whether certain information should qualify as *personal information*. I will also demonstrate how the proposed test would work in practice, using practical business cases as examples.

1. BACKGROUND LEADING TO THE DEFINITION OF PERSONAL INFORMATION

Concern for the protection of privacy has been stimulated by the growing pressures exerted by modern industrial society upon daily life; including such factors as the density of urban housing, the consequent difficulty of escaping from the prying eyes of neighbors, the ubiquity of commercial advertising and the increasing intrusiveness of social surveys, polls and market research.[27]

In this section, I will present an overview of the laws protecting privacy in North America and Europe in the last century. Then, I will discuss the technological changes, which have recently taken place.

1.1. Historical Background Leading to Laws Protecting Personal Information

> "(…) the idea that technology threatens privacy isn't new at all. Much of our modern notion of privacy, the threats to it, and the need to protect it, grew out of past encounters with new technology".[28]

This section will elaborate on the evolution of the notion of privacy, on the conception of privacy as "control over personal information", on the elaboration of the principles of FIPs, and on the origin and background of the definition of *personal information* which is at the heart of these FIPs.

1.1.1. Evolution of the Notion of Privacy

Various definitions of *privacy* have been adopted throughout time, illustrating a multifaceted and evolving concept. More precisely, there have been three different attempts at theorizing privacy since the late nineteenth century.

1.1.1.1. First Wave: Right to be Let Alone

A first step in theorizing privacy emerged in 1888 when U.S. Judge Cooley defined privacy quite simply as "the right to be let alone".[29] This was followed by the landmark

---

[27] *Report of the Committee on Privacy*, *supra* note 3 at 6, para. 20.

[28] George Radwanski, "Address to the Privacy Lecture Series" (Toronto, 26 March 2001) at 2, online: <http://privacy.openflows.org/pdf/radwanski_march26_2001.pdf>.

[29] See *Report of the Committee on Privacy*, *supra* note 3 at 327-28, Appendix K, c. 4, Definitions of Privacy.

1890 article that Warren and Brandeis published in the Harvard Law Review, entitled "The Right To Privacy".[30] Warren and Brandeis were defending privacy against "recent inventions and business methods" and more specifically against the threat of new technology, namely instantaneous photography in the popular press which was "invading the sacred precincts of private and domestic life".[31] It was precisely this "right to be let alone" that was being threatened and this definition of privacy has been, to a certain extent, followed by some over the years.[32] This concept of privacy is viewed by some as being far too broad[33] or too limited in today's context.[34]

1.1.1.2. Second Wave: Right for Respect for Private and Family Life

In 1948, the General Assembly of the United Nations adopted the Universal Declaration of Human Rights,[35] in order to ensure that the atrocities that took place during the Second World War would not be repeated.[36] The Declaration states, at article 12, that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation (…)". Soon after, the Council of Europe, founded in 1949 and based in Strasbourg, adopted its own Convention for the Protection of Human Rights and Fundamental Freedoms.[37]

---

[30] Warren & Brandeis, *supra* note 5.

[31] Waldo, Lin & Millet, *supra* note 6 at 20.

[32] For instance, U.S. Chief Justice Burger in May 1970 defined privacy as: "The very basic right to be free from sights, sounds and tangible matter we do not want." In the conclusions of the Nordic Conference on the Right of Privacy (1967), privacy was defined as follows: "2. The right to privacy is the right to be let alone to live one's own life with the minimum degree of interference." Professor Alan Westin (1967), in one of two definitions of privacy which he provided, states: "Viewed in terms of the relation of the individual to social participation, privacy is the voluntary and temporary withdrawal of a person from the general society through physical and psychological means, either in a state of solitude or small group intimacy or, when among larger groups, in a condition of anonymity or reserve." These definitions are detailed in *Report of the Committee on Privacy*, *supra* note 3, Appendix K, c. 4, Definitions of Privacy.

[33] See Anita Allen, *Uneasy access: privacy for women in a free society* (Totowa, New Jersey: Rowman & Littlefield, 1988) at 7: "If privacy simply meant 'being let alone', any form of offensive or harmful conduct directed toward another person could be characterized as a violation of personal privacy. A punch in the nose would be a privacy invasion as much as peep in the bedroom."

[34] Solove, "Conceptualizing", *supra* note 23 at 1101-02; Radwanski, *supra* note 28 at 2.

[35] *Universal Declaration of Human Rights*, *supra* note 7.

[36] *Ibid*. See preamble, second paragraph: "Whereas disregard and contempt for human rights have resulted in barbarous acts which have outraged the conscience of mankind, and the advent of a world in which human beings shall enjoy freedom of speech and belief and freedom from fear and want has been proclaimed as the highest aspiration of the common people (…)".

[37] *European Convention for the Protection of Human Rights and Fundamental Freedoms*, *supra* note 7, second paragraph of the Introductory section: "Considering the Universal Declaration of Human Rights proclaimed by the General Assembly of the United Nations on 10th December 1948."

With regards to privacy, article 8 provided a similar right to respect for one's private and family life, his home and his correspondence, subject to certain restrictions.[38]

Many then followed this trend in conceptualizing privacy. For example, the 1967 Nordic Conference on the Right of Privacy[39] (the "Nordic Conference") expanding on what they meant by the right of privacy (which they equated with the "right to be let alone", therefore in reference to the first wave), also spoke of a person's "private, family or home life" as the first area to be protected.[40]

This concept is still relevant nowadays and the protection of someone's private life, personal correspondence and communications is often protected by law.[41] This particular wave did not originate from a fear of technological developments; rather, it arose out of a fear that the carnage of the Second World War would be repeated.

1.1.1.3. Third Wave: Control over Personal Information

A third wave in theorizing privacy came in the late 1960s and early 1970s, motivated, once again, by technological threats to privacy. In 1967, it had already been argued that the European Convention on Human Rights was flawed and would quickly become obsolete, as it lagged behind technological developments.[42] Suggesting that most of these developments could not have been foreseen by their authors when it was drafted,[43] Karl Czernetz, a member of the Council of Europe, stressed that:

---

[38] *Ibid*. art. 8.

[39] The Nordic Conference on Privacy was organized by the International Commission of Jurists and it took place in Stockholm in May 1967.

[40] The Nordic Conference on the Right of Privacy (1967) concluded that privacy was: "2. (…) The right of the individual to lead his own life protected against: (a) interference with his private, family and home life; (…) (h) interference with his correspondence (…)". See the Conclusions of the Nordic Conference of International Jurists on the Right of Privacy, Stockholm, 1967, discussed in *Report of the Committee on Privacy*, *supra* note 3 at 18, para. 60, Appendix K.

[41] For example, in Quebec, someone's private life, his home and his correspondence are protected by articles 36 (2) and (6) of the C.c.Q. which states that: "The following acts, in particular, may be considered as invasions of the privacy of a person: (…) (2) intentionally intercepting or using his private communications; (…) (6) using his correspondence, manuscripts or other personal documents." See also article 9 of the French Civil Code.

[42] Council of Europe, Explanatory Memorandum of the Consultative Assembly of the Council of Europe, *Report on human rights and modern scientific and technological developments*, Doc. 2326 (1968) at s. III, para. 4 [Council of Europe, *Report on human rights*].

[43] *Ibid*. at s. III, para. 11.

> "If we are not soon to live under conditions which exceed by far what Orwell imagined we must act and find an answer to the question of how human rights and fundamental freedoms can effectively be protected in the modern State and modern society and what measures must be taken in order to prevent the technical revolution from being a threat to the dignity and integrity of the human person".[44]

Most of the documents produced by privacy experts (including Alan Westin's 1967 book on *Privacy and Freedom*) and from the Council of Europe or other organizations which took place in the late 1960s referred to technologies such as phone-tapping, electronic eavesdropping, surreptitious observation, hidden television-eye monitoring, truth measurement by polygraphic devices, personality testing for personnel selection, the illegitimate use of official statistical and similar surveys to obtain private information, and subliminal advertising and propaganda.[45]

At the Council of Europe level, two motions pertaining to new technical devices for eavesdropping[46] and modern scientific and technological developments[47] were referred by the Assembly to the Legal Committee in 1967.[48] What followed was a Report on human rights and modern scientific and technological developments,[49] directed to the Legal Committee,[50] which in turn resulted in *Recommendation 509 of 31 January 1968, on human rights and modern scientific and technological developments* ("Recommendation 509").[51] This Recommendation 509 was addressed to the Committee of Ministers requesting to examine whether the European Human Rights Convention[52] offered an adequate protection to the right of personal privacy vis-à-vis

---

[44] *Ibid*. at s. III, para. 13.

[45] *Ibid*. at s. III, paras. 3-6. Also see Alan F. Westin, *Privacy and Freedom* (New York: Atheneum, 1967) [Westin, *Privacy and Freedom*].

[46] Council of Europe, PA, *Motion for a Resolution calling for a study of the problem of legislation and control with regard to new technical devices for eavesdropping*, Doc. 2226 (1967) [Council of Europe, *Motion for a Resolution calling for a study*].

[47] Council of Europe, PA, *Motion for a Resolution on Human rights and modern scientific and technological developments*, Doc. 2206 (1967), presented by Mr. Karl Czernetz [Council of Europe, *Motion for a Resolution on Human rights*].

[48] Council of Europe, *Report on human rights*, *supra* note 42 at s. III, para. 3.

[49] *Ibid*.

[50] Council of Europe, PA, 16th sitting, *on the Human rights and modern scientific and technological developments*, Doc. 2326 (1968), Directed to the Legal Committee [Council of Europe, 16th sitting].

[51] Council of Europe, Consultative Assembly of the Council of Europe, *Recommendation (509) 68 of 31 January 1968, on human rights and modern scientific and technological developments* [Council of Europe, *Recommandation (509) 68*].

[52] And the domestic laws of the member States.

these modern scientific and technical methods.[53] A study conducted from 1968 to 1970 in response to Recommendation 509 concluded that foremost of all privacy concerns were: the ever expanding files of personal data about millions of citizens, the development of automated data banks and the growing use of computers in sharing, matching, and mining data.[54] More specifically, the study showed how article 8 of the European Convention on Human Rights and existing European national legislations touched upon the protection of privacy only from a limited point of view, such as secrecy of correspondence, communications and inviolability of the domicile (what I refer to as the second wave),[55] and therefore did not provide adequate protection to individual privacy and other rights and interests of individuals with regard to automated data banks.[56] Therefore, although Recommendation 509 did not specifically refer to automated databanks, it is at the root of the Council of Europe's work in the field of data protection.

As the growing number of automated data banks and computers represented the biggest concern for policymakers in the early 1970s, most of the privacy work pursued at that time focused on this main threat.[57] For instance, a 1973 U.S. report addressed the unease arising from new computer-based record keeping practices, placing emphasis on the fact that, more and more, information was to be collected using an impersonal method:

> "Concern about the effects of computer-based record keeping on personal privacy appears to be related to some common characteristics

---

[53] Council of Europe, *Recommandation (509) 68*, *supra* note 51 at para. 8 (i).

[54] See Council of Europe, *Report on human rights*, *supra* note 42 at s. III, paras. 4-6.

[55] See section 1.1.1.2 entitled "Second Wave: Right for Respect for Private and Family Life" which elaborates on this issue.

[56] See Council of Europe, Comitte of Ministers, *Explanatory Report: Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector* at para. 2 [Council of Europe, *Explanatory Report: Resolution (73) 22*].

[57] See for instance the work which was undertaken by the OECD's Computer Utilisation Group, which produced a number of Informatics Studies in 1971 with titles such as "Computerised Data Banks in Public Administration", "Digital Information and the Privacy Problem", and "Policy Issues in Data Protection and Privacy". In Canada, a federal government task force report on privacy and computers was produced in the early seventies: Department of Communications and Department of Justice, *Privacy and Computers: A Report of a Task Force* (Ottawa: Information Canada, 1972); In the U.S., the principles of FIPs for the protection of personal information were first enunciated in a 1973 report of the U.S. Department of Health, Education and Welfare: U.S. Department of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens* (Washington: U.S. Government Printing Office, 1973); See also Arthur R. Miller, *The Assault on Privacy: Computers, Data Banks, and Dossiers* (Ann Arbor: The University of Michigan Press, 1971).

> of life in industrialized societies. In the first place, industrial societies are urban societies. The social milieu of the village that allowed for the exchange of personal information through face-to-face relationships has been replaced by the comparative impersonality of urban living. Industrial society also demands a much more pervasive administration of governmental activities-the collection of taxes, health insurance, social security, employment services, education-many of which collect and use personal data in an impersonal way."[58]

The way to address this specific threat has led to conceptualizing privacy as the individuals in "control of their personal information", as detailed in section 1.1.2. Certain key documents generated in the late 1960s, such as the Justice Bill adopted in the U.K., illustrate the transition from the second wave to the third wave. This "Justice" Bill, also known as the Brian Walden's Right of Privacy Bill (November 1969), made a link between the second and third waves: it spoke of a person's state of being "protected from intrusion upon himself, his home, his family, his relationships and communications with others, his property and his business affairs (…)"[59] in reference to what I refer to as the second wave.[60] Interestingly, this bill also added to a person's protection from the forms of intrusion mentioned above, the: "intrusion by (…) the unauthorised use or disclosure of confidential information, or facts (including his name, identity or likeness) calculated to cause him distress, annoyance or embarrassment, or to place him in a false light"[61] which relates to the third wave.[62]

1.1.2. Control over Personal Information and Fair Information Practices

The privacy threats resulting from the growing number of automated data banks and computers has led to conceptualizing privacy as the "control over personal information", initially with a focus on information located in electronic data banks and eventually to all information, whether in electronic form or not. This concept of "control"

---

[58] See U.S. Department of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *supra* note 57.

[59] See Justice Committee on privacy, "Privacy and the Law" reported in *Report of the Committee on Privacy*, *supra* note 3 at 17, para. 47, Appendix J, clause 9.

[60] See section 1.1.1.2 entitled "Second Wave: Right for Respect for Private and Family Life" which elaborates on this issue.

[61] See *Report of the Committee on Privacy*, *supra* note 3 at 18, para. 61.

[62] For details on this third wave, please refer to section 1.1.1.3 entitled "Third Wave: Control over Personal Information".

has also led to the well-known international standard for data protection FIPs,[63] which is at the core of DPLs and the foundation for most DPLs around the globe, up until today.[64]

1.1.2.1. Initial Concern: Computers and Electronic Data Banks

In the early 1960s, computers made their first appearance as administrative aids. At that point, given the fact that computers were expensive and their use was limited to a small number of public services, the need to protect citizens against possible risks for their privacy did not appear to be urgent.[65] By the late 1960s and early 1970s, data processing had already become an essential feature of administration and management and had invaded individuals' daily lives.[66] Electronic data processing was present in all facets of human activity, it had become virtually indispensable in certain fields and was seen as an efficient and powerful instrument to solve complex problems.[67]

At the same time, a particular new source of possible intrusion into privacy had been created by the rapid growth and popularisation of computer technology.[68] An increasing amount of information on almost every citizen was now recorded in automated files, with greater capacity and storage capabilities than manual files.[69] Naturally, many

---

[63] These principles were set out by the OECD, *Guidelines*, *supra* note 11. In Canada, they were further developed by the Canadian Standards Association in its *Model Code for the Protection of Personal Information* (CSA Publications, 1996), and adopted in the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, Schedule 1 [PIPEDA]. In Europe, they were incoporated in Convention 108 and more recently, in Directive 95/46/EC.

[64] See section 1.1.2.2 entitled "Still about Control: Canadian and French Data Protection Laws" which elaborates on this issue.

[65] See Council of Europe, Committee of Ministers, *Explanatory Report: Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector* at para. 1 [Council of Europe, *Explanatory Report: Resolution (74) 29*].

[66] Council of Europe, PA, *Report on data processing and the protection of human rights*, Doc. 4472 (1980) at s. II, s. 2, para. 1 [Council of Europe, *Report on data processing*].

[67] Council of Europe, *Explanatory Report: Resolution (74) 29*, *supra* note 65 at para. 2.

[68] Council of Europe, *Explanatory Report: Resolution (73) 22*, *supra* note 56 at para. 3.

[69] Council of Europe, *Report on data processing*, *supra* note 66 at s. II, s. 2, para. 1; Also see Council of Europe, *Explanatory Report: Resolution (73) 22*, *supra* note 56 at para. 21: "A rule concerning the volume of the information is necessary in view of the capacity of electronic data banks to absorb an almost unlimited quantity of information, to preserve it indefinitely, to hand it out instantly and to link scattered information" (…) "By way of illustration it may be mentioned that currently the most popular form of storage, which will allow the retrieval of data in an average of 30/1000ths of a second, is on magnetic disk. Each disk contains 100 million characters, or 200 million numeric digits of information. The major banks in Britain hold approximately 25 000 million characters 'on-line' on disks for essential overnight processing. Users of electronic data banks have a material interest to store in one single operation the optimum

individuals feared that they would relinquish the control over their personal information to those controlling the databases (i.e. the information).[70]

The discussions that took place in most of the industrial nations around this period revolved around the following themes: loss of individuality, loss of control over information, the possibility of linking data banks to create dossiers, rigid decision making by powerful, centralized bureaucracies.[71] These discussions prompted official action by various governments and other transnational or international organizations. Regulating the manner in which information could be gathered seemed necessary in order to prevent the use of improper methods or a lack of transparency surrounding the collection of information.[72] The fact that these automated files could be linked together and that information collected could be used for an undisclosed or new purpose was another concern.[73]

The Council of Europe team working on these issues was aware that it is was much more difficult for an individual to take steps to protect his personal interests towards a computerised information system than it was with regard to a traditional data register.[74] Also, given that problems could arise from the ease in transmitting data between computers and computer terminals installed in different jurisdictions, the fact that this was an international issue was already being examined.[75]

---

amount of information, both information for immediate use and information for later use. Although normally electronic data banks contain only such amounts of information as are economically justifiable, it seems advisable to adopt a rule which would halt unbridled hoarding of data."

[70] *Report of the Committee on Privacy*, *supra* note 3 at 180, para. 582: "On the first count the computer's facility to assist the compilation of complete personal profiles or individuals is seen by some to facilitate the exercise of power over them in the hands of those who control this information (…)."

[71] U.S. Department of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *supra* note 57.

[72] See Council of Europe, *Explanatory Report: Resolution (73) 22*, *supra* note 56 at para. 22.

[73] Council of Europe, *Report on data processing*, *supra* note 66 at s. II, s. 2, para. 1: "The growing number of files containing information on the health, the social, economic or penal situation and the opinions of individuals is reckoned as a threat in our societies not only because of discrimination between the minority having access to this information and the rest, but also because of the possibility of establishing interconnections between data banks and using the information obtained for undisclosed purposes."

[74] See Council of Europe, *Explanatory Report: Resolution (73) 22*, *supra* note 56 at para. 3.

[75] *Ibid*. at para. 4: "(…) certain aspects of the problem can only be satisfactorily solved by a concerted intergovernmental action (for example problems arising from the facility of transmission of data between computers and computer terminals installed in different States)"; Council of Europe, PA, *Opinion on data processing and the protection of human rights presented by the Legal Affairs Committee*, Doc. 4484 (1980) at s. III, para. 16: "The Council of Europe has endeavoured to find international solutions to the

1.1.2.1.1. Control Over Information in Electronic Data Banks

Council of Europe working documents leading to Convention 108 reported that privacy issues pertaining to the use of automated files should be dealt with by enabling individuals to control their own information. This method proved to be more practical than trying to define privacy, as it allowed for more objectivity.[76]

Various authors, during this period and already as early as the late 1960s, started conceptualizing privacy as "control over personal information". For example, according to Alan Westin: "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others".[77] Similarly, Hyman Gross approached privacy as "control over acquaintance with one's personal affairs".[78] According to Charles Fried, "Privacy is not simply an absence of information about us in the minds of others; rather it is the *control* we have over information about ourselves".[79] Arthur Miller declared that "the basic attribute of an effective right of privacy is the individual's ability to control the circulation of information relating to him".[80] Documents and reports from this period pertaining to privacy concerns and legislation initiatives began conceptualizing privacy as the individual's control over his or her personal information.[81] Numerous other scholars have since

---

problems posed by the international flow of personal data"; See also *ibid*. at s. IV, para. 21: "The difficulties raised by the international flow of personal data cannot be solved entirely satisfactorily at national level: they require international solutions."

[76] See *Report of the Committee on Privacy*, supra note 3 at 180, para. 583: "We suggest below the principles which, in our view, should govern the collection and dissemination of information by computer in the private sector."; See also *ibid*. at 187, para. 608: "The Bill would require the Tribunal to have regard to certain considerations, of which the main ones would be the 'general utility' of the 'data bank', the right of the individual to control the handling of the information about him, and the propriety of disclosing certain information."

[77] Westin, *Privacy and Freedom*, *supra* note 45 at 7.

[78] Hyman Gross, "The Concept of Privacy" (1967) 42 N.Y.U.L. Rev. 34 at 36.

[79] Charles Fried, "Privacy" (1968) 77 Yale L.J. 475 at 482, 493 [Fried, "Privacy"].

[80] Miller, *supra* note 57 at 25.

[81] See for example U.S. Department of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *supra* note 57 at s. III "Safeguards for Privacy": "An individual's personal privacy is directly affected by the kind of disclosure and use made of identifiable information about him in a record. A record containing information about an individual in identifiable form must, therefore, be governed by procedures that afford the individual a right to participate in deciding what the content of the record will be, and what disclosure and use will be made of the identifiable information in it. Any recording, disclosure, and use of identifiable personal information not governed by such procedures must be proscribed as an unfair information practice (…). This formulation does not provide the basis for determining a priori which data should or may be recorded and used, or why, and when. It does, however, provide a basis for establishing procedures that assure the individual a right to participate in a meaningful way in decisions about what goes into records about him and how that information shall be used."

articulated privacy theories similar to privacy as control of information.[82] Security expert Bruce Schneier believes that the privacy theory of *privacy as control* remains more relevant than ever.[83]

Recommendation 509 led the way to two resolutions on data protection at the Council of Europe level: *Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector* ("Resolution (73) 22") established principles of data protection for the private sector[84] and *Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector* ("Resolution (74) 29") did the same for the public sector[85] (hereinafter, "Resolutions (73) 22 and (74) 29"). These listed a number of general rules to be complied with when personal information was stored in electronic data banks. These rules were putting individuals in control of their information in the sense that they were to have the right to know the information stored about them, the purpose for which their information had been recorded, particulars of each release of their information, and have a right to have corrected or erased inaccurate information. These principles, more commonly known as the principles of FIPs, form the "hard core" of Convention 108 and

---

[82] See Adam Carlyle Breckenridge, *The Right to Privacy* (Lincoln: University of Nebraska Press, 1970) at 1: privacy is "the individual's right to control dissemination of information about himself"; Randall P. Benzanson, "The Right to Privacy Revisited: Privacy, News, and Social Change, 1890-1990" (1992) 80 Cal. L. Rev. 1133 at 1135: "I will advance a concept of privacy based on the individual's control of information"; Ian Goldberg et al., "Trust, Ethics, and Privacy" (2001) 81 B.U. L. Rev. 407 at 418: "We build our own definition of privacy on what we consider the most elegant definition, 'informational self-determination,' which refers to a person's ability to control the flow of his own personal information"; See also Chris Jay Hoofnagle & Kerry E. Smith, "Debunking the Commercial Profilers' Claims: A Skeptical Analysis of the Benefits of Personal Information Flows" (June 2003) at 1, online: SSRN <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=504622>: "The public benefits from open and transparent flows, consistent with FIPs, where the control of the information resides with the individual."

[83] Bruce Schneier, "Privacy and Control" (6 April 2010), online: Schneier on Security <http://www.schneier.com/blog/archives/2010/04/privacy_and_con.html> [Schneier, "Privacy and Control"]: "To the older generation, privacy is about secrecy. And, as the Supreme Court said, once something is no longer secret, it's no longer private. But that's not how privacy works, and it's not how the younger generation thinks about it. Privacy is about control. When your health records are sold to a pharmaceutical company without your permission; when a social-networking site changes your privacy settings to make what used to be visible only to your friends visible to everyone; when the NSA eavesdrops on everyone's e-mail conversations -- your loss of control over that information is the issue. We may not mind sharing our personal lives and thoughts, but we want to control how, where and with whom. A privacy failure is a control failure."

[84] Council of Europe, *Resolution (73) 22*, *supra* note 13.

[85] Council of Europe, *Resolution (74) 29*, *supra* note 13.

were to be incorporated into all national DPLs. Most work done on data protection issues around that period revolved around these FIPs.[86]

The aforementioned Resolutions (73) 22 and (74) 29 paved the way for one of the first transnational privacy policy instruments: Convention 108.[87] Its purpose was to protect personal data undergoing automatic processing. The issues of privacy and automated databanks were discussed within the auspices of several international organizations such as the United Nations, UNESCO and the OECD.[88] From the latter's perspective, one of the main concerns was that there was a danger that disparities in national DPLs could hamper the free flow of personal information across borders.[89] This could cause serious disruptions in important sectors of the economy, such as banking and insurance. The principles of FIPs found in Convention 108 were similar to the OECD Guidelines.[90] In fact, efforts were made to minimize the divergences between the two initiatives.[91]

1.1.2.1.2. Electronic Databanks becomes All Databanks

The initial focus of the protection was the collection of personal information in electronic databases, which caused more apprehension than manual or paper files.[92]

---

[86] In the U.S., 1973, the United States Department of health Education and Welfare (HEW) issued a report in 1973 which was entitled: "Records, Computers, and the Rights of Citizens," which analyzed these problems in depth and which recommended the passage of a code of FIPs. See U.S. Department of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *supra* note 57. See also Daniel J. Solove, "A Brief History of Information Privacy Law" (2006) *Proskauer on Privacy PLI* at I-25.

[87] Convention 108, *supra* note 10.

[88] Council of Europe, *Explanatory Report: Resolution (74) 29*, *supra* note 65 para. 6. Certain reports have also been published by the OECD in its "Informatics Studies" series in 1971 with titles such as "Computerised Data Banks in Public Administration", "Digital Information and the Privacy Problem" and "Policy Issues in Data Protection and Privacy".

[89] Council of Europe, *Report on data processing*, *supra* note 66 at 11, ss. II, 6.

[90] OECD, *Guidelines*, *supra* note 11.

[91] Convention 108, *supra* note 10 at paras. 14-16.

[92] For example, see Council of Europe, *Explanatory Report: Resolution (73) 22*, *supra* note 56 at para. 3: "While few would deny the great advantages offered by the application of electronic data processing techniques, there is a growing concern among the public about the possibility of improper use being made of sensitive personal information stored electronically. It is, for example, much more difficult for an individual to take steps to protect his personal interests vis-a-vis a computerised information system than it is with regard to a traditional data register." Also see Council of Europe, *Report on data processing*, *supra* note 66 at ss. II, 2, para. 1: "Although only thirty years old, data processing has become an essential feature of administration and management and is invading our daily lives. An increasing amount of information on almost every citizen is recorded in automated files whose capacity is much greater than that of manual files. These files offer obvious advantages to their users, but the risks they involve for the rights and freedoms of those about whom data are recorded are difficult to assess."

According to working documents leading to Convention 108, the initial goal was to cover only those electronic data banks which actually disseminated information and not those used strictly for internal purposes.[93]

Eventually, "electronic databanks" became "all databanks". While preparing the Resolutions (73) 22 and (74) 29, the Council of Europe Committee on the protection of privacy emphasised that threats to privacy may arise not only from the use of computerised information systems, but also from other kinds of data collections.[94] According to the Committee, the likelihood that some Member States would adopt new regulations applicable both to electronic and manual data collections was high. The Committee also instructed governments to make sure that the introduction of new rules on electronic data processing would not complicate the modernisation of administration.[95] Similar positions were taken by various European jurisdictions. In the U.K., the 1978 *Report of the Committee on Data Protection* by Norman Lindop (the "Lindop Report") stated that:

> "(…) many of those who submitted evidence to us stressed that, to avoid unfair discrimination between those data users who use up-to-date technology and those who do not, data protection measures should apply to all personal data systems whether they make use of computers or not, whether they are automated fully, partly or not at all, and regardless of whether the data are recorded on stone, vellum, paper, film or magnetisable materials."[96]

More specifically, the Lindop Report raised another argument in favour of extending legislation to all personal data systems, which was the difficulty of distinguishing automated and manual systems. All automated systems involved some type of manual

---

[93] See Council of Europe, *Explanatory Report: Resolution (73) 22*, *supra* note 56 at para. 13: "As the resolution refers to electronic data banks which actually disseminate information (see paragraph 16), it will not normally apply to electronic data banks which are used only for internal purposes, such as a personnel administration. If, however, at a later stage, such a bank does disseminate information, it will be covered by the resolution. It is left to the discretion of the member States whether they wish to extend the principles set out in the resolution to all electronic data banks, even to those, which are used only for internal purposes." This was different for the public sector since they felt that with regard to the public sector, it was difficult to distinguish between "internal" and "external" use: See Council of Europe, *Explanatory Report: Resolution (74) 29*, *supra* note 65 at para. 13.

[94] See Council of Europe, *Explanatory Report: Resolution (73) 22*, *supra* note 56 at para. 9.

[95] *Ibid*. at para. 9.

[96] Chairman Sir Norman Lindop, *Report of the Committee on Data Protection: Presented to Parliament by the Secretary of State for the Home Department by Command of Her Majesty* (London, UK: H.M.S.O., 1978) at 11-12, para. 2.12.

data handling, for there were always clerical processes and human consideration of the data before and/or after the automatic handling.[97] In Scotland, the 1972 *Report of the Committee on Privacy* also shared similar views.[98]

This distinction between different mediums (electronic vs. paper) is still relevant today in certain jurisdictions such as Europe. The Article 29 Working Party, a group made up of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisor and the EC, suggests that those who interpret the *Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*[99] ("Directive 95/46/EC") should not forget that the reasons for enacting the first DPLs in the 1970s was largely due to the fact electronic data processing allowed for easier and more widespread access to personal data than traditional forms of data handling.[100] In fact, Directive 95/46/EC aims at protecting such forms of processing of personal data which are typical for a higher risk of "easy access to personal data"[101] and the processing by non-automatic means would only be within the scope of the Directive 95/46/EC where the data form part of a filing system.[102]

---

[97] *Ibid*. at 12, para. 2.13: "All automated systems involve some manual data handling, for there are always clerical processes and human consideration of the data before and after the automatic handling." See also *ibid*. at 18, para. 3.20: "Because it is becoming increasingly difficult to draw a clear distinction between computer and manual systems, it seems likely that, within the foreseeable future, there will be few – in any – significant personal data handling systems that will not be making some use, if only indirectly, of computer technology."

[98] See *Report of the Committee on Privacy*, *supra* note 3 at 186, para. 605: "In Mr Baker's Bill 'data banks' were defined as 'computers which record and store information'; in Mr Huckfield's Bill 'any store of information containing details of individuals' would be a 'data bank' and so liable to come within the Bill's terms. Mr Huckfield's Bill would therefore cover both computerised and non-computerised data banks as his proposals are designed to apply controls to the whole problem of information stores and thus go further in their purpose than legislation to control computerised information only, which is the subject we are examining here."

[99] EC, *Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, [1995] O.J., L. 281/31 [EC, *Directive 95/46/EC*].

[100] Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*, [2007] 01248/07/EN WP 136 at 5 [Article 29 Data Protection Working Party, *Opinion 4/2007*]: "It is useful to recall that the reasons for enacting the first data protection laws in the seventies stemmed from the fact that new technology in the form of electronic data processing allows easier and more widespread access to personal data than the traditional forms of data handling."

[101] See EC, *Directive 95/46/EC*, *supra* note 99 at recital 27.

[102] Or if the data is intended to be part of such system. See *ibid*. at art. 3.

1.1.2.2. Still about Control: Canadian and French Data Protection Laws

France introduced its DPL, a legislation relating to personal data and computer files, as far back as the late 1970s, with law Nr. 79-17 of 6 January 1978.[103] In Canada, the Privacy Act of 1980[104] marked Canada's first attempt to legislate in the area of data protection; however, it only covered the public sector. With the rapid advances in information technology and the pressure to conform to European standards to facilitate cross-continental trade, new legislation was soon required.

At the end of the 1980s, it became clear in Europe that Convention 108 could not be used as a harmonizing tool across European states adopting DPLs as the ones which had adopted such laws had substantial differences which created problems in the European internal market.[105] This has led to the adoption, at the European level, of Directive 95/46/EC which had two objectives: protecting the fundamental rights and freedoms of natural persons, in particular their right to privacy with respect to the processing of personal data, and facilitating the free flow of personal data between Member States.[106]

In North America, the conception of "privacy as control over personal information" has been adopted by Canadian courts[107] as well as U.S. ones.[108]

In Canada, this concept has also been adopted by the Office of the Privacy Commissioner of Canada ("OPCC")[109] and incorporated in DPLs. Quebec was the first

---

[103] Despite this early start in introducing a DPL in France, it took years for Directive 95/46/EC to be introduced. In the meantime, the protection of privacy was covered in a piecemeal fashion, by the Law of 12 April 2000 on the Rights of Citizens and their Relationship with Administration, and the Law of 4 March 2002 on Patients' Rights. Directive 95/46/EC was finally incorporated into the French DPL with Law Nr. 2004-801 of 6 August 2004 relating to the Protection of Data Subjects as Regards the Processing of Personal Data. This law amended the 1978 French DPL, and the bulk of it came into force immediately.

[104] C. 1980, c. P-21.

[105] Colin J. Bennett & Charles D. Raab, *The Governance of privacy* (Cambridge: MIT Press, 2006) at 93.

[106] See EC, *Directive 95/46/EC*, *supra* note 99 at Preamble.

[107] The conception of privacy as "control over personal information" has been adopted by the Supreme Court of Canada on several occasions, for instance in *R. v. Tessling*, [2004] 3 S.C.R. 432, 2004 SCC 67*,* at para. 23 [*Tessling*, cited to S.C.R.]; in *R. v. Edwards*, [1996] 1 S.C.R. 128*,* at para. 61; and in *R. v. Dyment*, [1988] 2 S.C.R. 417*,* at paras. 17, 20 [*Dyment*].

[108] The U.S. Supreme Court has also echoed this conception by stating that privacy "encompass[es] the individual's control of information concerning his or her person". See *United States v. Reporters' Comm. for Freedom of the Press*, 489 U.S. 749 at 763 (1989).

[109] In Canada, the OPCC has also confirmed that *privacy* is about "control". See Privacy Commissioner of Canada, "Speech at the Freedom of Information and Protection of Privacy conference" (2002) cited online:

province to adopt *An Act respecting the protection of personal information in the private sector*[110] in 1993 (the "Quebec DPL"). At the federal level, the *Personal Information Protection and Electronic Documents Act* ("PIPEDA") was introduced in 2000 and came into force in the private sector in 2004.[111] The threat of loss of trade as a result of Directive 95/46/EC and its adequate protection requirements was a strong motivating factor for the Canadian Government's decision to enact PIPEDA.[112] Therefore, the notion of privacy as "individuals in control over their personal information" was not reopened nor re-examined in order to ensure that, at the time of the adoption of PIPEDA, it was the most efficient way to protect individuals against the risks resulting from the collection, use or disclosure of their information.

In Canada, the federal government may exempt organizations or activities in Canadian provinces that have their own DPLs if they are substantially similar to PIPEDA.[113] The provinces of British Columbia, Alberta and Quebec have enacted provincial DPLs that have been recognized as substantially similar to PIPEDA: as mentioned earlier, Quebec has had its DPL since 1993 and Alberta and British Columbia introduced their *Personal Information Protection Acts* in 2003 (hereinafter, the "Alberta DPL"[114] and the "B.C. DPL"[115]). Having read the Quebec parliamentary debates which led to the adoption of the Quebec DPL in 1993, it is interesting to once again note the concern in ensuring that Quebec would have a DPL which would be in line with the OECD

<http://www.tbs-sct.gc.ca/pgol-pged/piatp-pfefvp/course1/mod1/mod1-2-eng.asp> ("The right to privacy means that individuals get to decide what and how much information to give up, to whom it is given, and for what uses.")

[110] *An Act Respecting the Protection of Personal Information in the Private Sector*, R.S.Q. 1993, c. P-39.1 [Quebec DPL].

[111] PIPEDA, *supra* note 63 at s. 3.

[112] See Steve Coughlan et al., "Global reach, Local Grasp: Constructing extraterritorial jurisdiction in the Age of Globalization", (2007) 6 CJLT 29, at 33. In 2002, the European Commission decided that PIPEDA did provide adequate safeguards for certain personal data to flow freely from the EU to Canada, in line with Directive 95/46/EC. See EC, *Commission Decision 2002/2/EC of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act*, [2002] O.J., L. 002/0013.

[113] These DPLs operate in place of PIPEDA in those provinces for intra-provincial matters. However, PIPEDA continues to apply to the federally-regulated private sector in those provinces, and to personal information in inter-provincial and international transactions by all organizations engaged in commercial activities. In addition, some provinces have passed legislation to deal specifically with the collection, use and disclosure of personal information in specific areas, such as health care, and separate privacy laws or DPLs apply to the public sector (these will not be specifically addressed in this thesis).

[114] *Personal Information Protection Act* (Alberta), S.A. 2003, c. P-6.5 [Alberta DPL].

[115] *Personal Information Protection Act* (British Columbia), S.B.C. 2003, c. 63 [B.C. DPL].

Guidelines.[116] Whether the FIPs were the proper or most efficient instruments to protect individuals was not on anyone's agenda and discussions regarding this issue never took place. In light of this, it is reasonable to maintain that the notion of privacy as "individuals in control over their personal information" was not re-evaluated in order to ensure that at the time of its adoption, the incorporation of the FIPs into the Quebec DPL was the way to move forward in order to protect individuals against harmful data handling activities by private sector entities.

Given that the standard provided through the FIPs has been adopted on a wide scale,[117] that different versions of the FIPs can be found in most if not all DPLs, transnational or international policy instruments up until today, that many authors still today value this FIPs standard and the concept of privacy as "control over personal information", and that individuals surveyed about their online privacy still refer to the notion of privacy as "control",[118] it is therefore reasonable to say that we are still, today,

---

[116] Various references are made on the fact that Quebec is "behind" on the data protection front since it has not yet adopted a DPL in line with the OECD Guidelines although Canada is a member of the OECD. These debates also elaborate on the fact that Quebec needs to adopt a DPL in order to have a law in line with data protection efforts made at the international level, especially with efforts made in Europe. See *Les travaux parlementaires*, 34th législature, 2nd session, Commission permanente de la culture, cahier no 11 (February 23, 1993), at 2, 5, 12, 27, 57, 58, 66; *Les travaux parlementaires*, 34th législature, 2nd session, Commission permanente de la culture, cahier no 12 (February 24, 1993), at 38, 41, 49; *Les travaux parlementaires*, 34th législature, 2nd session, Commission permanente de la culture, cahier no 13 (March 1, 1993), at 2, 6 and 8; *Les travaux parlementaires*, 34th législature, 2nd session, Commission permanente de la culture, cahier no 14 (March 2, 1993), at 6, 25, 36, 38, 40, 43 and 65; *Les travaux parlementaires*, 34th législature, 2nd session, Commission permanente de la culture, cahier no 16 (March 4, 1993), at 35, 55; *Les travaux parlementaires*, 34th législature, 2nd session, Assemblée, cahier no 73 (March 16, 1993), at 2, 3, 9, 23, 27; *Les travaux parlementaires*, 34th législature, 2nd session, Assemblée, Motion, cahier no 73 (March 16, 1993), at 1 and 2; *Les travaux parlementaires*, 34th législature, 2nd session, Commission permanente de la culture, cahier no 23 (May 13, 1993), at 9, 11, 14; *Les travaux parlementaires*, 34th législature, 2nd session, Assemblée, cahier no 112 (June 14, 1993), at 2; *Les travaux parlementaires*, 34th législature, 2nd session, Commission permanente de la culture, cahier no 32 (June 8, 1993), at 4, 12.

[117] Aside from Canada and the European countries which have adopted DPLs in line with Directive 95/46/EC, the FIPs have also been incoporated in DPLs in other countries including in various U.S. sector specific DPLs such as the Children's Online Privacy Protection Act ("COPPA") and the "Safe Harbor" framework adopted in the U.S. in order to ensure that this level of protection is achieved regarding the transfer to personal data from the European Union to the United States. See online: <http://export.gov/safeharbor/> for details on the safe harbor agreement.

[118] See Jayne S. Ressler, "Privacy, Plaintiffs, and Pseudonyms: The Anonymous Doe Plaintiff in the Information Age" (2004) 53 U. Kan. L. Rev. 195 at 5, online: SSRN <http://ssrn.com/abstract=542782>, referring to Humphrey Taylor, "Most People Are 'Privacy Pragmatists' Who, While Concerned About Privacy, Will Sometimes Trade It Off For Other Benefits" (2003) 17 The Harris Poll, online: <http://www.harrisinteractive.com/vault/Harris-Interactive-Poll-Research-Most-People-Are-Privacy-Pragmatists-Who-While-Conc-2003-03.pdf> (article by Humphrey Taylor reporting the results of a February 2003 Harris poll telephone survey of 1,010 adults on the public's concern of an erosion of privacy): "Indeed, recent surveys show that Americans feel that the government has too much access to personal information. More than three-quarters of survey participants stated that they believe that it is

under the third wave. As a matter of fact, the term "privacy laws" are usually meant to refer to DPLs.

1.1.3. Definition of Personal Information: Origin and Background

At the time that the definition of *personal information* was initially being established in the 1970s, although some attempted various distinctions (between "sensitive" and "non-sensitive" information, between "private" and "public" information, etc.),[119] there was, in the end, a consensus on the fact that the only feasible definition of *personal information* for the purposes of DPLs was *any information which relates to any data subject who is, or can be, identified.*[120] Most European jurisdictions were in fact already using this definition (or similar ones) in the late 1970s.[121]

At the European Council level, the FIPs were to protect all "personal information". As a matter of fact, in the Resolutions (73) 22 and (74) 29, the principles of FIPs applied to personal information stored in electronic data banks in the private and public sectors. For the purposes of these resolutions, the term *personal information* was defined as: "information relating to individuals (physical persons)".[122] Many jurisdictions adopted or proposed similar definitions during the early 1970s, although some also included the notion that the information had to be linked or be able to "identify" a particular individual

---

important both to be in control of who can get personal information and to trust those with whom they share confidential information."

[119] Lindop, *supra* note 96 at 153, para. 18.24: "Paragraph 37 of the White Paper invites us to say 'how personal information should be defined', and that was therefore one of the questions on which we asked our witnesses to submit their views. We were offered a wide variety of opinions. Some attempted an exhaustive list. Others, perhaps predictably, sought to exclude from the definition the kinds of information which they themselves were most concerned to handle. Some attempted a distinction between 'sensitive' and 'non-sensitive' information, and others between 'private' and 'public' information. Many however, recommended that the definition should include all information which related to anybody, provided the person concerned was (or could be) identified."

[120] See below in the present section, which elaborates on the definition of *personal information* adopted in Canadian and European DPLs. See also Lindop, *supra* note 96 at 154, para. 18.27: "Accordingly, we have come to the conclusion that the only feasible definition of 'personal information' for this purpose is any information which relates to any data subject who is, or can be, identified – including the information whereby he can be identified, as for example his name, address, date of birth, or telephone number (although this definition will have to be extended before it is ready for inclusion in the statute – see paragraph 18.42)."

[121] *Ibid*. at 154, para. 18.27: "Here again, we are reinforced in our conclusion by the fact that the foreign statutes all adopt similar definitions. The US privacy Act, for example, uses 'any information about an individual that contains his name…or identifying particulars', the Swedish Acts speaks of 'information concerning an individual' and the Norwegian Bill defines it as 'information and assessments which are directly or indirectly traceable to identifiable individuals, associations or foundations'. France, Austria, Denmark and West Germany all use similar terms in their proposed or enacted legislation."

[122] See Council of Europe, *Explanatory Report: Resolution (73) 22*, *supra* note 56 at para. 12.

in order to qualify as *personal*.[123] This notion of "identifiability" was also eventually incorporated in Convention 108[124] and included in the definition in other transnational instruments thereafter. For the last thirty or forty years, the same definition of *personal information* or very similar ones have been used repetitively in other transnational policy instruments such as the OECD Guidelines[125] and the APEC Privacy Framework.[126]

Identical or similar definitions are also at the core of DPLs, which can be found around the world.[127] In Canada, PIPEDA defines *personal information* as *information about an identifiable individual*.[128] Alberta and British Columbia DPLs have the same or at least very similar definitions.[129] In Quebec, the DPL defines it as *any information which relates to a natural person and allows that person to be identified.*[130] In France, the

[123] See for example, *Report of the Committee on Privacy*, *supra* note 3 at 183, para. 591: "In this context information means information relating to any particular individual and linked or capable of being linked to his identity (…)."; See also Lindop, *supra* note 96 at 153, para. 18.24: "Many however, recommended that the definition should include all information which related to anybody, provided the person concerned was (or could be) identified."; U.S. Department of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *supra* note 57 at s. IV "Recommended Safeguards for Administrative Personal Data Systems" states: "We define an *automated personal data system* as a collection of records containing personal data that can be associated with identifiable individuals, and that are stored, in whole or in part, in computer-accessible files. Data can be 'associated with identifiable individuals' by means of some specific identification, such as name or Social Security number, or because they include personal characteristics that make it possible to identify an individual with reasonable certainty."

[124] See Convention 108, *supra* note 10 at art. 2 (a): "*personal data* means any information relating to an identified or identifiable individual".

[125] See OECD, *Guidelines*, *supra* note 11 at art. 1 b): "*personal data* means any information relating to an identified or identifiable individual".

[126] APEC, *Privacy framework*, *supra* note 363 at art. 9 states: "Personal information means any information about an identified or identifiable individual."

[127] Many European countries have adopted a definition of *personal information* which is identical to the one from the Directive 95/46/EC.

[128] But is excluded from the definition the name, title or business address or telephone number of an employee of an organization. See PIPEDA, *supra* note 63 at art. 2 (1).

[129] Alberta defines "personal information" as information about an identifiable individual. Alberta DPL, *supra* note 114 at s. 1(1) (k); The BC DPL uses the same definition but with certain exclusion for contact information or work product information. It defines personal information as "information about an identifiable individual and includes employee personal information but does not include (a) contact information, or (b) work product information". "contact information" means "information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual". B.C. DPL, *supra* note 115 at Part 1, s. 1.

[130] Quebec DPL, *supra* note 110 at s. 2.

definition is very similar[131] and follows the definition of "personal data" provided by the Directive 95/46/EC which is *any information relating to an identified or identifiable natural person*.[132] Thus, the definition has remained largely unchanged since it was initially articulated in the early 1970s. As a point of clarification, while European jurisdictions usually refer to "personal data"[133] and North American jurisdictions such as Canada to "personal information",[134] throughout this analysis, the term of reference will be "personal information" and the words "information" or "data" (or "personal information" and "personal data") may be used interchangeably.

Some jurisdictions are adopting similar definitions of *personal information* - without reconsidering the kind of data that should be protected by DPLs - simply in order to ensure consistency across borders. For example, the OPCC has recently concluded that *work product* should not be omitted from the definition of *personal information* in PIPEDA since the current definition is based on known Canadian and International precedent and consensus (and the introduction of a *work product* exemption would mean that Canada would be taking a position different from that taken in other jurisdictions, particularly those in Europe).[135]

---

[131] *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, J.O., 7 January 1978, c. 1, art. 2 [*Loi informatique et liberté*]: "Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres."

[132] EC, *Directive 95/46/EC*, *supra* note 99 at art. 2(a): "An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."

[133] See Lindop, *supra* note 96 at 154, para. 18.28: "The computing community make much use of the word 'data' (the Latin word 'datum', of which 'data' is the plural, literally means 'that which is given'), using it to mean raw material which is put into data processing systems. (…) "we think that, for statutory purposes, the word 'data' rather than 'information' should be used". More recently, we can refer to the European Direction 1995 which still refers to the term 'data'."

[134] Although in the U.S., sectoral DPLs usually refer to "personally identifiable information" ("PII") instead of *personal information* or *personal data*. As a matter of fact, U.S. laws protecting personal information often refer to "PII" which stands for "personally identifiable information*"*. See for example COPPA and *California Online Privacy Protection Act*, Bus & Prof. Code §§ 22575-22579 (2004).

[135] See OPCC, "The Privacy Commissioner of Canada's Position at the Conclusion of the Hearings on the Statutory Review of PIPEDA", Appendix III, "Work Product" Information, online: <http://www.priv.gc.ca/parl/2007/sub_070222_03_e.cfm>. While the OPCC admitted that it had not investigated whether a change in PIPEDA's definition of personal information would affect the perception that PIPEDA was sufficiently harmonized with European law, it noted that during a recent review of the Directive 95/46/EC, the European Commission was asked to add a "work product" exemption to the Directive 95/46/EC's definition of *personal information* and that in general, the European Commission advised against modifying the Directive 95/46/EC. See IMS Health, "European Commission Review of the

***

The Internet is a global electronic communications medium comprised of innumerable computer networks, which communicate by using a common language and set of data transfer protocols.[136] The concept of a computer network, with a series of small computers storing data, connected with one another and with a central computer, was foreseen as early as the beginning of the 1970s.[137] Nevertheless, taking into account the various changes that were brought on by the Internet, I maintain that it is reasonable to doubt that the principles of FIPs were drafted with the modern Internet reality in mind. These main changes and recent technological developments are further discussed next.

1.2. Technological Background Affecting Personal Information

Changes triggered by Internet and related technologies have taken place since privacy was conceptualized as individuals having "control over their personal information" during the third wave of the late 1960s and early 1970s.[138] Among the most important changes are: an increase in the volume of data in circulation or storage, the emergence of new collection tools, new types of data, as well as new data-mining techniques or tools which allow to easily link individuals to information. This new phenomenon has resulted in the development of new business models, in an increased availability of personal information, or of an increase in knowledge about individuals.

EU Data Protection Directive (Directive 95/46/EC): Submission by IMS Health" (July 2002), online: <http://ec.europa.eu/>.

[136] Gavin Skok, "Establishing a Legitimate Expectation of Privacy in Clickstream Data" (2000) 6 Mich. Telecomm. Tech. L. Rev. 61. See also Stephan K. Bayens, "The Search and Seizure of Computers: Are We Sacrificing Personal Privacy for the Advancement of Technology?" (2000) 48 Drake L. Rev. 239 at 248-49: "The Internet is not a physical or tangible entity, but rather a giant network which interconnects innumerable smaller groups of linked computer networks. The Internet is an overwhelming mass of information that has no centralized administrator, storage location, or control point. It exists and functions as a result of the fact that hundreds of thousands of separate operators of computers and computer networks independently decided to use common data transfer protocols to exchange communications and information with other computers (which in turn exchange communications and information with still other computers)."

[137] Council of Europe, *Report on data processing*, *supra* note 66 at 5, s. II, s. 3: "The present technical trend is towards the spread of small computers storing small quantities of data, but which may be connected with each other and with a central computer, thus forming a network in which all sorts of information circulate. From this point of view, control is necessary not only over the information stored, but also over its use and the means by which it is obtained, i.e. data processing control."

[138] See section 1.1.2 entitled "Control over Personal Information and Fair Information Practices" which elaborates on this issue.

1.2.1. Increase in Volume of Information

There has been a major increase in the volume of data available and of data exchanges, mainly due to the enhanced storage capabilities of computers as well as heightened connectivity to the Internet, be it through computers or other devices. In addition, the new generation of the Internet, also known as the web 2.0, has triggered new ways of using the Internet (Internet users are increasingly encouraged to disclose and share their personal information online).[139] The greater volume of data available may also allow for an easier identification of individuals.

1.2.1.1. Increase in Storage Capabilities, Number of Users and Exchanges

In the early 1970s, when the principles of FIPs were articulated,[140] the main concerns resulting from electronic data processing were the great volume of data, the techniques for their storage and retrieval, their transmission over large distances, the speed with which all these operations could be performed together with the high storage capabilities of computers.[141]

Nowadays, there are larger volumes of cross-border data flows taking place at higher speeds, reaching broader geographical areas, transferring alpha-numeric data, audio, video and other types of data between an ever greater number of actors.[142] Peter

---

[139] See section 1.2.1.2 entitled "New Ways of Using the Internet: Web 2.0*"* which elaborates on this issue. See also EC, *Directive 95/46/EC*, *supra* note 99 at Whereas (4): "Whereas increasingly frequent recourse is being had in the Community to the processing of personal data in the various spheres of economic and social activity; whereas the progress made in information technology is making the processing and exchange of such data considerably easier".

[140] See section 1.1.2 entitled "Control over Personal Information and Fair Information Practices*"* which elaborates on this issue.

[141] See Council of Europe, *Explanatory Report: Resolution (73) 22*, *supra* note 56 at para. 3: "What is setting computers apart from the traditional means of data storage and processing is the extraordinary ease with which they have overcome at a stroke a whole series of problems raised by the management of information: the great volume of data, the techniques for their storage and retrieval, their transmission over large distances, their correct interpretation and, finally, the speed with which all these operations can be performed." See also *ibid*. at para. 21: "A rule concerning the volume of the information is necessary in view of the capacity of electronic data banks to absorb an almost unlimited quantity of information, to preserve it indefinitely, to hand it out instantly and to link scattered information."

[142] OECD, *Report on the Cross-Border Enforcement of Privacy Laws* (Paris: OCDE, 2006) at 8, online: <http://www.oecd.org/dataoecd/17/43/37558845.pdf>.

Fleisher, CPO of Google, qualifies the current information age as an "information deluge".[143]

The storage capabilities of computers have increased exponentially ever since the advent of the computer age.[144] So much so that it is difficult to imagine that this deluge of information in the 21st century could have been predicted in the early 1970s, a time when the storage capacity of computers was comparatively quite modest. The central processor unit in a computer doubles in speed every 18 months resulting in an exponential growth in computing power.[145] Over the last ten years, we have gone through about seven generations of computers, which in turn means that the power of the central processing unit has increased by a factor of more than one hundred.[146]

Personal computers appeared in the early 1980s.[147] Cell phones made their entry in the 1980s,[148] the BlackBerry in the late 1990s[149] and the iPhone not before 2007.[150] The prevalence of these personal mobile devices and laptop computers which can also

---

[143] Peter Fleischer, "The data deluge" *Peter Fleischer: Privacy…?* (21 April 2010), online: <http://peterfleischer.blogspot.com/2010/04/data-deluge.html?spref=tw> [Fleischer, "The data deluge"]: "But whether you like it or not, we're entering an age of data ubiquity. Clearly, technology trends are making this possible, computing power, storage capacity, Internet transmissions have all allowed this to happen. And like all trends in technology, it will have good and bad applications: the same ease of transmission of data that enables billions of people to access information from around the globe makes it easy to transmit malicious viruses as well. Statistics about the scale of the data deluge are indeed sobering, even if they reflect scales that human brains can't really understand."

[144] It has been reported that over the past decade, memory size has in some cases increased by a factor of 100 or more, which allows not only for faster computation but also for the ability to work on vastly larger data sets than was possible before. See, Waldo, Lin & Millet, *supra* note 6 at 91-93. Also, Some studies show that storage capacity has increased at a rate that has outpaced the rate of increase in computer power, in average doubling every 12 months. See: E. Grochowski and R.D. Halern, "Technological Impact of magnetic Hard Disk Drives on Storage Systems" (2003) 42:2 IBM Systems Journal 338.

[145] See Waldo, Lin & Millet, *supra* note 6 at 90.

[146] *Ibid*.

[147] The first PC from IBM was released in 1981 and the first laptop, the Osborne 1, a portable computer that weighed 24 pounds and cost US$1795, was produced and released by Osborne Computer in 1981. See online: <http://oldcomputers.net/osborne.html>.

[148] The commercial take-off of the analog cellular phone took place in the mid-1980s (see Center for Science, Technology, and Economic Development (CSTED), *The Role of NSF's Support of Engineering in Enabling Technological Innovation. Phase II, Chapter 4: The Cellular Telephone*, online: <http://www.sri.com/policy/csted/reports/sandt/techin2/chp4.html>).

[149] Blackberry devices have been around since 1999. See "The history of the Blackberry" (15 April 2008), online: BBGeeks <http://www.bbgeeks.com/blackberry-guides/the-history-of-the-blackberry-88296/>.

[150] The iPhone was released on July 30th 2010 in Canada: <http://www.iphoneincanada.ca/iphone-news/official-iphone-4-release-date-in-canada-on-july-30/> and on November 29 2007 in France. See Jacqui Cheng, "Apple announces iPhone launch in France: November 29", online: ars technica <http://arstechnica.com/apple/2007/10/apple-announces-iphone-launch-in-france-november-29/>.

be used as media players, games consoles, location aware devices and interfaces to payment systems or to store vast quantities of personal data[151] surely could not have been predicted even a few decades ago. There are over 25.5 million users of mobile devices in Canada[152] and 59.5 million in France.[153] One method of communication between mobile devices is through text messages. In England alone, some 60 billion text messages were sent in just one year (2009).[154]

The modern web has been around since the early 1990s and became widely available to individuals mostly around the mid 1990s.[155] The volume of *personal information* collected, disclosed and used by organizations has subsequently increased. Once online, individuals frequently disclose personal information as they register and buy products, browse web pages, post comments online, etc. Various online business models are focused on collecting, using or disclosing this data.[156] Individuals also use the Internet to communicate: by 2010, the world was already transmitting 2.8 million emails a second.[157] There are over one trillion web pages now, growing by billions per

---

[151] EC, Peter Hustinx, *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on the follow up of the Work Programme for better implementation of the Data Protection Directive*, [2007] O.J., C. 255/1 at 2; Neil Robinson et al., *Review of the European Data Protection Directive* (Santa Monica, CA: RAND Corporation, 2009) at 17.

[152] The number of wireless telephone subscribers in Canada topped 25.5 million at the end of September 2011 according to numbers compiled by industry trade group, the Canadian Wireless Telecommunications Association (CWTA). See Hugh Thompson, "Latest numbers show Canada has over 25.5 million wireless customers" (16 January 2012), online: digitalhome.ca <http://www.digitalhome.ca/2012/01/latest-numbers-show-canada-has-over-25-5-million-wireless-customers/>.

[153] France had 59.543 million subscribers in total as of December 2009. See online: <http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/CellularSubscribersPublic&ReportFormat=HTML4.0&RP_intYear=2009&RP_intLanguageID=1&RP_bitLiveData=False>.

[154] William Maclean, "Is the Big Brother watching you??" *Balkan news* (28 June 2010), online: Balkans.com <http://www.balkans.com/open-news.php?uniquenumber=62265>.

[155] Devin Brown, "Happy 20th birthday, World Wide Web!" *Cnet news* (6 August 2011), online: cnet.com, <http://news.cnet.com/8301-10797_3-20089085-235/happy-20th-birthday-world-wide-web/>: "On August 6, 1991--20 years ago--Tim Berners-Lee posted a summary of a project for organizing information on a computer network using a 'web' of hyperlinks: the 'WorldWideWeb,' or W3. At the same time, the W3 made its debut as a publicly available service on the Internet." The Internet is decades old but the web is 20 years old.

[156] See section 1.2.4.1 entitled "New Business Models (Customization and Sponsored Services)" which elaborates on this issue.

[157] Maclean, *supra* note 154.

day.[158] The Economist recently reported that the total amount of data in the world is growing by 60% per year.[159]

In the early 1970s, at the time that a first draft of the principles of FIPs was circulated at the Council of Europe level, neither the number of devices available nor their potential role in collecting and sharing personal information was given any consideration. At the time, computers were only used by public and private sector organizations, for data storage and processing which were no different from those served by more traditional forms of data storage and processing.[160] Basically, the only tasks that were foreseen were administrative tasks from these organizations such as the facilitation of the storage and the handling of the data.[161] Policymakers directed their attention strictly on the growing number of organizations from the private and the public sector, which would eventually be using computers and databases. Never could they have predicted that billions of individuals located worldwide would also be using computers and other similar devices to connect to one all-encompassing network known as the Internet.[162]

1.2.1.2. New Ways of Using the Internet: Web 2.0

One of the most important social changes of the 21st century has been ushered in by a recent shift in computing platforms. With the advent of web 2.0, which is fundamentally about what individuals use computers to do, the way individuals manage their personal information has undergone a significant transformation. Randal Picker raises that:

> "We have moved from creating documents in Microsoft Office to living life online: searching on Google, buying and selling on eBay, hanging out with our friends on MySpace and Facebook, watching the newest viral video on YouTube".[163]

---

[158] Fleischer, "The data deluge", *supra* note 143.

[159] *Ibid*.

[160] See Council of Europe, *Explanatory Report: Resolution (73) 22*, *supra* note 56 at para. 3: "The purposes which computers are increasingly serving in the public and private sectors are by themselves not basically different from those served by more traditional forms of data storage and processing."

[161] Council of Europe, *Explanatory Report: Resolution (74) 29*, *supra* note 65 at paras. 1-2;

[162] Internet Governance Forum, *Internet Fact Sheet: The basics of worldwide Internet usage* (November 2007), online: <http://www.intgovforum.org/mediaup/IGF%20BN%20Internet%20Fact%20Sheet.pdf>: "September 2007, it was estimated that 1.2 billion, or more than one sixth of the world's population were using the Internet."

[163] Picker, *supra* note 21 at 3.

The second generation of the Internet, with the proliferation of OSNs, blogging, podcasting and life-casting, has become a virtual agora for the sharing of information and ideas of all kinds.[164] Individuals now actually use and manage the personal data of *others*. This veritable revolution in online social interaction has given rise to large amounts of personal data stored on mobile phones, PDAs, similar devices and OSNs.

The recent trend in the voluntary sharing of personal information online may therefore translate into an increase of the availability of information as visitors and users to these websites and participants in these chat groups, blogs or in OSNs will generate considerable traces of their information. Moreover, the number of online users sharing information is constantly increasing. In December 2009, more than 350 million people around the world were using Facebook to share their lives online.[165] In February 2010, this number reached 400 million users[166] and in July 2011, 500 million active users.[167] There are over 40 billion photos on Facebook alone,[168] more than 3 billion pictures on the site Flickr.com[169] and YouTube users were reported to upload over 24 hours of video every minute.[170] Individuals share their personal information online voluntarily, they may publish their travel schedule on Dopplr[171] or disclose their recent credit card

---

[164] Pierre Trudel, "Privacy Protection on the Internet: Risk Management and Networked Normativity" in Serge Gutwirth et al., eds., *Reinventing Data Protection?* (Dordrecht, London: Springer, 2009) 317 at 326-27 [Trudel, "Privacy Protection"]: "The Internet is not uniform: it contains spaces of many different kinds. Some are more risky than others for the privacy of people who visit them. For example, social networking web sites make it possible for people to meet and connect through social networks. Sites such as *MySpace* (http://www.myspace.com) and *LinkedIn* (http://www.linkedin.com/) offer online services that allow people to get together. Such sites can be used to make friends, create professional relationships, publicize music groups, meet people who share the same interests, find old classmates, etc. (…) since users can decide to display certain pieces of personal information, we have to postulate that on the Internet there is information belonging to collective life in addition to that belonging to private life." See also European Parliament, Committee on Civil Liberties, Justice and Home Affairs, "Public Seminar Data protection on the Internet (Google-DoubleClick and other case studies)", Monday 21 January 2008, Brussels, Room PHS 3C50 at 2 [European Parliament, *Seminar Data protection*].

[165] Mark Zuckerberg, "An Open Letter from Facebook Founder Mark Zuckerberg" *Le blogue Facebook* (1st December 2009), online: Facebook <http://blog.facebook.com/blog.php?post=190423927130>.

[166] Erick Schonfeld, "Privacy-Per-Post: Facebook Rolls Out Its New Privacy Settings" (9 December 2009), online: Tech Crunch <http://techcrunch.com/2009/12/09/facebook-privacy-per-post/>.

[167] Paul Sawers, "Could Facebook reach one billion users in 2011?" (10 July 2011), online: thenextweb <http://thenextweb.com/socialmedia/2011/01/20/could-facebook-reach-one-billion-users-in-2011/>.

[168] Fleischer, "The data deluge", *supra* note 143.

[169] See online post dated February 4th, 2009: <http://code.flickr.com/blog/2009/02/04/100000000-geotagged-photos-plus/>.

[170] Fleischer, "The data deluge", *supra* note 143.

[171] *Dopplr* is a service for sharing personal and business travel plans privately with the people you trust. See online: <http://www.dopplr.com/>.

purchases on Blippy.[172] Their taste in movies, music and books may be available on Netflix,[173] iTunes[174] and Amazon.com.[175] Their DNA profile may even be available on 23andMe.[176]

1.2.1.3. Easier Identification of Individuals

The volume of available personal information may trigger a situation in which an individual is more easily identifiable. For instance, it has been shown that, in certain instances, it is possible to use the content of search queries to identify a specific person. On August 4, 2006, AOL Research published a compressed text file on one of its websites containing twenty million search keywords which had been punched into AOL's search engine for over 650,000 anonymous AOL users over a 3-month period, intended for research purposes.[177] According to reports in the press, it was possible to identify individual users on the basis of the content of their various combined search queries.[178]

A similar privacy concern exists in the mobile space. Some time ago, several U.S. companies such as Intelligent Transportation Society of America[179] had requested the Federal Communication Commission ("FCC") to allow them to anonymously track the

---

[172] *Blippy* is a website where people may write reviews about their purchases. See online: <http://blippy.com/>.

[173] Netflix, Inc. [Nasdaq: NFLX] is the world's leading Internet subscription service for enjoying movies and TV shows. See online: <http://www.netflix.com/>.

[174] iTunes is a free application for your Mac or PC that lets people organize and play digital music and video on their computer and allow automatic download of new music, app, and book purchases across all devices and computers. See online: <http://www.apple.com/itunes/>.

[175] See online: <http://www.amazon.com/>.

[176] See online: <https://www.23andme.com/howitworks/>.

[177] See the resolution approved by various privacy commissioners at the 2006 International Data Protection and Privacy Commissioners' Conference: *Resolution on Privacy Protection and Search Engines*, 28th International Data Protection and Privacy Commissioners' Conference, London, UK, 2 and 3 November 2006 [*Resolution on Privacy Protection*].

[178] While none of the records on the file were personally identifiable *per se*, certain keywords contain personally identifiable information by means of the user typing in their own name (ego-searching), as well as their address, social security number or by other means. The New York Times was able to locate individuals from the released and anonymized search records by cross referencing them with phonebooks or other public records. This list, although quickly withdrawn by AOL recognising that it was an error, had by the time of the withdrawal reportedly been downloaded and re-posted many times, and made available in searchable form on a number of websites. Nate Anderson, "AOL releases search data on 500,000 users (updated)" (7 August 2006), online: ARS technica <http://arstechnica.com/uncategorized/2006/08/7433/>.

[179] Public/private partnership serving as a utilized Federal Advisory Committee to the U.S. Department of Transportation, Educational and scientific research organization created in 1991 for the purpose of fostering the development and deployment of intelligent transportation systems.

location of mobile users over time without having to disclose this tracking to the users themselves.[180] The claim being made was that the potential value of anonymous location data was significant, particularly to promote optimal traffic flows, to efficiently allocate transportation resources and to properly reroute traffic in emergency situations. Location data collected may be anonymized in the sense that the phone or unique number relating to a specific mobile device may have been removed and instead replaced by a profile number (for example profile ABC). However, if the location data collected is very accurate and collected over a long period of time, then it may be possible to determine the identity of "profile ABC"; for instance someone who spends every night at a specific location (his residence?) and spends his days at another one (work place?).[181]

These examples illustrate how the volume of data available creates new challenges and concerns as it can allow the identification of individuals more easily. Although isolated pieces of personal data acquired during the course of online service activities may not qualify as *personal information*, the context of the information, especially in light of profiling practices, may bring the personal information within the scope of "sensitive data".[182] In this new Information Age, it could be argued that individuals generate too much information too often to be able to "keep the genie in the bottle".[183]

1.2.2. New Types of Information and Collection Tools

Apprehension towards electronic devices capable of surreptitiously collecting personal information is not new and was already mentioned during the third wave as illustrated by the following excerpt of a Report on Privacy dating back to 1972:

> "To some extent the new public concern on this subject is the direct result of new technological developments. Numerous sophisticated electronic devices have been invented and marketed, which greatly

---

[180] U.S., Federal Communications Commission, *In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles: Intelligent Transportation Society of America Reply Comments* (WT Docket No. 01-72) (Washington, D.C.: 24 April 2001) at 7 [FCC].

[181] This example is discussed in Gratton, "Personalization", *supra* note 16.

[182] See section 1.2.3 entitled "New Identifying Methods" which elaborates on this issue.

[183] A. Michael Froomkin, "The Death of Privacy?" (2000) 52 Stan. L. Rev. 1461 at 1469: "Once created or collected, data is (…) hard to eradicate; the data genie does not go willingly, if ever, back into the bottle."

> increase the possibilities of surreptitious supervision of people's private activities and of spying upon business rivals."[184]

However these concerns were not meant to be addressed by the principles of FIPs.[185] Instead, the primary targets were the increase in the number of computers and electronic databanks and the fear that people would lose control over their personal information were it to be handled electronically.[186] With the Internet and related technologies, these concerns of technical tools stealthily collecting personal information, both online and offline, are now back on the table. Organizations or third parties may often collect information online such as what the individual is looking for, the details of his or her purchases, who his or her friends are and what they are interested in, using various types of online collection tools.

1.2.2.1. New Collection Tools

Various online tracking tools such as cookies,[187] web bugs[188] or spyware[189] can collect personal information including web browsing habits (or *clickstream* data), websites

---

[184] *Report of the Committee on Privacy*, *supra* note 3 at 6, para. 18.

[185] See section 3.1.1.2 entitled "Original Purpose Behind Regulating the Collection of Personal I" and more specifically section 3.1.1.2.2 entitled "Surveillance: Dataveillance not Specifically Addressed" which elaborate on this issue.

[186] See section 1.1.2.1 entitled "Initial Concern: Computers and Electronic Data Banks" which elaborates on this issue.

[187] Cookies are small pieces of code transferred from a website to a home computer when a user is surfing or visiting a website. They are then retransmitted back to the server each time the browser accesses a server's webpage. Rebecca Wong & Daniel B. Garrie, "Demystifying Clickstream Data: A European and U.S. Perspective" (2006) 20:2 Emory International I. Rev. 563, referring to: Rachel K. Zimmerman, "The Way the 'Cookies' Crumble: Internet Privacy and Data Protection in the Twenty-First Century" (2000-2001) 4 N.Y.U. J. Legis. & Publ. Pol'y 439 at 440.

[188] Also called "web beacons," "gif bugs," "clear GIFs" or "pixel tags," web bugs are small graphics (usually a single pixel or a transparent image such that it is invisible to the user) that are embedded in a web page's or e-mail HTML code to enable monitoring of who is reading the page or e-mail. There are two types of web bugs. One type is an executable web bug, which is a file that monitors a machine's traffic and hard drive and periodically sends the information back to the website that planted the bug on the machine. The second type is not physically located on the machine and uses scripts (i.e. JavaScript, ActiveX and Perl) to scan a hard drive searching for files. Janet Lo, *A "Do Not Track List" for Canada?* (Ottawa: Public Interest Advocacy Centre, 2009) at 47, online: <www.piac.ca/files/dntl_final_website.pdf>.

[189] Spyware is software that is usually downloaded into a computer when the user downloads free software from the Internet. It can gather information about the online user web-browsing habits or e-commerce data, and sends such data to a third-party company. Spyware is also being used by criminal law enforcement officials. FBI agents trying to track the source of e-mailed bomb threats against a Washington high school in the summer of 2007 sent to the owner of an anonymous MySpace profile suspected to having made those threats a secret surveillance spyware program. This led the FBI to a student at the school, who pleaded guilty to making these bomb threats. See: Kevin Poulsen, "FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats" (18 July 2007), online: WIRED <http://www.wired.com/print/politics/law/news/2007/07/fbi_spyware>. More specifically they used a

visited, purchases made, comments posted online, and searches made online. There are also new "points of collection" that may be collected and even sometimes included as *personal information*, and this may include data such as IP addresses. These new collection tools are reaching higher levels in terms of their tracking capabilities. For instance, certain ad networks are replacing or supplementing traditional tracking cookies with new enhanced tracking technologies. "Flash cookies" (local shared objects), represent the next generation of cookies; they cannot be deleted through the traditional privacy settings of a web browser and may be used to assign unique values to online users.[190] Flash cookies have also been used explicitly as a tool to restore "traditional cookies" that were refused or erased by an online user.[191]

In the mobile space, new tracking tools are also more widely available raising privacy concerns.[192] Mobile devices may disclose their location, and consequently their user's location, through various ways: network-based solutions, handset-based solutions (many phones are now using GPS locators) or some type of hybrid solution.[193] Location data can also be deduced, for example, from the IP address of the terminals and Wi-Fi access points.[194]

Other new types of technologies (online and offline) which may collect personal information are more and more widely distributed and available. For example, RFID

"Computer & Internet Protocol Address Verifier" (CIPAV) which installed on the suspect's machine remotely and was able to collect the suspect's current logged-in user name and the last visited URL, designed to surreptitiously monitor him and report back to a government server. See also Nate Anderson, "FBI uses spyware to bust bomb threat hoaxters" (18 July 2007), online: ARS Technica <http://arstechnica.com/security/2007/07/fbi-uses-virus-to-bust-bomb-threat-hoaxster/>. [Anderson, "FBI"].

[190] Lo, *supra* note 188 at 22: "We find that more than 50 per cent of the sites in our sample are using flash cookies to store information about the user. (…) Flash cookies are more effective at tracking users' visits around websites than traditional HTTP cookies because they operate in the shadows and are infrequently removed. As well, Flash cookies do not have a built-in expiry date. Third party advertising networks were the most common source of Flash cookies."

[191] Flash cookies are capable of storing information about the settings and circumvent the user's preferences. See Ashkan Soltani et al., "Flash Cookies and Privacy" (10 August 2009), online: SSRN <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862>, cited in Article 29 Data Protection Working Party, *Opinion 2/2010 on online behavioural advertising*, [2010] 00909/10/EN WP 171 at 6 [Article 29 Data Protection Working Party, *Opinion 2/2010*].

[192] For example, concerns have been raised with the iPhone collecting location data of iPhone users. See "Apple Q&A on Location Data" *Apple Press Info* (27 April 2011), online: Apple <http://www.apple.com/pr/library/2011/04/27location_qa.html> [Apple].

[193] See Eloïse Gratton, *Internet and Wireless Privacy: A Legal Guide to Global Business Practices* (Toronto: CCH Canada, 2003) at 29-32 [Gratton, *Internet and Wireless Privacy*].

[194] Article 29 Data Protection Working Party, *Opinion 2*/2010, *supra* note 191 at 7.

Radio Frequency Identification ("RFID") technology which consists of a system of tags and readers that can be used to identify and encode a variety of information is becoming more widely used.[195] RFID tags can be implanted in or attached to virtually any object (such as washing machines, sweaters) to livestock and even perhaps in human beings. These devices broadcast information to radio signal scanners and may be used to collect personal information;[196] for instance, to track the movements and habits of a particular customer within a given store.[197] A variety of other collection methods and techniques are being introduced such as the automated road toll systems like EZ Pass, Intelligent Vehicle Highway Systems, Closed Circuit Television ("CCTV") or video surveillance technology, face recognition systems, biometrics, thermal imaging, and more. These collection tools may be collecting various types of information, including news ones.

1.2.2.2. New Types of Information

At the time that the FIPs were adopted, the notion of personal information referred to *information about an identifiable individual*. For instance, the Lindop Report referred to "any information which relates to any data subject who is, or can be, identified", including the information whereby he can be identified, for example his name, address, date of birth, or telephone number.[198] In the 1973 U.S. Report on data protection, it was suggested that data can be "associated with identifiable individuals" by means of

---

[195] Stephanie Allen et al., *RFID Tagging: Final Report*, online: <http://www.rahulnair.net/files/RFID_Final_Report.pdf>.

[196] RFID technology may also be used to collect information that is directly or indirectly linked to personal information. See Article 29 Data Protection Working Party, *Working document on data protection issues related to RFID technology*, [2005] 10107/05/EN, WP 105 at 5-6 [Article 29 Data Protection Working Party, *RFID technology*]; See also Ann Cavoukian, *Tag You're It: Privacy Implications of Radio Frequency Identification (RFID) Technology* (Toronto: Information and Privacy Commissioner, 2004) at 15: "Corporations which compile the data transmitted by the tags could determine which products a consumer purchases, how often those products are used, and even where the product – and by extension the consumer – travels. By aggregating data to form consumer profiles, corporations could make inferential assumptions about a consumer's income, health, lifestyle, buying habits, and location. That information could be sold or exchanged with government agencies to create dossiers of individual citizens, or simply sold to other corporations for marketing purposes."

[197] For example, by installing a series of readers through a store, a business could garner information about how customers move through the store, which areas are most heavily browsed, and so on. See Teresa Scassa et al., *An Analysis of Legal and Technological Privacy Implications of Radio Frequency Identification Technologies*, Prepared for the Office of the Privacy Commissioner of Canada (28 April 2005) at 13, online: <http://www.library.dal.ca/law/Guides/FacultyPubs/Scassa/RFIDs_Report2(Single).pdf>, discused in George Hariton, John Lawford & Hasini Palihapitiya, *Radio Frequency Identifiation and Privacy: Shopping Into Surveillance* (Ottawa: Public Interest Advocacy Center, 2005) at 15.

[198] Lindop, *supra* note 96 at 154, para. 18.27.

some specific identification, such as name or Social Security number, or because they include personal characteristics that make it possible to identify an individual with reasonable certainty.[199]

With recent Internet technologies, new types of data have emerged and this data, instead of referring to an *identifiable individual*, may instead often relate to a device such as a computer. For example, *clickstream* data[200] can be collected through online tracking tools such as *cookie*s,[201] which can collect basic information from a web user (such as the type of computer and the Internet browser) and more private information including web pages visited,[202] how long the individual has looked at any given page,[203] as well as geographical location and any transactions or comments made.[204] Although this data pertains to a device connected to the Internet, it may also be possible to indirectly identify specific users. An IP address refers to an Internet connection.[205] Even if using dynamic IP addresses,[206] it may be possible to link an IP

---

[199] See U.S. Department of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *supra* note 57 at section IV: "'Personal data' include all data that describe anything about an individual, such as identifying characteristics, measurements, test scores; that evidence things done by or to an individual, such as records of financial transactions, medical treatment, or other services; or that afford a clear basis for inferring personal characteristics or things done by or to an individual, such as the mere record of his presence in a place, attendance at a meeting, or admission to some type of service institution."

[200] Mouse clicks translate into an electronic signal, which is then sent by the user's computer to other computers on the Internet, sending or requesting certain information from them. See Eric Johnson, *An Examination of the Role of Clickstream Data in Marketing through the Internet* (12 May 1997), online: <http://www.ftc.gov/bcp/privacy/wkshp97/comments2/johnson0.htm>.

[201] For details on *cookies*, please refer to section 1.2.2 entitled "New Types of Information and Collection Tools". See also Solove, "Privacy", *supra* note 1 at 1411.

[202] Wong & Garrie, *supra* note 187, referring to: Karen Dearne, "You are Being Monitored Online" (2002) The Australian at 31 and Fusun Feride Gonul, "Stereotyping Bites the Dust; Marketers No Longer Focusing On Demographic Profiling" (2002) Pitt. Post-Gazette (Pa.) at B3.

[203] Joel R. Reidenberg & Paul M. Schwartz, *Data protection law and online services: regulatory responses*, delivered to Commission of the European Communities (December 1998) at 6.

[204] See Center for Democracy & Technology, *CDT's guide to online privacy* (22 October 2009), online: <http://www.cdt.org/privacy/guide/start>: "Use of the network, however, generates detailed information about the individual -- revealing where they 'go' on the Net (via URLs), who they associate with (via list-servs, chat rooms and news groups), and how they engage in political activities and social behavior."; Jerry Berman & Deirdre Mulligan, "Privacy in a Digital Age: Work in Progress" (1999) 23 Nova L. Rev. 551 at 554: "The data trail, known as transactional data, left behind as individuals use the Internet is a rich source of information about their habits of association, speech, and commerce. Transactional data, click stream data, or 'mouse droppings,' as it is alternatively called, can include the Internet protocol address ('IP address') of the individual's computer, the browser in use, the computer type, and what the individual did on previous visits to the Web site, or perhaps even other Web sites."

[205] An IP address is a numerical identification assigned to a device each time that it connects to the Internet in order to enable that device to communicate with other connected devices.

address to a subscriber to an Internet connection service, using a publicly available database to determine which ISP owns a specific IP address, and then using that ISP's log file to match a certain IP address to a specific ISP's subscriber. An IP address may also be used to disclose the physical location of a device, although it may not always be accurate.[207]

Other types of data may also be collected on the Internet. Search engines may collect and process a variety of data on top of IP addresses, *clickstream* data and information collected through cookies; including the content of search queries and user preferences.[208] Other service providers may request that users create an account in order to use their online services (participate in blogs, view or post videos, participate in an OSN) and will therefore collect the username of the user participating in the service. In the Google/Viacom case,[209] the U.S. court took the position that *usernames* were not *personal information*.[210] Orin Kerr, law professor at George Washington University and an expert in digital privacy, suggested that the court was wrong in thinking that user IDs are not personally identifiable since many people include parts of their name, their birthday or other personal information in their user IDs on the Internet, which can be used to identify them.[211] Email addresses are another relatively new kind of contact information which may or may not identify an individual at all times.[212] In the wireless space, location data can identify the location of a mobile device (and therefore, potentially the mobile users' physical location as well) which creates many

---

[206] A device can connect to the Internet either with the same IP address each time (static IP address), or with a different number each time (dynamic IP address).

[207] Article 29 Data Protection Working Party, *Opinion 1/2008 on data protection issues related to search engines*, [2008] 00737/EN WP 148 at 6 [Article 29 Data Protection Working Party, *Opinion 1/2008*].

[208] *Ibid*.

[209] For details on the suit, see Miguel Helft, "Judge Sides With Google in Viacom Video Suit" *The NY Times* (23 June 2010), online: <http://www.nytimes.com/2010/06/24/technology/24google.html>.

[210] "Google Ordered To Turn Over All Personal YouTube Viewing Records To Viacom", online: Search Engine World <http://www.searchengineworld.com/google-search/3458026.htm>.

[211] Matt Hartley, "YouTube told to hand over users' data" *Globe and Mail* (3 July 2008).

[212] For an email address to qualify as *personal information*, it would have to identify an individual. See Pierre Trudel, France Abran & Gabriel Dupuis, *Analyse du cadre réglementaire québécois et étranger à l'égard du pourriel, de l'hameçonnage et des logiciels espions*, Rapport préparé pour la Direction des politiques du ministère des services gouvernementaux du Québec (Montréal : Chaire L.R. Wilson et CRDP, 2007) at 55.

privacy concerns[213] to the point that certain jurisdictions have taken the position that location data should qualify as *personal information*.[214]

With new types of data generated through the Internet and related technologies, it may not always be clear if such data actually relates to an *identifiable* individual and therefore, qualifies as *personal information*.[215]

1.2.3. New Identifying Methods

When the principles of FIPs were initially articulated, one of the key concerns was the fact that while certain data concerning an individual may be inoffensive by itself, it may be correlated in such a way as to threaten that individuals' private interests.[216] Chief among these threats was the capacity to easily compile "personal profiles" and correlate information.[217] These concerns were not objective however, since technological advancements at that time were such that it was technically difficult to build a detailed profile of an individual.[218]

Nowadays, technological developments are triggering the emergence of new identification tools, which allow for easier identification of individuals. While information collection by tracking tools may be anonymous, simple learning algorithms can automate the process of linking, or re-identifying identities back to their seemingly anonymous data.[219] This process may be done using the IP address, enabling the correlation of different types of data made available on the web or through online

---

[213] See Gratton, *Internet and Wireless Privacy*, *supra* note 193 at 265-325.

[214] OPCC, *PIPEDA Case Summary #2006-351: Use of personal information collected by Global Positioning System considered* (9 November 2006) [OPCC, *PIPEDA Case Summary #2006-351*]. See also Julien L., "L'Europe veut faire de la géolocalisation une donnée personnelle" (13 May 2011), online : Numerama <http://www.numerama.com/magazine/18787-l-europe-veut-faire-de-la-geolocalisation-une-donnee-personnelle.html>.

[215] See section 2.1.2.2.1 entitled "Notion of Identifiable Individual" which elaborates on this issue.

[216] See Council of Europe, *Explanatory Report: Resolution (73) 22*, *supra* note 56 at para. 3.

[217] *Report of the Committee on Privacy*, *supra* note 3 at 180, para. 582: "Of these fears about the computer, the three which seem to be uppermost in the public mind are its facility to compile 'personal profiles', its capacity to correlate information and its provision of new opportunities for unauthorised access to personal information."

[218] Council of Europe, *Explanatory Report: Resolution (74) 29*, *supra* note 65 at para. 1: "(…) In fact, it is by no means a simple matter to build up such profiles – a number of technical difficulties stand in the way. Nevertheless, this potential capacity of modern public administration has awakened in some people a fear that their privacy is losing ground."

[219] Bradley Malin, "Betrayed By My Shadow: Learning Data Identity via Trail Matching" (2005) Journal of Privacy Technology at 1.

services.[220] Trail re-identification can take place via the pattern of locations that individuals visit.[221] Furthermore, as online browsing behaviour becomes more complex, the less sparse a trail becomes, the easier it is for an IP address trail to be re-identified.[222] Some report the tactics which might be used to identify anonymous Internet posters, even in cases where IP addresses might not have been logged by the site which hosts the comment.[223]

An important question then emerges: how *is* the notion of "identifiable individual" challenged by this new generation of data-collection techniques; whether it be through the aggregation and the correlation of data, through improved data-mining capabilities or through the convergence of several technologies?

1.2.3.1. Aggregation and Correlation of Data

While a certain piece of information may be meaningless on its own, it may take on a whole new meaning when aggregated or correlated with other pieces of data. While aggregating and correlating information is not a new activity, its power and scope have increased along with Internet technologies.

Internet technologies allow for the grouping of widespread information of various types about an individual, which can lead to identification. The website www.123people.fr is an example of an online service provider that groups and aggregates all kinds of information (such as pictures, email addresses, links, etc.) pertaining to the name of an individual searched and displays the data available, which would otherwise be more difficult to obtain in a logical and comprehensive manner. This type of service can

---

[220] Many services providers may also, using IP addresses and correlating it with other data that they have collected, identify an individual behind an IP address. For example, a search engine provider may be able to link an IP address to an individual by linking different requests and search sessions originating from a single IP address to track and correlate all the web searches originating from a single IP address if these searches are logged. See *Resolution on Privacy Protection*, *supra* note 177.

[221] Malin, *supra* note 219 at 2: "In this paper, we make an extension to trail re-identification, which considers how re-identification can occur via the pattern of locations people visit. (…) In some cases, a location also collects and shares, in a different release of data, this allows for trails to be constructed, where a trail is a characterization of the locations that an individual visited. Similar patterns in the trails of de-identified and identified data can be used to link the two."

[222] *Ibid*. at 16.

[223] TJ Mcintyre, "Alternative routes to identifying 'anonymous' online users" (18 February 2010), online: IT Law in Ireland <http://www.tjmcintyre.com/2010/02/alternative-routes-to-identifying.html>: "The key insight is that sites typically embed multiple external services (such as advertising, stats counters and video hosting) which may either individually or in combination enable the identity of particular users to be pinned down."

create a new profile of the individual, which results in a much more expansive intrusion into that individual's life than if each item of data posted on the Internet remained separate.[224]

Online service providers may offer different types of services and may collect different types of data for each service offered. Therefore, data correlation across services raises additional privacy concerns.[225] For instance, many search engine providers offer users the option of personalising their use of services through a personal account.[226] With web 2.0 and OSNs and the new trend towards increased cross-site profile linkage, certain types of data which could not previously be used to identify an Internet user may now be used to do just that.[227] Many service providers on the Internet explicitly admit in their privacy policy that they enrich data provided by users with data from third parties.[228] Privacy concerns have even put a stop to potential corporate

---

[224] Article 29 Working group has raised their concerns with regards to the retrieving and grouping capabilities of search engines. See Article 29 Data Protection Working Party, *Opinion 1/2008*, *supra* note 207 at 5, 14.

[225] In February 2012, privacy concerns were raised when Google's new privacy policy consolidated more than 70 policies into one general policy. See Jordan Press, "Google tries to allay concerns over new privacy Policy" *The Montreal Gazette* (29 February 2012), online: <http://www.montrealgazette.com/technology/Google+tries+allay+privacy+concerns/6230292/story.html>.

[226] They may also, on top of search services, offer email services or other communication tools such as messenger or chat, and social networking tools. As an example, Google offers gmail email services. Some have raised their concerns with the potential data correlation that may take place with online service providers such as search engines. See: Article 29 Data Protection Working Party, *Opinion 1/2008*, *supra* note 207 at 21.

[227] Dan Brickley, "YouAndYouAndYouTube: Viacom, Privacy and the Social Graph API" (3 July 2008), online: danbri's foaf stories <http://danbri.org/words/2008/07/03/359#comment-15692>: "YouTube users who have linked their YouTube account URLs from other social Web sites (something sites like FriendFeed and MyBlogLog actively encourage), are no longer anonymous on YouTube. (…) It can give them a mechanism for sharing 'favourited' videos with a wide circle of friends, without those friends needing logins on YouTube or other Google services. This clearly has business value for YouTube and similar 'social video' services, as well as for users and Social Web aggregators. Given such a trend towards increased cross-site profile linkage, it is unfortunate to read that YouTube identifiers are being presented as essentially anonymous IDs: this is clearly not the case. If you know my YouTube ID 'modanbri' you can quite easily find out a lot more about me, and certainly enough to find out with strong probability my real world identity. (…) To understand YouTube IDs as being anonymous accounts is to radically misunderstand the nature of the modern Web."

[228] For example Microsoft, in its Microsoft Online Privacy Notice Highlights says: "When you register for certain Microsoft services, we will ask you to provide personal information. The information we collect may be combined with information obtained from other Microsoft services and other companies". See online: <http://privacy.microsoft.com/>. About the sharing of data with advertising partners, Microsoft in its full privacy statement, states: "We also deliver advertisements and provide website analytics tools on non-Microsoft sites and services, and we may collect information about page views on these third party sites as well". See online: <http://privacy.microsoft.com/en-us/fullnotice.aspx>. Google in its privacy policy states: "We may combine personal information collected from you with information from other Google services or third parties to provide a better user experience, including customizing content for you". See online: <http://www.google.com/intl/en/privacy.html>. Yahoo!, in its privacy policy, states: "Yahoo! may combine

mergers in a few cases. At issue was the amount of personal information possessed by the respective corporations which, once pooled together, would have resulted in very detailed files on individuals. In the potential merger of DoubleClick and Abacus (2000)[229] and more recently, of Lotus Development and Equifax Inc.,[230] the companies collaborating on a new venture backed off from merging, citing negative publicity.

1.2.3.2. Extensive Data-mining Capabilities

New algorithms are being developed that allow extraction of information from a sea of collected data.[231] Data-mining techniques and capabilities are reaching new levels of sophistication, even compared with just a few years ago,[232] creating concerns in certain programs or initiatives involving the massive collection of readily available information. For example, anti-terrorism initiatives relating to the collection of data available through the network such as the "Total Information Awareness" program in the U.S. or the "Lawful Access initiative" in Canada that provides police and government spies broader powers to snoop on citizens have generated much discussion and debate.[233]

---

information about you that we have with information we obtain from business partners or other companies." See online: <http://info.yahoo.com/privacy/us/yahoo/details.html> [Yahoo! Privacy Policy].

[229] Courtnet Macavinta, "Privacy advocates rally against DoubleClick-Abacus merger" *Cnet News* (22 November 1999), online: Cnet.com <http://news.cnet.com/Privacy-advocates-rally-against-DoubleClick-Abacus-merger/2100-1023_3-233413.html#ixzz1O8HfI0GS>.

[230] In the U.S., one case that spured a storm of protest centered on Lotus Marketplace: Households, a database intended for distribution on CD-ROMs which contained aggregated information about roughly 120 million individuals in the United States, including names, addresses, types of dwelling, marital status, gender, age, approximate household income, and so forth. Discussed in Helen F. Nissenbaum, "Privacy as Contextual Integrity" (2004) 79:1 Washington Law Review 119 at 121-22.

[231] See Waldo, Lin & Millet, *supra* note 6 at 2.

[232] Conseil de l'Europe, *L'autodétermination informationnelle*, *supra* note 20 at 24: "Comme nous l'avons noté, les technologies, plus par implémentation que par nécessité, génèrent et conservent les 'traces' de l'utilisation des services et autorisent, par des capacités de traitement sans commune mesure avec celles existantes il y a à peine dix ans, une connaissance de l'individu et de ses comportements, individuels ou collectifs, personnels ou anonymes."

[233] Renée M. Pomerance, "Redefining Privacy in the Face of New Technologies: Data Mining and the Threat to the 'Inviolate Personality'" (2005) 9 Can. Crim. L. Rev. 273 at 283-84: "One of the anti-terrorism initiatives that have generated much discussion and debate is the program known in the United States as 'Total Information Awareness' (TIA). The TIA contemplated a broad sweep of information from both the public and private sphere including, but not restricted to, medical and financial history, political activities, travel patterns, prescription purchases, buying habits, communications (including e-mails and internet surfing patterns), school records, land sales transactions, records of asset holdings, employment status, marital status, personal and family associations and a host of other personal matters. TIA was highly criticized on the grounds that it contemplated massive invasions of privacy." In Canada, similar concerns were raised with the Lawful Access reform. See Michael Geist, "Privacy Commissioner of Canada on

Projects involving the collection of information available on OSNs have also raised concerns.[234] For example, in a class project at the Massachusetts Institute of Technology (M.I.T.) two researchers, Carter Jernigan and Behram Mistree, analyzed more than 4,000 Facebook profiles of students (including links to friends who disclosed themselves as homosexual).[235] Using powerful data mining techniques, which relied on sophisticated statistical correlations, they were able to predict, with 78 percent accuracy, whether a profile belonged to a homosexual male.[236] A few years ago, Netflix awarded $1 million to a team of statisticians and computer scientists who won a three-year contest to analyze the movie rental history of 500,000 subscribers and improve the predictive accuracy of Netflix's recommendation software by at least 10 percent.[237] In 2008, a pair of researchers at the University of Texas[238] showed that the customer data released for Netflix's first contest, despite being stripped of names and other direct identifying information, could often be "de-anonymized" by statistically analyzing an individual's distinctive pattern of movie ratings and recommendations.[239] This was possible from having ready access to other large sets of data where the subjects were already known. By overlaying social graphs and other intricate data-comparison

---

lawful Access: Deep Concerns" (28 October 2011), online: Michael Geist <http://www.michaelgeist.ca/content/view/6093/125/>.

[234] See "Scientists Develop World's Fastest Program to Find Patterns in Social Networks" (2 July 2012), online: Socialator <http://socialator.com/scientists-develop-worlds-fastest-program-to-find-patterns-in-social-networks/1609>.

[235] Carter Jernigan & Behram Mistree, "Gaydar: Facebook Friendships expose sexual orientation" (2009) 14:10 First Monday, online: First Monday <http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2611/2302>.

[236] Steve Lohr, "How Privacy Vanishes Online" *The New York Times* (16 March 2010), online: The New York Times http://www.nytimes.com/2010/03/17/technology/17privacy.html?emc=eta1 [Lohr, "How Privacy Vanishes Online"].

[237] *Ibid*.

[238] Vitaly Shmatikov, an associate professor of computer science at the University of Texas, and Arvind Narayanan, now a researcher at Standord University.

[239] Netflix carried out a project providing a monetary incentive for researchers to improve their movie-recommendation system. The company provided data on 500,000 of its subscribers' ratings of various movies and removed the subscribers' names and other PII. Two researchers at the University of Texas collated this data with reviews found in the database of the International Movie Database (or IMDb) and were able established the identity of two Netflix subscribers (IMDb's terms of use prevented them from executing a more comprehensive search of their records). According to the study, even attempting to complicate the re-identification task by inserting errors into the dataset would not overwhelm the researchers' algorithm used, which could theoretically identify up to 99% of the Netflix subscribers. See Arvind Narayanan & Vitaly Shmatikov, "Robust De-anonymization of Large Sparse Datasets" (2008) University of Texas at Austin. See also Natasha Singer, "When 2+2 Equals a Privacy Question" *The New York Times* (18 October 2009), online: The New York Times <http://www.nytimes.com/2009/10/18/business/18stream.html?_r=3&adxnnl=1&adxnnlx=1256572818-Q9UvohAQV7pfxZ1TkU/C+Q>.

methods, the "anonymous" datasets were quickly re-identified. Their research demonstrated just how trivial it was to re-identify the "anonymized" Netflix database.[240] Netflix cancelled its contest after privacy concerns were raised.[241]

Pete Warden ("Warden"), a former Apple engineer, has harvested and analyzed data from an astounding 215 million public Facebook profile pages.[242] Warden accumulated a database of names, fan pages, and lists of friends associated with the Facebook accounts.[243] Warden has already done some impressive analysis of this data at an aggregate level and was looking to release the results of his research.[244] Michael Zimmer, among others, believes that Warden should not disclose or use this data since individuals could be easily identified and that it has the potential to help re-identify *other* datasets, ones that might contain much more sensitive or potentially damaging data.[245] Facebook asked Warden to delay releasing this data to the academic community.[246]

---

[240] "Breaking the Netflix Prize dataset" (27 November 2007), online: The Physics arXiv blog <http://arxivblog.com/?p=142>.

[241] Steve Lohr, "Netflix Cancels Contest After Concerns Are Raised About Privacy" *New York Times* (12 March 2010), online: The New York Times <http://www.nytimes.com/2010/03/13/technology/13netflix.html>.

[242] He was exploiting a flaw in Facebook's architecture to access public profiles without needing to be signed in to a Facebook account, effectively avoiding being bound by Facebook's Terms of Service preventing such automated harvesting of data. Pete Warden, "How to harvest Facebook profiles from emails without logging in" (6 February 2010), online: Pete Warden blog <http://petewarden.typepad.com/searchbrowser/2010/02/how-to-harvest-facebook-profiles-from-emails-without-logging-in.html> [Warden, "harvest Facebook profiles"].

[243] *Ibid*.

[244] Pete Warden, "How to split the US" (6 February 2010), online: Pete Warden blog http://petewarden.typepad.com/searchbrowser/2010/02/how-to-split-up-the-us.html [Warden, "split the US"].

[245] Michael Zimmer, "Why Pete Warden Should Not Release Profile Data on 215 Million Facebook Users" (12 February 2010), online: Michael Zimmer.org <http://michaelzimmer.org/2010/02/12/why-pete-warden-should-not-release-profile-data-on-215-million-facebook-users/> [Zimmer, "Pete Warden"]: "Warden's release of this dataset — even with the best of intentions — poses a serious privacy threat to the subjects in the dataset, their friends, and perhaps unknown others. Warden claims to be sensitive to the privacy of the subjects in the database, and in response he has removed the identifying URL's that are unique to each profile, but the dataset retains the subjects' names *(really!)*, locations, Fan page lists and partial Friends lists (I'm not sure what is meant by a "partial" list of friends). So, obviously, individuals can be easily identified within the dataset. But that's not the greatest threat with the release of this data. What is most dangerous is its potential use to help re-identify *other* datasets, ones that might contain much more sensitive or potentially damaging data."

[246] Pete Warden, "The Facebook Whisperer" (10 February 2010), online: Pete Warden blog <http://petewarden.typepad.com/searchbrowser/2010/02/the-facebook-whisperer.html#idc-container>.

In a document published in 2009, two researchers from Carnegie Mellon University[247] reported that they could accurately predict the full, nine-digit Social Security numbers for 8.5 percent of the people born in the U.S. between 1989 and 2003 which account for nearly five million individuals.[248] The researchers used publicly available information from many sources, including profiles on OSNs. By identifying the date of birth and hometown (or home State) of a given person, the first three digits of their Social Security number could be revealed, which the government has assigned by location.[249]

The power of computers to identify people from social patterns alone was demonstrated last year in another study by the same pair of researchers that cracked Netflix's anonymous database. By examining correlations between various online accounts, the researchers demonstrated that they could identify more than 30 percent of the users of both Twitter[250] and Flickr,[251] even when the accounts had been stripped of identifying information like account names and e-mail addresses.[252]

1.2.3.3. Convergence in Technologies

The convergence of different technologies now makes it possible to collect data that are more intrusive and of a far more personal nature than before. For example, the changes to the core architecture of the Internet and its protocols (to Internet Protocol version 6) may permit many more physical objects to have an Internet address. A wider

---

[247] Alessandro Acquisti and Ralph Gross.

[248] Alessandro Acquisti & Ralph Gross, "Predicting Social Security numbers from public data" (2009) 106:27 Proceedings of the National Academy of Sciences of the United States of America 10975.

[249] Lohr, "How Privacy Vanishes Online", *supra* note 236: "Social Security numbers are prized by identity thieves because they are used both as identifiers and to authenticate banking, credit card and other transactions. The Carnegie Mellon researchers used publicly available information from many sources, including profiles on social networks, to narrow their search for two pieces of data crucial to identifying people — birthdates and city or state of birth. That helped them figure out the first three digits of each Social Security number, which the government had assigned by location. The remaining six digits had been assigned through methods the government didn't disclose, although they were related to when the person applied for the number. The researchers used projections about those applications as well as other public data, like the Social Security numbers of dead people, and then ran repeated cycles of statistical correlation and inference to partly re-engineer the government's number-assignment system."

[250] The microblogging service. See online: twitter <http:www.twitter.com>.

[251] An online photo-sharing service. See online: flickr <http://www.flickr.com/>.

[252] Arvind Narayanan & Vitaly Shmatikov, "De-anonymizing Social Networks" (2009) Proceedings IEEE Symposium on Security and Privacy 173.

range of devices may thus be able to connect to the Internet. Combining these objects with technologies such as RFID could affect privacy in many ways.[253]

The combination of various forms of technology may present a new set of privacy concerns. For example, video surveillance monitoring in retail spaces, when combined with readers and RFID tags, could facilitate identification of individual customers.[254] Facial recognition, quickly becoming available on a wide scale, is another example of one technology, which, once converged with another technology, may raise privacy concerns. Search engine providers may now call upon more refined forms of facial recognition technology in the context of image processing and image searches.[255] It was reported in 2010 that Facebook acquired facial recognition technology provider Divvyshot and began using a new facial recognition feature in its tagging process soon after, in the hopes of streamlining it.[256] Another example would be the application called Face.com which allows Facebook users to use photo recognition to find their friends in pictures (even if they have not been tagged, or if they have removed their tag).[257] Concerns around having a company unleash picture recognition on the Internet

---

[253] Robinson et al., *supra* note 151 at 17: "Communications networks and changes to the core architecture of the Internet and its protocols (e.g. Internet Protocol version 6, IPv6) will permit many more physical objects to have an Internet address, paving the way for a wide range of devices to be connected, such as vehicles, white goods and clothing. Combining these technologies with Radio Frequency Identification (RFID) could affect privacy in many ways, both good and bad." Certain privacy commissioners have also raised the fact that the percentage of search history data that can be linked to individuals is likely to further rise in the future due to the uptake of the use of fixed IP numbers in high-speed DSL or other broadband connections where user's computers are "always online", especially once the introduction of IPv6 is completed: See *Resolution on Privacy Protection*, *supra* note 177.

[254] Teresa Scassa et al., *supra* note 197 at 13. These authors suggest that the mere recording of RFID-signaled location and related information could produce a fairly accurate trajectory for the consumer even without accompanying video surveillance. This would enable retailers to link this information with pre-sales behaviour (perhaps even from past visits) if the consumer is identified through payment identification, loyalty card or other similar program. See also Hariton, Lawford & Palihapitiya, *supra* note 197 at 15, 28-29. These authors dicuss how, in *combination* with the video surveillance that is prevalent in a retail environment, RFID enables another, powerfully detailed dimension to video surveillance and that even without accompanying video surveillance, RFID would allow a retailer to track customers' movements through a store and even whether they had picked up an item.

[255] Article 29 Data Protection Working Party, *Opinion 1/2008*, *supra* note 207 at 14.

[256] Mike Melanson, "Facebook Adds Facial Recognition" (2 July 2010), online: Read Write Web <http://www.readwriteweb.com/archives/facebook_adds_facial_recognition.php?utm_source=twitterfeed&utm_medium=twitter&utm_campaign=Feed%3A+readwriteweb+%28ReadWriteWeb%29&utm_content=Twitter>.

[257] David Thompson, "The Future of Privacy: Facial Recognition, Public Facts, and 300 Million Little Brothers" (11 June 2010), online: The Volokh Conspiracy <http://volokh.com/2010/06/11/the-future-of-privacy-facial-recognition-public-facts-and-300-million-little-brothers/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+volokh%2Fmainfeed+%28The+Volokh+Conspiracy%29&utm_content=Google+Reader>.

could be huge given that there are billions of pictures on sites such as Flickr.com and Facebook, and in automated surveillance systems.[258] The convergence of surveillance and facial recognition technologies raise additional privacy concerns. For instance, it has been argued that a person's name could be logged each time he or she walks past a security camera.[259]

The lists of services that incorporate location data or *geotagging* has been growing recently, with sites such as Twitter, Flickr and other website service providers enabling users to include their location in the content that they post. As the list of programs that collect users' location information grows, so do the privacy concerns.[260] Twitter acquired a company involved in providing location-based services in December 2009.[261] Twitter started attaching geolocation within Twitter.com in winter 2010[262] and Twitter users can pull up location information from individual's tweets. Concerns were immediately raised over the potential of burglars becoming privy to the location of tweeters.[263] An increasing number of websites and OSN services are adopting geotagging, allowing users to include their exact location when they update their status

---

[258] See section 1.2.1.2 entitled "New Ways of Using the Internet: Web 2.0" which discusses web 2.0 and the volume of information in OSNs. See also Thompson, *supra* note 257.

[259] *Ibid*.: "Why would anti-abortion groups not photograph every person who walks into an abortion clinic, use facial recognition to identify them, and use public name-and-address databases (see below) to target mailings (or harassment) to each person's home? Why would anti-gay advocates not do the same for people who frequent gay bars, or liberals target 'Tea Party' activists, or statists target libertarians, etc? Or insurance companies outside bars to monitor drinking and driving, smoking, or any other risk factor that could increase rates? What does this mean for privacy (…) What does it mean when Google indexes a list of these names and it comes up first for a search for your name? How will it affect job prospects, inter-personal relations, and more?"

[260] See Jennifer Valentino-DeVries, "As Location-Sharing Services Grow, Privacy Concerns Do Too" *The Wall Street Journal* (10 March 2010), online: The Wall Street Journal <http://blogs.wsj.com/digits/2010/03/10/as-location-sharing-services-get-more-popular-privacy-concerns-grow/?mod=wsj_share_twitter>; See also The Canadian Press, "Privacy commissioner looking at how Facebook gets data" (18 January 2010), online: ctv.ca <http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/20100118/facebook_privacy_100118/20100118/?hub=SciTech>.

[261] Agence France-Presse Washington, "Twitter acquiert une entreprise de géolocalisation" *La presse affaires* (24 December 2009), online : Lapresse.ca <http://lapresseaffaires.cyberpresse.ca/economie/technologie/200912/24/01-933976-twitter-acquiert-une-entreprise-de-geolocalisation.php>.

[262] Ben Parr, "Twitter's Website Now Attaches Location to Tweets [PICS]" (10 March 2010), online: Mashable <http://mashable.com/2010/03/10/twitter-geolocation-tweets/>; Jeff Bertolucci, "Twitter Adds Location-Sharing: I'm Eating Tacos…In Texarkana" (12 March 2010), online: PC World <http://www.pcworld.com/article/191457/twitter_adds_locationsharing_im_eating_tacosin_texarkana.html>

[263] Kit Eaton, "Geotagging's Seasonal Danger: Burglary" (29 December 2009), online: Fast Company <http://www.fastcompany.com/blog/kit-eaton/technomix/geotaggings-seasonal-danger-burglary?partner=rss>.

via wireless devices. For instance, Facebook has recently added location technology to its service, allowing its 400 million users to see the current locations of their friends stream through their live news feed feature,[264] raising various privacy concerns.[265] In the mobile context, Unique Device Identifiers which are the unique serial number assigned to every mobile device (such as a smart phone), can be combined with location or other information provided to a third party mobile application to track a particular consumer's behavior or real-world whereabouts.[266]

All of these examples illustrate how the notion of *identifiable individual* can be challenged in the information age, with the emergence of new methods to identify individuals as well as the prevalence of new aggregation and data-mining techniques, or with the convergence in various technologies.

1.2.4. New Uses of Information

Both the private and the public sectors are interested in using collection tools generating data that have emerged as well as the data made available through the Internet and its related technologies. In the public sector, new types of data are being used to achieve security and crime fighting objectives.[267] Recent cases show how IP

---

[264] John Brownlee, "Facebook to become location aware in April" (9 March 2010), online: geek.com <http://www.geek.com/articles/news/facebook-to-become-location-aware-in-april-2010039/#ixzz0ojX7rsOf>.

[265] The Canadian Press, *supra* note 260: "Emerging social media trends include mobile access and location-based features. Foursquare encourages users to share details about where they go on a daily basis, including which shops and restaurants they frequent. With many phones now using GPS locators, 'it's going to be very easy to know where everybody is at every moment and I think there's going to be a lot of problems around that,' Israel said. 'Law enforcement can access this kind of information if it's on someone's server, often just by asking or with some type of warrant. So they'll be able to know where everybody was at any given time.'"

[266] See Gratton, *Internet and Wireless Privacy*, *supra* note 193 at 32-36; See also Jacqui Cheng, "iPhone user privacy at risk from apps that transmit personal info" (3 October 2010), online: Ars Technica <http://arstechnica.com/apple/news/2010/10/iphone-user-privacy-at-risk-from-apps-that-transmit-personal-info.ars>.

[267] Access to this new data flow would be used in prosecuting illegal activities such as identity fraud and would be useful when combating organized crime and terrorist activities. Public sector and governmental entities want access to data generated on the Internet in order to identify those who have or are likely to engage in anti-social or criminal behaviour. See Google webpage describing the types of government requests that they receive: <http://www.google.com/governmentrequests/>; See also Michel-Adrien Sheppard, "Google Releases Data on Government Requests for Private User Data" (21 April 2010), online: Slaw <http://www.slaw.ca/2010/04/21/google-releases-data-on-government-requests-for-private-user-data/>; Rob Wright, "Google Launches New Site Detailing Government Data Requests" (21 April 2010), online: CRN <http://www.crn.com/software/224500123;jsessionid=YGOXRKPKTN2A3QE1GHPCKHWATMY32JVN>; See also Pomerance, *supra* note 233 at 277; See MacRonin, "Twitter & FaceBook Tapping / Law enforcement and its social surveillance" (13 December 2009), online: Privacy Digest

addresses, spyware and other new types of data or online collection tools are used by law enforcement officials to thwart illegal online activities or in the context of criminal investigations.[268] In spring 2006, the U.S. Department of Justice had requested millions of search requests from Google, in a court case *inter alia* dealing with protection against online child pornography. Google refused to comply and eventually won the case.[269] In Europe, telecoms and ISPs are mandated by the *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic* ("Directive 2006/24/EC")[270] to store call and connection data for up to two years under the national security and criminal investigation exceptions of Directive 95/46/EC.[271] Access to large amounts of data sets would be very useful in detecting fraud.[272] While this issue (access to data by public sector entities) is outside the scope of this thesis, it is interesting nonetheless to note the interest for, and value of, these new types of data collection tools, both at private and public sector levels.

<http://www.privacydigest.com/2009/12/13/twitter%20facebook%20tapping%20law%20enforcement%20and%20its%20social%20surveillance>; See also Orin Kerr, "Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn't" (2003) 97 NW. U. L. Rev. 607.

[268] In one recent Canadian case, after determining the IP address of username of the suspect, an officer did a trace on a program called WHO IS (command program available to the public) in an effort to learn from where the suspect was coming and was then able to ascertain that the person using the username was a Rogers Internet customer from the Toronto area: *Her Majesty the Queen* v. *Arthur Kwok*, Ontario Court of Justice W.A. Gorewich J., January 25, 2008, Docket: Newmarket 06-06029; In the U.S., summer 2007, the FBI used spyware to track down a bomb threat hoaxter, more specifically a "Computer & Internet Protocol Address Verifier" (CIPAV) that was installed on the suspect's machine remotely through his MySpace account, See: Anderson, "FBI", *supra* note 189; Poulsen, *supra* note 189; In a recent 2008 case, police had developed a system of searching that allowed them to view IP addresses of people sharing or making available certain child-pornography files. See Christie Blatchford, "A precedent on Internet privacy in the making", *The Globe & Mail* (9 April 2008); Shannon Kari, "Television beer pitchman at centre of pornography, privacy battle", *National Post* (9 April 2008).

[269] See *Resolution on Privacy Protection*, *supra* note 177.

[270] EC, *European Parliament and Council Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC*, [2006] O.J., L. 105/54.

[271] See *ibid*. which makes reference in its preamble (4) to "safeguard[ing] national security (i.e. State security), defence, public security or the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communications systems".

[272] For instance, it was reported that a social security agency in The Netherlands (GAK) saved the community 30 million dollars in 1996 by means of very simple computer matching procedures to detect fraud. The Italian government decided to match the list of people who receive government allowances because they are blind and the list of persons who recently got their drivers-licence. See M. Jeroen van den Hoven, "Privacy and the Varieties of Moral Wrong-doing in an Information Age" (1997) Computers and Society 33 at 33, online: <http://www.interwebbeheer.nl/img/pdf/test.pdf> [Van den Hoven, "Moral Wrong-doing"].

In the private sector, organizations may be interested in learning about the habits and preferences of consumers so that they can more effectively target their marketing strategies, establish strong ties with their most valued customers, and gain the knowledge which may be useful to improve their services and products or develop new ones.

1.2.4.1. New Business Models (Customization and Sponsored Services)

At the time that FIPs were elaborated, concerns regarding business models which involved the collection and distribution of personal information were already being raised:

> "(…) accompanying these technical developments, there has been a spectacular growth in the collection and distribution of information as a commercial activity, which has given rise to anxiety in connection with the granting of credit, mail-order business and other forms of promotion."[273]

These concerns are becoming more and more tangible with the advent of the Internet and related technologies. Online business models are increasingly based on the notion of greater customization of services and products. Businesses now look to use personal or new types of data to improve their marketing strategies. Due to the global dimension of its potential audience, the Internet has also become an increasingly attractive forum for advertisers who can target their campaigns more precisely and effectively than advertising in other media. In 2008, online advertising was a 27 billion dollar market, a figure which was projected to double within four years.[274] This extraordinary market growth can be explained by two factors.

First of all, technology now makes it possible to gather a lot of information to profile an individual and track their online conduct in order to send personalised advertising or tailor websites or services accordingly. More specifically, transactional websites can use information collected about users to make product recommendations based on purchase or browsing history. Behavioural advertising provides benefits to consumers in the form of free web content and personalized advertisements.[275] Online behavioural

---

[273] *Report of the Committee on Privacy*, *supra* note 3 at 6, para. 18.

[274] European Parliament, *Seminar Data protection*, *supra* note 164 at 2.

[275] Online behavioural advertising involves tracking consumers' online activities over time in order to deliver advertisements targeted to their inferred interests. Behavioural advertisers often use sophisticated

targeted advertising may allow the displaying of more relevant advertisements that reflect the user's interests or allow the website to ensure that the same advertisements are not repeatedly provided to a user.[276] The profitability of search engines generally relies on the effectiveness of the advertising that accompanies the search results.[277] Professor Eric Goldman believes that data mining can help marketers with targeting such that recipients would only receive substantive utility positive messages from marketers, resulting in increased social welfare.[278] Certain industry players also claim that personalized advertising is a real and a valued service since many individuals which could opt-out from this service, refuse or omit to do so.[279]

Secondly, many online service providers are offering services, information, and entertainment free of charge to online users as long as they accept to receive advertising and allow their online behaviour to be tracked.[280] Various services are offered for free online as they may be partially supported by advertising revenue; including OSN services such as Facebook and Google's web service Gmail.[281] Additionally, more individuals are able to access newspaper content on the Internet for free because it is subsidized by online advertising.[282] Some claim that the entire reason

---

algorithms to analyze the collected data, build detailed personal profiles of users, and assign them to various interest categories. Interest categories are used to present ads defined as relevant to users in those categories. See Office of the Privacy Commissioner of Canada, *Privacy and Online Behavioural Advertising*, Guidelines, December 2011, online: <http://www.priv.gc.ca/information/guide/2011/gl_ba_1112_e.pdf> [OPCC, *Online Behavioural*].

[276] Lo, *supra* note 188 at 48.

[277] Article 29 Data Protection Working Party, *Opinion 1/2008*, *supra* note 207 at 6.

[278] Eric Goldman, "Data Mining and Attention Consumption" in Katherine Jo Strandburg & Daniela Stan Raicu, eds., *Privacy and Technologies of Identity: A Cross-Disciplinary Conversation* (New York: Springer, 2006, online: SSRN <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=685241>, discussed in Lo, *supra* note 188 at 48.

[279] Alma Whitten & Peter Fleischer, "Le droit à l'oubli ne doit pas aboutir à une possible censure" *Les Echos* (20 April 2010), online : LesEchos.fr <http://www.lesechos.fr/info/comm/020487929397--le-droit-a-l-oubli-ne-doit-pas-aboutir-a-une-possible-censure-.htm>: "Plusieurs dizaines de milliers de personnes visitent déjà Google Ads Preferences tous les jours. Ce qui est intéressant, c'est que, sur 15 personnes qui utilisent cet outil de gestion, une seule choisit l'opt-out, quatre choisissent d'ajouter ou d'enlever des centres d'intérêt et de recevoir des publicités ciblées sur d'autres domaines et dix ne changent rien. Cela signifie que la publicité ciblée apporte un vrai service aux gens."

[280] Google, "Response to the Article 29 Working Party Opinion On Data Protection Issues Related to Search Engines" (8 September 2008) at 3: "to support this free service, Google primarily relies on being able to serve relevant advertising to its users".

[281] Users of Microsoft Outlook email application pay for a license, they download emails and store them on their own laptop. For users of Google Gmail services, their emails are managed through a web browser and are stored remotely with Google. The user pays for its Gmail account by being exposed to the advertisements that Google places on the far right edge of the screen. See Picker, *supra* note 21 at 7.

[282] Lo, *supra* note 188 at 48.

to use services such as OSNs, is to trade privacy for other benefits, giving up personal information to find long-lost friends or to share pictures.[283] Certain studies even show that individuals don't want and don't expect to be paying for web services.[284] Similar issues can take place offline, for instance with RFID technology. For example, frequent shopper programs and discount cards could enable the scanner data to be matched to data about individual consumers and offer savings in return for personal information and the ability to track a person's grocery purchases.[285]

In light of this, personal information is seen increasingly as a commodity on the Internet.[286] On April 8, 2010, three advocacy organizations filed a complaint in the U.S. with the Federal Trade Commission ("FTC"), demanding that it investigate and impose drastic requirements on entities involved in online data analytics and behavioural advertising.[287] One of the requests made by the advocacy groups to the FTC was to ensure that consumers receive fair financial compensation for the use of their data.

---

[283] L. Gordon Crovitz, "Privacy Isn't Everything on the Web" *The Wall Street Journal* (24 May 2010), online: The Wall Street Journal <http://online.wsj.com/article/SB10001424052748704546304575260470054326304.html>: "Privacy advocates this month filed a complaint against Facebook with the Federal Trade Commission, but would-be regulators need to recognize something unusual about privacy expectations on social media sites: The entire reason to use these sites is to trade privacy for other benefits. Some people give up information about themselves to find long-lost friends or to share pictures—there are some 48 billion photos on Facebook, making it the world's largest photo archive. Others use sites like Twitter to find links to news stories their friends find interesting or to see what colleagues think about the Senate finance-reform bill."

[284] Internet Advertising Bureau, *PIPEDA + IAB Canada's Industry Self-Regulation Initiatives: A Win-Win For Canadian Consumers, Web Publishers + Web Innovators Going Forward…*, Submission for the 2010 Privacy Commissioner Consultation, 15 March 2010, at 5 [IAB]: "Online Consumers have come to expect that all the content that they wish to consume – whether it is developed by industry professionals, or by themselves – will be supplied to them free of charge. In fact, according to the latest survey by Forrester Research, a full 80% of Internet users would abandon both Magazine and Newspaper products Online, if they were suddenly asked to pay for them."

[285] Robert O'Harrow, Jr., "Bargains at a Price: Shoppers' Privacy; Cards Let Supermarkets Collect Data", *The Washington Post* (31 December 1998) at A1.

[286] Solove, "Privacy", *supra* note 1 at 1448: "In order to receive such services as book recommendations, software upgrades, free email, and personal web pages, users must relinquish personal information not knowing its potential uses. In short, useful information and services are being exchanged for personal information, and this represents the going 'price' of privacy."; See Malin, *supra* note 219 at 1: "Data collections have become commodities that can be shared, licensed, or sold for profit in many different communities."

[287] In their complaint, the U.S. Public Interest Research Group ("U.S. PIRG"), the Center for Digital Democracy and the World Privacy Forum targeted Google, Yahoo! and others for allegedly participating in what the U.S. PIRG terms a "Wild West" of online collection and auctioning of data for marketing purposes. See U.S., Federal Trade Commission, *In the Matter of Realtime Targeting and Auctioning, Data Profiling Optimization, and Economic Loss to Consumers and Privacy, Complaint, Request for Investigation, Injunction, and Other Relief: Google, Yahoo, PubMatic, TARGUSinfo, MediaMath, eXelate, Rubicon Project, AppNexus, Rocket Fuel, and Others* (Washington, D.C., 8 April 2010).

In the recent Canadian Internet Policy and Public Interest Clinic ("CIPPIC") complaint against Facebook,[288] one of the issues raised was the fact that since users were not allowed to opt out of Facebook ads, Facebook was unnecessarily requiring users to agree to such ads as a condition of service, in violation of Principle 4.3.3 of PIPEDA.[289] The finding of the privacy commissioner on this issue took into account the fact that the site is free to users and that since advertising is essential to the provision of the service, individuals who wish to use the service must be willing to receive a certain amount of advertising.[290] This case may illustrate a change in mentality as to what is acceptable from a privacy and business perspective, where a certain trade-off is necessary.

These findings may also have an impact in the mobile space. Wireless devices are powerful communication devices with respect to immediacy, interactivity and mobility and can act as the most powerful marketing communications devices.[291] Advertisers may wish to sponsor content alerts and location-specific services which may include traffic, navigation information, proximity and directory or information services,[292] mobile gaming, mobile-commerce and shopping support, mobile dating services[293] and buddy

---

[288] Office of the Privacy Commissioner of Canada, *PIPEDA Case Summary #2009-008, Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc., Under the Personal Information Protection and Electronic Documents Act by Elizabeth Denham, Assistant Privacy Commissioner of Canada* (16 July 2009) [OPCC, *PIPEDA Case Summary #2009-008*].

[289] Principle 4.3.3 of PIPEDA sets out that "an organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfill the explicitly specified and legitimate purposes".

[290] OPCC, *PIPEDA Case Summary #2009-008*, *supra* note 288 at Section 3, Finding 131: "Facebook has a different business model from organizations we have looked at to date. The site is free to users but not to Facebook, which needs the revenues from advertising in order to provide the service. From that perspective, advertising is essential to the provision of the service, and persons who wish to use the service must be willing to receive a certain amount of advertising."

[291] There is great also value in location data. It may be useful for marketers that may want to target and send mobile ads to mobile users, which are at a specific location to make a certain ad relevant (for example a discount for a coffee shop while the user is passing near the coffee shop). It may also be useful for marketers to have access to the historical location data of mobile users in order to gain knowledge about these users' interests and habits. For example, if a user often attends a stadium at the time when there is a football game taking place, then a marketer could make the assumption that this user is a football fan and promote goods or services relating to this interest. See Gratton, *Internet and Wireless Privacy*, *supra* note 193 at 24-29.

[292] For example, wireless users might be interested in receiving a service that would provide them with movie schedules, locations and reviews based on their location, for example when and if they are downtown on a weekend night.

[293] Wireless users may be interested in a dating service that would alert them if someone corresponding to the desired profile were in their area. At the same time, a content provider, like a specific coffee shop,

lists.[294] Since these advertisers may play a significant sponsorship role in the financing of mobile data services,[295] issues similar to those discussed regarding the Internet will potentially also take place in the mobile space.

1.2.4.2. Knowledge, Analytics and Innovation

Many online or mobile service providers may well wish to, and potentially benefit from, using analytics solutions in order to better understand consumer behaviour.[296] For instance, many websites and online service providers disclose, through their privacy policies, that they may collect some type of information in order to improve their websites, products or services.[297] Collecting data from users enables these companies to employ data mining techniques, analytics and similar tools or calculations, as well as to capture, analyze and correlate the data in order to uncover hidden patterns and future behaviors. The wealth of customer information may then be managed more strategically, while capitalizing on the information collected and optimizing the value of each customer.

The knowledge gained by organizations using analytics solutions and having them better understand the behaviour of their users may in certain cases be translated into direct or indirect benefits for consumers. Direct benefits would include personalised services, products and advertising where online businesses may be in a position to offer the right services to the right users at the right time.[298] Indirect benefits may

---

might want to sponsor this dating service by inviting these people, through their wireless devices, to meet at the closest coffee shop for a free coffee.

[294] For instance Facebook friends signed up with this service could be alerted on their mobile device when they are in close proximity, for example, within half a kilometer range.

[295] See Gratton, *Internet and Wireless Privacy*, *supra* note 193 at 24-29.

[296] Gratton, "Personalization", *supra* note 16.

[297] See Microsoft privacy policy, which states: "Microsoft collects and uses your personal information to operate and improve its sites and services. These uses may include (…) performing research and analysis aimed at improving our products, services and technologies", online: <http://privacy.microsoft.com/en-ca/fullnotice.mspx#EAB> [Microsoft privacy policy]. See Google privacy policy which states: "Google only processes personal information for the purposes described in this Privacy Policy (…) such purposes include: (…) protect and improve our services; (…) and Developing new services." Google privacy policy, online: <http://www.google.com/privacypolicy.html>; See Yahoo! Privacy Policy, *supra* note 228 which states: "Yahoo! uses information for the following general purposes: to customize the advertising and content you see, (…) improve our services (…)."

[298] Benefits include remembering customization settings, making product recommendations based on the user's previous purchases or browsing history, developing and improving the website to increase its usability for users and customizing how information is displayed on websites to appeal to each user's tastes. Behavioural advertising provides benefits to consumers in the form of free web content and

include organizations upgrading their current products and services based on their users' needs, developing new products and deploying new applications and services or the "repackaging" of certain products and services. This could mean that their users may only be charged for the services that they actually use instead of sponsoring other users' usage of certain services that they have no interest for (thus potentially reducing the costs for these users).

Data collection can also promote innovation.[299] It has been argued that blocking Google from collecting and analyzing information about its users would be a negative outcome, "because while we all reflexively hate the thought of a company analyzing our digital lives, we also benefit from this practice in many ways that we don't appreciate."[300] Some even claim that Google's best products (including the spell checker) would not be possible without users' data.[301]

Location data is also quite valuable and serves many purposes. Google Maps features a service called "My Location," which can collect anonymous location data of mobile smartphone devices.[302] By collecting and analyzing this location information, Google

---

personalized advertisements or by displaying more relevant advertisements that reflect the user's interests.

[299] See section 2.1.1.1.1 entitled "Ignoring the Importance of Information Flow For the Society" and section 2.1.1.1.2 entitled "Ignoring Legitimate Reasons for Collecting, Using and Disclosing Information" which elaborate on this issue. See also Robinson et al., *supra* note 151 at 13. See also Farhad Manjoo, "No More Privacy Paranoia, Want Web companies to stop using our personal data? Be ready to suffer the consequences" (7 April 2011), online: Slate <http://www.slate.com/articles/technology/technology/2011/04/no_more_privacy_paranoia.html?wpisrc=newsletter_tis>: "Broadly speaking, there are two types of data that Web companies keep on us—personally identifiable information (like your name and list of friends), and information that can't be tied to you as an individual. In our discussions about privacy, we rarely make this important distinction. While we focus on the disadvantages of companies collecting our information, we rarely look at the innovations that wouldn't be possible without our personal data. This is especially true when it comes to anonymous data—information that can't be used to identify you, but which serves as the building blocks of amazing things."

[300] *Ibid*.

[301] *Ibid*.: "How does Google know you meant *Rebecca Black* when you typed *Rebeca Blacke*? Note that this is a trick that no ordinary, dictionary-based spell-checker could perform—these are proper nouns, and we're dealing with an ephemeral personality. But since Google has stored lots of other people's search requests for Black, it knows you're looking for the phenom behind 'Friday.' The theory behind the spell-checker can be applied more broadly. By studying words that often come together in search terms—for instance, people may either search for 'los angeles *murder* rate' or 'los angeles *homicide* rate'—Google can detect that two completely different words may have the same meaning. This has profound implications for the future of computing: In a very real sense, mining search queries is teaching computers how to understand language (and not just English, either). If Google were forced to forget every search query right after it served up a result, none of these things would be possible."

[302] Dave Barth, "The Bright Side of Sitting in Traffic: Crowdsourcing road congestion data" (25 August 2009), online: Official Google Blog <http://googleblog.blogspot.com/2009/08/bright-side-of-sitting-in-traffic.html>.

can create real-time traffic reports on highways and even surface streets.[303] Location information of individuals collected over time may have the potential to provide traffic engineers and planners with rich data feeds necessary to promote optimal traffic flows and would also allow them to efficiently allocate transportation resources and to properly reroute traffic in emergency situations.[304] Information means knowledge, which in turn can promote the innovation of science and technology and benefits for the society.[305]

1.2.5. Increased Availability of Data

Concerns about personal information being widely disseminated and thereby causing a privacy breach are by no means a new social phenomenon. For example, during the first wave of conceptualizing privacy,[306] Brandeis and Warren's unease related to the loss of privacy prompted by the technological and media developments of their time. This development was a new form of sensationalist journalism, known as "yellow journalism," which made newspapers wildly successful and led to dramatically increased circulation and technological developments, specifically photography.[307] Some even argue that the Internet and related technological advancements may very well constitute the "yellow journalism" of the new millennium, since information can be circulated rapidly and inexpensively on the Internet.[308]

Interestingly, similar concerns were raised during the third wave of conceptualizing privacy as "individuals in control of their personal information".[309] A major fear was that computers could disseminate private information for purposes other than those for

---

[303] Manjoo, *supra* note 299.

[304] In the U.S. the Intelligent Transportation Society of America looking to anonymously track the location of mobile users, has argued that there may be great value in knowing, for instance, that a given individual lives in a certain area, works in another one and uses a certain road at a specific time of the day. This seemingly mundane information would, according to the companies, have the potential to provide traffic engineers and planners with rich data feeds necessary to promote optimal traffic flows. Location data would also allow them to efficiently allocate transportation resources and to properly reroute traffic in emergency situations. FCC, *supra* note 180 at 7.

[305] See section 2.1.1.1.1 entitled "Ignoring the Importance of Information Flow For the Society" which elaborates on the value of having personal information free flow in our society.

[306] See section 1.1.1.1 entitled "First Wave: Right to be Let Alone" which elaborates on the first wave.

[307] Warren & Brandeis, *supra* note 5.

[308] Ressler, *supra* note 118 at 3.

[309] See section 1.1.1.3 "Third Wave: Control over Personal Information" which elaborates on the third wave.

which it was supplied.[310] The privacy issue raised by *mass media* was on many legislators' and privacy groups' agendas since this allowed personal information to be made available to a very broad group.[311]

This simply illustrates how, during various waves of conceptualizing privacy, similar concerns re-appear with a focus on the specific technology at stake. An analogy can be drawn between privacy concerns emerging from the first wave (with yellow journalism), the third wave (pertaining to the dissemination of personal information by mass media) as well as with the current concerns resulting from Internet technologies. For example, the danger of information compiling and search engine capacities has often been noted.[312] Information, even public information, can be found more easily and then compiled so as to deduce private information. Pierre Trudel ("Trudel") articulates the view that this changes the scale of threats to privacy on the Internet.[313]

As a matter of fact, the Internet and related technologies have triggered a situation whereby there are temporal and physical shifts under which the availability of personal information has increased. The Internet has also triggered a potential increase in the volume of the audience to the information displayed online.

1.2.5.1. Shift in Size of Audience

As already mentioned, in the early 1970s, while the adoption of various DPLs around the world was being discussed, the threat to privacy presented by mass media was also on many legislators' and privacy groups' agendas. The 1972 U.K. *Report of the Committee on Privacy* pointed to the steady flow of complaints about the intrusiveness of mass media reporting.[314] These reports included intimate details which would not normally be thought of as being in the public domain. The concern was that personal information was made available to a broader group:

> "It is not contended in all evidence to us that the information concerned need be private, though if the information is also confidential its

[310] *Report of the Committee on Privacy*, *supra* note 3 at 6, para. 18.

[311] *Ibid*. at 19-20, para. 65.

[312] Daniel J. Solove, "Access and Aggregation: Public Records, Privacy and the Constitution" (2002) 86 Minn. L. Rev. 1137 [Solove; "Access and Aggregation"].

[313] Trudel, "Privacy Protection", *supra* note 164 at 326-27.

[314] *Report of the Committee on Privacy*, *supra* note 3 at 6, para. 19.

> unauthorised handling is all the more objectionable. The unauthorised handling of information which may well be known or available through approved sources can also constitute a breach of privacy in certain circumstances. The most obvious examples is where it is published at large to a far wider audience than would otherwise learn of it: the conduct of the mass information media is the main object of criticism under this heading."[315]

Although the threat posed by mass media was already in the minds of legislators, DPLs were not adopted to address these risks as they were targeting the specific concerns of automated data banks of personal information which were increasing with the rise in the volume of computers used by private and public sector entities.[316]

Still, we can draw an analogy between the privacy concern that was taking place in the early 1970s pertaining to the dissemination of personal information by mass media and the Internet. The fact that data on the Internet can be available to a much broader audience (all Internet users) than if in printed format (limited to individuals accessing the printed document which is available in a given jurisdiction) increases the impact of a disclosure. Once the data is released online, the audience and number of individuals who may access it are huge.[317]

Certain business models using new Internet technologies also illustrate these new concerns of "broad audience". For example, the Google Street View technology has created many privacy concerns because images of individuals doing things while in public, end up on the Internet, for everyone to see.[318] In the U.K., a business model under which commercial CCTV footage would be displayed on the Internet in order for Internet users to watch the footage and assist businesses in catching criminals has also raised concerns.[319] This last business model also raised temporal issues: while

---

[315] *Report of the Committee on Privacy*, *supra* note 3 at 19-20, para. 65.

[316] See section 1.1.2.1 entitled "Initial Concern: Computers and Electronic Data Banks" which elaborates on this issue.

[317] See section 1.2.1 entitled "Increase in Volume of Information" which elaborates on this issue.

[318] Katie, "20 Crimes Caught on Google Street View", online: Disordel Conduct <http://www.criminaljusticeschools.com/blog/20-crimes-caught-on-google-street-view>; "Craziest Google Street View Shots OF ALL TIME (PHOTOS, POLL)" (18 March 2010), online: The Huffington Post <http://www.huffingtonpost.com/2009/11/15/google-street-view-funny_n_357433.html>.

[319] Dhruti Shah, "CCTV site Internet Eyes hopes to help catch criminals" *BBC News* (3 October 2010), online: BBC News <http://www.bbc.co.uk/news/uk-11460897>. See also Daniel Hamilton, "Big Brother Watch: Internet Eyes Invades Privacy" (4 March 2011), online: <http://www.outlookseries.com/A0998/Security/3603_Daniel_Hamilton_Big_Brother_Watch_Internet_Eyes_Invades_Privacy_Daniel_Hamilton.htm>.

CCTV footage taken from the security camera may usually be deleted by the business if there is no incident reported,[320] once released on the Internet, it may become very difficult to keep any control on the duration of the availability of this footage.

1.2.5.2. Temporal Shift

In the early 1970s, the Lindop Report noted that while many individuals were looking to draw a distinction between what they called "public" and "private" information (the former class, including matters such as data subject's name, address, and sometimes age and marital status)[321] they did not believe that the simple distinction (between "public" versus "private" information) was feasible, or that it would be useful if it could be made.[322] This report also questioned the relevance of drawing a distinction between published and unpublished information. Such a distinction would overlook two important facts: "the fact that no one can know everything, and the fact that people forget even what they once knew."[323] This report suggested that any piece of information about any data subject would at any given time be known only to a limited number of people.[324]

With the Internet, information is now available for longer periods of time (if not forever).[325] Trudel articulates the view that with Internet technologies, there is a **temporal shift** in the sense that the persistence of information entails that pieces of data can outlive the context in which they were created and considered legitimate.[326] For example, it may be legitimate for a piece of information to be available to the public

---

[320] See section 3.1.1.2.2 entitled "Surveillance: Dataveillance not Specifically Addressed" which elaborates on the Quebec, Canadian and French legal framework regulating video surveillance.

[321] Lindop, *supra* note 96 at 270, para. 31.02.

[322] *Ibid*. at 270, para. 31.03.

[323] *Ibid*. at 270, para. 31.04.

[324] *Ibid*. at 270, para. 31.05: "The truth is that any piece of information about any data subject will at any given time be known only to a finite number of people. The number may be large or small, but (with very few exceptions) it will never comprise the whole of the population of the United Kingdom. Moreover, as time passes the number will necessarily become smaller – by death and by forgetting – unless the information is circulated anew. In short, personal information is not just either 'public' or 'private': there is a wide range of possible knowledge among the public for any given item."

[325] Trudel, "Privacy Protection", *supra* note 164 at 328: "There is also a temporal shift. The persistency of information entails that it can last longer than the circle in which it was legitimate. For example, it may be legitimate for a piece of information to be available to the public owing to a current event but archiving and virtual permanent availability on the Internet could go beyond what is necessary to report the news."

[326] *Ibid*.

owing to a current event but archiving and virtual permanent availability on the Internet could go beyond what is necessary to report the news. He suggests that now that information can be found effortlessly, we have to reassess the arguments used to determine whether a given piece of information is public or private.[327] On this issue, Scheiner also suggests that part of the privacy concern nowadays relates to the fact that digital data can remain available indefinitely since now routine transactions such as credit card payments, paying tolls via transponders and opening OSN accounts such as Facebook all generate digital records that are much easier and less expensive to store than to sort and delete.[328] As a result, digital data never dies. That is very different than what has happened for the rest of human history when fewer records or none at all were kept and after a while, people forgot details about particular incidents. He states: "We're a species that forgets stuff (…) We don't know what it's like to live in a world that never forgets."[329]

As the "lifespan" of data increases, so too does its dissemination. In response to these concerns, certain countries, such as France, have begun to entertain the adoption of laws that would allow individuals to request the deletion/removal of online data referring to or concerning them under the "droit à l'oubli" or the "right to be forgotten".[330]

1.2.5.3. Spatial Shift

Although personal records have been kept for centuries, only in contemporary times has the practice become a serious concern.[331] With Internet technologies, there is also a spatial shift in the sense that physical spaces seem to dissolve. According to Trudel, the place where information is now located has little impact on its accessibility, since as

---

[327] *Ibid*.

[328] Tim Greene, "Schneier: Fight for Privacy Or Kiss it Good-Bye" (9 March 2010), online: CIO <http://www.cio.com/article/569914/Schneier_Fight_for_Privacy_Or_Kiss_it_Good_Bye?page=2&taxonomyId=3089>.

[329] *Ibid*.

[330] Cécilia Gabizon, "Vers l'instauration d'un 'droit à l'oubli' numérique" *Le Figaro* (13 November 2009), online : <http://www.lefigaro.fr/web/2009/11/13/01022-20091113ARTFIG00012-vers-l-instauration-d-un-droit-a-l-oubli-numerique-.php>.

[331] See Solove, "Privacy", *supra* note 1, at 1400 to 1403 for a historical perspective on public sector databases and at 1403 to 1409 for a historical perspective on private sector databases.

soon as a document is available on a server, it can be found using general Internet search tools or other specialized tools.[332]

Certain online business models have been built around analyzing data already available, and therefore using it for business purposes by disclosing the analyzed data or the searched data. This may involve search engines or organizations that provide a specific profile of an individual online while searching what is already available on the web, but which would take a lot of time for an individual to gather. By "Googling" an individual's name,[333] much more can often be learned, including educational background and civic involvement (on LinkedIn), and various interests (Facebook). Mailana's Twitter analyzer discloses which 20 other individuals a twitter user most regularly interacts with.[334] www.123people.fr groups and aggregates all kinds of information (such as pictures, email addresses, links, etc.) pertaining to the name of an individual searched and displays the data available online in a comprehensive manner. This illustrates how technology and business models allow for easier access to information already available.

Significant personal information can be obtained for those willing to spend the time and efforts to access the information. On this issue, the 1978 Lindop Report noted that there was a barrier of accessibility to data which had once been published since anyone wanting to access it would have to spend enough time and trouble in retrieving it:

> "In theory, of course, much information which has once been published is accessible to anyone who is willing to spend enough time and trouble in retrieving it. The British Library newspaper library at Colindale, for example, has copies of all newspaper ever published in the United Kingdom. But the diligent researcher needs to do a good deal more than go to Colindale, for there is no subject index to the collection: he first

---

[332] Trudel, "Privacy Protection", *supra* note 164 at 327-28: "Distance in space and the passage of time seem to have much less impact on the real availability of information. The Internet makes publication routine and information can easily be published outside of legitimate circles, thus the increased risk. Naturally, cyberspace is made up of both public and private spaces but the reference points that distinguish between private and public have been blurred."

[333] "Googling" means searching for information on the Web, particularly by using the Google search engine.

[334] See online: <http://web.mailana.com/demo/>; Marshall Kirkpatrick, "The Inner Circles of 10 Geek Heroes on Twitter" (20 March 2009), online: ReadWriteWeb http://www.readwriteweb.com/archives/the_inner_circles_of_10_geek_heroes_on_twitter.php [Kirkpatrick, "The inner Circles"].

> needs to know where to look among some hundreds of thousands of files newspapers. Unless he has a pretty accurate idea of the date and place of the original report, he is unlikely to be able to find what he wants. The same is true for many other public records."[335]

Several authors suggest that the Internet has made the information much more easily accessible.[336] Outside the networked world, gaining access to a piece of information can be very difficult but that on the Internet, it seems that much information is within the reach of a simple search engine query.[337] Daniel Solove ("Solove") observes that until recently, public records were difficult to access since, for most of recorded history, they were only available locally.[338] Following the Internet revolution, public records can be easily obtained and searched from anywhere.

Access to court records is also emblematic of the quantitative and qualitative changes generated by the Internet. Solove discusses the U.S. federal courts, along with many state courts and agencies, which are developing systems to place their records online.[339] He suggests that while these records are readily available at local courthouses or government offices, placing them online has given rise to an extensive debate over privacy.[340] One of the concerns is triggered by the fact that court records may contain very sensitive information.[341] If one has access to special databases (and this access is fairly easy to get, in most instances), an interested party can ascertain a litigant's information such as his or her credit history, occupation, income, etc.

---

[335] Lindop, *supra* note 96 at 270-71, para. 31.06.

[336] Karl D. Belgum, "Who Leads at Half-time?: Three Conflicting Visions of Internet Privacy Policy" (1999) 6 Rich. J.L. & Tech. 1, reported in Trudel, "Privacy Protection", *supra* note 164 at 327-28: Belgum notes that: "Personal data, such as address, phone number, income, property value and marital status have always been available to those willing to dig. The Internet can make it possible for a much wider class of persons – essentially all Internet users – to gain access to similar types of personal information at little or no cost."

[337] Trudel, "Privacy Protection", *supra* note 164 at 327-28.

[338] Solove, "Access and Aggregation", *supra* note 312 at 1139.

[339] Daniel J. Solove, "A Taxonomy of Privacy" (2006) 154:3 U. Penn. L. Rev. 477 at 536 [Solove, "A taxonomy"]; See also Solove, "Privacy", *supra* note 1, at 1409: "Government agencies have begun to place records on their websites, and public records, once physically scattered across the country, can now be searched or gathered from anywhere in the country."

[340] Solove, "A taxonomy", *supra* note 339 at 536.

[341] Natalie M. Gomez-Velez, "Internet Access to Court Reports: Balancing Public Access and Privacy" (2005) 51 Loyola L. Rev. 365 at 371, reported in Trudel, "Privacy Protection", *supra* note 164 at 327-28: "Providing Internet access to court records increases exponentially the availability of court records, including any sensitive information they contain. Examples of sensitive information that might be found in court records include: social security numbers, home addresses, names of minor children, financial account numbers and medical information."

While some may argue that if information is already made public offline, then it should be available online as well; others may raise privacy concerns due to the fact that the data will become increasingly available once online. Many administrative bodies charged with examining the issue of making public records available online have hesitated because of the increased accessibility the Internet will bring.[342] In order to address these concerns, Solove suggests that in light of the revolution in accessibility provided by modern computer capabilities and the Internet, we must rethink the accessibility of the information in public records.[343] Helen F. Nissenbaum ("Nissebaum") also raises that the question of whether public records ought to be available online provokes similar questions about court records in general, and more particularly, whether some of the information contained in them and other public records should be reclassified as personal and deserving of greater protection.[344]

It is interesting to note that in one French precedent, in reviewing directories on the Internet, the Commission Nationale de l'Informatique et des Libertés ("CNIL") argued that data accessible to the general public does not lose its protection as "nominative information".[345] Specifically, the CNIL noted that consent for disclosure of directory information in a paper format should not preclude opposition to disclosure of the same information on-line or on CD-ROM. The rationale for this distinction lies in the CNIL's concern for the risks to finality that arises with the availability of directory information on-line.

1.2.5.4. Already Available Data Analyzed and Broadcasted

With new Internet technologies, there are certain types of disclosures that may take place, which may or may not be currently covered by DPLs.

This first type of activity relates to the disclosure of certain data or pieces of data which, independently, may not be covered by DPLs. The aggregation or analysis of this data may allow the formation of a profile, which may potentially identify an individual and may disclose facts that may be sensitive or of an intimate nature. As a matter of

---

[342] Nissenbaum, *supra* note 230 at 120-21; See also Solove, "A taxonomy", *supra* note 339 at 536.

[343] Solove, "Privacy", *supra* note 1 at 1456.

[344] Nissenbaum, *supra* note 230 at 131-32.

[345] See CNIL, *17e Rapport d'activité*, 73 (1997) [CNIL, *17e Rapport*].

fact, individuals' online and offline activities may reveal information such as the individuals' financial information, race, religion, marital status, hobbies, occupation, and the like. This is especially true with web 2.0 which is all about creating new technologies that makes it easy for everyday people to publish their thoughts, social connections and activities. The next stage of innovation online may be services like recommendations, *self and group awareness*, and other features made possible by software developers building on top of the huge mass of data that web 2.0 made public. This issue is that - once analyzed - the data may be released, showing the individual under a new light. Section 1.2.4.1 provides examples of certain recent business models built around analyzing available data and therefore using it for business purposes such as Google Street View or Mailana's Twitter analyzer.

Certain researchers are collecting data available online, analyzing it for research purposes and then releasing their findings. One such study was the *Tastes, Ties, and Time* Facebook project in 2008, where researchers wanted to release the dataset to the academic community.[346] More recently, there was the aforementioned Warden experiment[347] who had done some impressive analysis of the data available on Facebook at an aggregate level.[348] Warden created a social graph illustrating certain trends in information, which may be useful for various purposes.[349] He suggested that while his observations were interesting, they were only the beginning of what is possible and that name, location, friends and interests were great data points to analyze. Another concern could be that all these data points can be cross-referenced with external data and an example to illustrate this is what members of Facebook's own staff did when they compared users' last names to U.S. Census data, allowing them to

---

[346] Berkman Center for Internet and Society, Harvard University, "Tastes, Ties, and Time: Facebook data release" (25 September 2008), online: <http://cyber.law.harvard.edu/node/4682>.

[347] Warden, "harvest Facebook profiles", *supra* note 242.

[348] Warden, "split the US", *supra* note 244.

[349] Marshall Kirkpatrick, "The Man Who Looked Into Facebook's Soul" (8 February 2010), online: ReadWriteWeb <http://www.readwriteweb.com/archives/facebook_user_data_analysis.php>: "There's so many interesting ways to slice the data - especially as I'm starting to get changes over time. I'm also trying to map out political networks in aggregate; how polarized the fans of particular politicians are - so how likely a Sarah Palin fan is to have any friends who are fans of Obama, and how that varies with location too. One of my favorite results is that Texans are more likely to be fans of the Dallas Cowboys than God." (…) "Nobody thinks about how much valuable information they're generating just by friending people and fanning pages. It's like we're constantly voting in a hundred different ways every day. And I'm a starry-eyed believer that we'll be able to change the world for the better using that neglected information. It's like an x-ray for the whole country - we can see all sorts of hidden details of who we're friends with, where we live, what we like."

estimate changes in Facebook's racial composition over time based on the likelihood of people with particular last names to report a particular racial backgrounds.[350]

***

The modern definition of privacy as the individuals' right to "control their personal information" is to some degree inspired by the work that was done during the late 1960s and early 1970s.[351] In the late 1960s, when attempting to determine as to whether the privacy provision of the European Convention on Human Rights needed to be re-evaluated in light of technological changes, the Consultative Assembly of the Council of Europe raised the fact that most of the then new technological and scientific developments which were potentially a great danger to human dignity and freedom, had occurred after the drafting of the European Convention on Human Rights. Therefore, that they could not have been foreseen by their authors.[352] The same reasoning can be applied with the modern Internet and related technologies.

At the time at which it was decided that having individuals in control of their personal information was the best way to protect their privacy in the context of the growing number of computers and electronic databanks (and the definition of *personal information* was elaborated), late 1960s and early 1970s, could the changes brought on by the Internet related technologies have been foreseen? It is doubtful.

I maintain that the recent changes triggered by the Internet and related technologies are important enough to suggest that we have entered a fourth wave, and that we should therefore be going back to the drawing board.

---

[350] Marshall Kirkpatrick, "Facebook Becomes More Racially Diverse, Ought To Release Data for Outside Analysis" (16 December 2009), online: ReadWriteWeb <http://www.readwriteweb.com/archives/facebook_scientists_dissect_facebook_say_its_alive.php>.

[351] See section 1.1.1.3 entitled "Third Wave: Control over Personal Information" and section 1.1.2 entitled "Control over Personal Information and Fair Information Practices" which elaborate on this issue. See also Radwanski, *supra* note 28 at 3.

[352] See Council of Europe, *Report on human rights*, *supra* note 42 at s. III, para. 11: "Most of these new technological and scientific developments which, if they are not subject to a sufficient control, are a great danger to human dignity and freedom, have occurred since the European Convention on Human Rights and most of the constitutions of the Council of Europe member States were drafted, and they could not be foreseen by their authors."

2. CONSTRUCTING THE DEFINITION OF PERSONAL INFORMATION

Mindful of the technological challenges detailed in section 1.2, we can not help but wonder if the concept of privacy as the "control of an individual over his or her personal information" is still relevant in our day and age. In section 2.1, entitled "Deconstructing the Definition of Personal Information", I will address the challenges with the notion of "control" and elaborate on how the notion of "personal information" also raises various issues. In section 2.2 entitled "Reconstruction Taking into Account Underlying *Risk of Harm*", I will propose to reconstruct the notion of *personal information* and interpret this notion in light of the ultimate purpose behind DPLs: protecting individuals against a *risk of harm* which may take place upon their information being collected, used and disclosed.[353]

2.1. Deconstructing the Definition of Personal Information

In this section, I will deconstruct the notion of privacy as "control of personal information". More specifically, I will discuss how this conception may place the right to privacy ahead of other rights or conflicting values, and how protecting too much information may interfere with the free flow of information, which may be beneficial to the society. I will address the challenges that we are now facing with this notion of "control" of information in an Information Age in which individuals are constantly being asked to provide their consent to various data handling activities without necessarily understanding the risks involved.

I will then discuss how the object of protection of DPLs, the notion of "personal information," also raises various issues when we use a literal interpretation. More specifically, I will discuss how this notion of *personal information* may prove to provide for an over-inclusive framework or an under-inclusive one, how this notion presents various uncertainties (as to which data qualifies as *personal*) and discuss how this notion may prove to be obsolete in certain situations.

2.1.1. Deconstructing the Concept of Privacy as Control

The conceptualization of privacy as "control over personal information" has given rise to a variety of privacy related concerns. As it is shown in section 1.2, the Internet and

[353] See section 2.2.2 entitled "Determining Risk of Harm as Purpose Behind the Protection of Personal Information" which elaborates on the ultimate purpose behind DPLs.

related technologies have triggered an increase in the volume of data available and the number of data exchanges; not to mention the development of new types of data and collection tools, new methods for identifying individuals, new uses for this data as well as an increased availability of data. Consequently, it is becoming increasingly difficult for an individual to actually *maintain* "control" over his or her personal information, especially online.

The Lindop Report (U.K. 1978) suggested that while protecting the interests of individuals is important, it is also very important to protect the interests of organizations handling personal information (and the interest of society at large):

> "The best interests of the individual often lie in the provision of data about himself (and similar provision by other individuals) rather than in the with-holding of such information. It is instructive to observe the alacrity with which personal data are supplied, for example, to derive a financial advantage, or to enjoy the privilege of public office. (…) It is therefore very much in the interests of individuals that the interests of those to whom data are provided are also protected, together with the interest of society at large."[354]

Many believe that conceptualizing privacy as "control over personal information" can be too vague, too broad, or too narrow.[355] Some may reject the control-based paradigm as it would be fundamentally misguided.[356] Others argue that this conception is simply

---

[354] Lindop, *supra* note 96 at 10, para. 2.08.

[355] Solove, "Conceptualizing", *supra* note 23 at 1114-15: "Conceptions of information control are too vague when they fail to define what types of information over which individuals should have control. When theorists attempt to define what constitutes 'personal information', the conceptions become overly limited or expansive. Further, when theorists attempt to define what 'control' entails, they often define it as a form of ownership, making the conception falter in a number of respects. Finally, conceptions of information control are too narrow because they reduce privacy to informational concerns, omit decisional freedom from the realm of privacy, and focus too exclusively on individual choice"; Solove refers to various authors which have criticized the privacy as control conception. Tom Gerety, "Redefining Privacy" (1977) 12 Harv. C.R.-C.L. L. Rev. 233 at 262-63. Gerety claims that Westin's definition "on its face includes *all* control over *all* information about oneself, one's group, one's institutions. Surely privacy should come, in law as in life, to much less than this"; Daniel A. Farber, "Book Review: Privacy, Intimacy, and Isolation by Julie C. Inness" (1993) 10 Const. Comment. 510 at 514; David O'Brien also criticizes the conception of "privacy as the control of information" for being too narrow, suggesting that privacy interests usually involve an individual's "freedom to engage in private activities" rather than the disclosure or nondisclosure of his or her information; Paul Schwartz argues that the conception of information control focuses too heavily on individual choice and wrongly assumes that individuals have the autonomy to exercise control over their personal data in all situations, an assumption that fails to recognize "that individual self-determination is itself shaped by the processing of personal data". See Paul M. Schwartz, "Privacy and Democracy in Cyberspace" (1999) 52 Vand. L. Rev. 1609 at 1661. See also section 2.2.2.1 entitled "Privacy and Data Protection are not One and the Same" which elaborates on this issue.

[356] Richard A. Posner, "The Right of Privacy" (1978) 12 Ga. L. Rev. 393 at 408: Posner rejects the control-based paradigm as it would be fundamentally misguided mainly because if its disregard for the economic efficiencies of data collection: "we have no right to control other people's thoughts. Equally, we have no

unrealistic.[357] Certain industry players claim that in the Information Age, the "blanket rule" provided by DPLs ("control over all personal information") is no longer workable and triggers unnecessary costs.[358]

I am of the view that since we are protecting all *personal information*, perhaps we are protecting too much information.[359] This translates into a burdensome framework under which consents for random data handling activities are being obtained from individuals, while reducing the relevancy of the consents which would in fact be necessary. I am of the view that it is reasonable to wonder whether, in this Information Age, this "control" conception of privacy still makes sense. I will first discuss how the control conception of privacy triggers a framework under which privacy is considered as an absolute right (ignoring the importance of data flow for the society and other countervailing values). I will then address the concerns which I have with the "notice and choice" approach.

2.1.1.1. Privacy as an Absolute Right

While the right to privacy is a very important one,[360] the very broad notion of privacy as "control over personal information" (the "control" definition of privacy), which is the

---

right, by controlling the information that is known about us to manipulate the opinions that other people hold of us. Yet this control is the essence of what students of the subject mean by privacy."

[357] Conseil de l'Europe, *L'autodétermination informationnelle*, *supra* note 20 at 26: "Ce souci de ne pas attenter, par le biais de la protection des données, à la liberté d'expression et d'opinion a jusqu'à présent été approché par quelques dispositions protectrices du travail des journalistes y compris 'électroniques'. Il apparaît de plus en plus que le problème est plus large dans la mesure où Internet offre à chacun (web logs, site personnel, etc.) d'affirmer son opinion et de faire part de ses activités y compris de ses relations avec des tiers". See also Trudel, "Privacy Protection", *supra* note 164 at 321: "Web 2.0 applications require greater user involvement as producers and suppliers of information. They make it all the more necessary to seek a theory that can situate privacy protection in a cyberspace environment that is slipping further and further away from prefabricated categories and theories inherited from a time when computer technology was seen by a certain elite as the realm of surveillance. The right to privacy is sometimes depicted as an overriding right to be protected from an infinity of constraints flowing from social life. This has been taken to such an extreme that, in order to evade the requirements of balance that flow from the right to privacy, we have come to use the notion of 'protection of personal life' to justify regulations inspired by people's desires to control information that displeases them."

[358] Microsoft Corporation, *Microsoft Response to the Commission Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data* (31 December 2009) at 5-6, online: <http://ec.europa.eu/justice_home/news/consulting_public/0003/contributions/organisations/microsoft_corporation_en.pdf>: "A more targeted approach to data protection will, we believe, become increasingly important in the era of online computing. As data flows increase in volume and complexity, the application of blanket rules will not make sense in many circumstances -- they will increase costs without meaningfully enhancing the protections provided to data subjects." See also section 2.1.2.1.1(d) entitled "Consequences of Over–Inclusiveness" which elaborates on this issue.

[359] See section 2.1.2.1.1 entitled "Potentially Over-Inclusive Definition" which discusses the fact that a literal interpretation of the notion of personal information may provide for an over-inclusive framework.

[360] See section 2.2.1.4.3(b)(i) entitled "Protecting Privacy is Important" which elaborates on this issue.

basis of DPLs around the world (as well as other policy instruments incorporating the FIPs)[361] results in protecting not only the privacy of individuals but also prohibiting the circulation of any kind of personal information on individuals. This concept therefore ignores the importance of the flow of data for society as a whole or the legitimate reasons for organizations collecting, using or disclosing personal information. Furthermore, this triggers the situation under which the right to privacy is placed ahead of other important rights and freedoms or competing values.

2.1.1.1.1. Ignoring the Importance of Information Flow For the Society

The concept of privacy as "control over personal information" would be too one-sided, as it would overlook the legitimate reasons for the public's interest in that information.[362] There are many reasons for favoring the collection, use and sharing of personal information, given that information flow is important and can be used to benefit society as a whole.[363] It is interesting to note that as early as 1980, the OECD expressed a desire to ensure that DPLs would not hamper the free flow of information across borders since this could cause serious disruptions in important sectors of the economy, such as banking and insurance.[364] In April of 1985, mindful of the social and economic benefits resulting from access to a variety of sources of information and of efficient and effective information services, Governments of OECD member countries adopted a *Declaration on Transborder Data Flows*, in order to outline the important role

---

[361] See section 1.1.2.2 which elaborates on this issue.

[362] Jeroen van den Hoven raises that the communitarian arguments to make more information on individuals available and to relativize privacy claims are often clear, straightforward and convincing. They refer to benefits to the community of having knowledge about its members freely available. See Van den Hoven, "Moral Wrong-doing", *supra* note 272 at 33; See also Stan Karas, "Privacy, Identity, Databases: Toward a New Conception of the Consumer Privacy Discourse" (2002) American University Law Review at 13.

[363] Many DPLs and data protection transnational policy instruments adopted for the last thirty or forty years (the OECD Guidelines, Convention 108, Directive 95/46/EC and the APEC privacy framework to name a few) already recognize the importance of free flow. See Convention 108, *supra* note 10 at Preamble, "Recognising that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples"; See EC, *Directive 95/46/EC*, *supra* note 99 at Whereas (3): "Whereas the establishment and functioning of an internal market in which, in accordance with Article 7a of the Treaty, the free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely from one Member State to another (…)"; Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005) at part. I, Preamble, s. 1 [APEC, Privacy Framework]: "(…) APEC economies realize that a key part of efforts to improve consumer confidence and ensure the growth of electronic commerce must be cooperation to balance and promote both effective information privacy protection and the free flow of information in the Asia Pacific region."

[364] See OECD, *Guidelines*, *supra* note 11 at Preface.

of the free flow of personal information in international trade.[365] In the United States, the government would be constitutionally prohibited under the First Amendment from interfering with the flow of information, except in the most compelling circumstances.[366]

Many authors outline the benefits of a society dominated by open information flows.[367] Personal information is necessary to provide and obtain public services.[368] We can think of the value in collecting, sharing and disclosing personal data in order to address national security concerns or to investigate and prosecute criminal activities.[369] The free flow of data would also be important in economic efficiency, as it would enable cost cutting in the private and/or public sector (by eliminating various inefficiencies).[370] For example, individuals with bad credit could be identified more easily, thereby protecting lenders as well as the financial system (i.e. the collective).[371]

Benefits associated with organizations moving to cloud computing include cost savings for businesses, as well as positive environmental impacts because of the energy-saving effects of server consolidation.[372]

---

[365] OECD, *OECD Declaration on Transborder Data Flows* (11 April 1985), online: OECD <http://www.oecd.org/document/60/0,3343,en_2649_34225_2373500_1_1_1_1,00.html>.

[366] Fred H. Cate, "The Changing Face of Privacy Protection in the European Union and the United States" (1999) 33 Ind. L. Rev. 173 at 180.

[367] *Ibid*. at 174: "My vision is dominated instead by the benefits we all share of a society dominated by open information flows, the wide range of valuable services that such flows make available, the broad array of steps that the very technologies and markets that Professor Krotoszynski laments make available to me to protect my privacy, and fear of burdensome and costly government regulation to protect privacy, such as Europe now enjoys"; See also Pierre Trudel and Karim Benyekhlef who suggest that personal information would be social data in the sense that their aggregation would be valuable to the society. Pierre Trudel & Karim Benyekhlef, "Approches et Stratégies pour Améliorer la Protection de la Vie Privée dans le Contexte des Inforoutes", in *Mémoire présenté à la Commission de la Culture de l'Assemblée Nationale dans le Cadre de son Mandat sur l'Étude du rapport quiquennal de la commission d'accès l'information* (Montréal : CRDP, Université de Montréal, 1997) at 4; See also Vincent Gautrais, "Introduction générale: Le défi de la protection de la vie privée face aux besoins de circulation de l'information personnelle" (2004) 9:2 Lex Electronica at 7-8: "Les renseignements personnels sont donc des outils indispensables à la réalisation d'une meilleure qualité de service qui passe bien souvent par un service personnalisé et donc très au fait des caractéristiques propres de la personne."

[368] Gautrais & Trudel, *supra* note 1, at 3.

[369] See section 1.2.4 which elaborates on this issue.

[370] Robinson et al., *supra* note 151 at 13.

[371] Ron A. Dolin, "Search Query Privacy: The Problem of Anonymization" (2010) 2:2 Hastings Science and Technology Law Journal 137 at 144.

[372] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change*: *A Proposed Framework for Businesses and Policymakers*, Preliminary Staff Report (December 2010) at 24 [FTC, Preliminary Staff Report].

Personal information would be increasingly used in healthcare, particularly in research and large-scale epidemiological studies.[373] Technological advancements provide for new ways to address health trends at an early stage. For example, Google suggests that it would be possible to use its search engine in correlation with the geographical region of given searches made (using IP addresses) in order to detect regional flu outbreaks early on. In 2008, Google launched a "Flu Trends" service,[374] which is basically a site that monitors increases in health-related searches in different parts of the world. The team behind the system published a research paper demonstrating that they can accurately predict the outbreak of a flu epidemic in a certain region before public health authorities catch on to it.[375] In 2009, Hal Varian, Google's chief economist, published a paper showing that Google searches can also be used to predict a bevy of economic data, including retail sales[376] and unemployment claims.[377] There may also be an interest in Google's ability to analyze search logs to detect large-scale computer security threats.[378] It has also been argued that preserving, and not anonymizing, online search queries would be ultimately beneficial to society:

> "Another example, perhaps just for curiosity, is what people are searching for in your local area. However, imagine looking for a signal that would indicate pending economic problems, such as a rise in several regions' queries about foreclosures or bankruptcies, and

---

[373] E.g. see CNIL, *2008 Annual Report of the Commission Nationale de l'Informatique et des Libertés* (Paris: CNIL, 2008) at c. 1 "Measuring Diversity: Ten Recommendations", discussed in Robinson et al., *supra* note 151 at 14.

[374] See online: <http://www.google.org/flutrends/>.

[375] Dolin, *supra* note 371 at 143: "For society at large, consider the following example from Google. Flutrends detects regional flu outbreaks two weeks before similar detection by the CDC by analyzing flu-related search terms such as 'flu' or 'influenza' in coordination with the geographical region as determined by IP addresses (though the data are anonymized prior to release in a similar way to census data). The work is accurate enough to have warranted publication in the well-known science journal Nature. (…) IP addresses can frequently yield geographical information down to the city or zip code level without identifying a user's identity. In principle, knowledge of a coming local flu outbreak can give people advance notice to get flu shots, wash hands more, etc., which can save lives. This tool was developed by looking over 5 years worth of non-anonymized data." See also, online: <http://www.nature.com/nature/journal/v457/n7232/full/nature07634.html>.

[376] Hal Varian & Hyunyoung Choi, "Predicting the Present with Google Trends" (2 April 2009), online: Google Research Blog <http://googleresearch.blogspot.com/2009/04/predicting-present-with-google-trends.html>.

[377] Hal Varian & Hyunyoung Choi, "Predicting Initial Claims for Unemployment Benefits" (22 July 2009), online: Google Research Blog <http://googleresearch.blogspot.com/2009/07/posted-by-hal-varian-chief-economist.html>.

[378] Manjoo, *supra* note 299: "when it notices anomalous collections of searches (which viruses have been known to perform to seek out vulnerable Web servers) it can stop viruses in their tracks. Then there's 'crowdsourced traffic'."

> imagine detecting that signal early enough to prevent a national or international economic crisis. It would require several years worth of data to be able to detect such a signal with sufficient reliability to be able to act on it. How many jobs or retirement funds could potentially be saved? Imagine comparing the spread of early domesticated plants and animals with the spread of ideas today. (…) If census data tells us who and where we are, then search queries tell us what we're thinking. Imagine what one could study with 100 years of search query data – non-anonymized. The assumption that such data are expendable is questionable at best, and certainly an odd determination to leave to the government; we give up a lot of value by deleting them rather than securely keeping them around."[379]

In 2005, the Article 29 Working Party drew criticism when it released its document on RFID technology and privacy, as societal benefits were overlooked when analyzing RFID applications.[380] Information would be useful in the development of new products and services. For example, the FTC in its recent 2012 Report suggested that: "the collection and use of consumer data has led to significant benefits in the form of new products and services."[381] Data flows may be beneficial to many individuals or society as a whole and it is reasonable to wonder if restrictions found in DPLs may have a limiting effect on this flow.

2.1.1.1.2. Ignoring Legitimate Reasons for Collecting, Using and Disclosing Information

There are various legitimate reasons for an organization collecting, using and disclosing personal information. The argument that individuals should be in "control" of their data at all times ignores the often legitimate reasons for such data handling activities.

Many online services require the collection of some type of personal information. ISPs need certain types of personal data in order to carry on their business of providing Internet access to their customers. Logs detailing the Internet traffic of account holders, may also be generated, including lists of online points of destination for legitimate

---

[379] Dolin, *supra* note 371 at 144.

[380] Article 29 Data Protection Working Party, *Results of the Public Consultation on Article 29 Working Document 105 on Data Protection Issues Related to RFID Technology*, [2005] 1670/05/EN at 2 [Article 29 Data Protection Working Party, *Results of the Public Consultation*]: "A repeated criticism of the paper is that the examples of RFID applications given in the paper do not represent reality. Societal benefits and a realistic appreciation of technical possibilities should be looked at when judging RFID applications."

[381] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (March 2012) at 2 [FTC, *Recommendations* 2012].

reasons such as billing, maintenance and monitoring.[382] Many websites use cookie-based technology for reasons that may be viewed as legitimate as well, such as: delivering user-specific solutions for each device that is accessing their web pages, to remember customization settings for individual users regarding content and layout, and to allow e-commerce sites to implement convenient shopping carts and "quick checkout" options.[383] It is also common for websites to keep a record of IP addresses of online visitors, keeping track of the total number of visitors, country of origin and choice of ISP; sometimes even as a security measure.[384] A majority of web portals and Internet companies would be severely limited or completely marginalized in the absence of *clickstream* data.[385]

Search engines collect and process vast amounts of user data including log files detailing use of search engine services (using technical means, such as cookies). These log files may include the content and history of search queries, the date and time, source (IP address and cookie), user preferences and data relating to the user's computer; data on the content offered (links and advertisements as a result of each query); and data on the subsequent user navigation (clicks).[386] Google claims to collect some of this data to improve its services,[387] to keep its services secure,[388] to protect its

---

[382] Amy Min-Chee Fong, "Unmasking the John Does of Cyberspace: Surveillance by Private Copyright Owners" (2005) 4:3 CJLT.

[383] Berman & Mulligan, *supra* note 204 at 554.

[384] For example, if a customer regularly accesses his account from an IP address in London, access to that customer's account from an IP address in Moscow might indicate fraud. See "IP addresses and the Data Protection Act" (March 2008), online: out-law.com <http://www.out-law.com/page-8060>.

[385] Wong & Garrie, *supra* note 187: "Elimination of clickstream data or cookies would impact such websites as: www.yahoo.com; www.google.com; www.wamu.com; www.schwab.com; www.ibm.com. Adjoining these web sites are a slew of Internet and web applications that utilize cookies and clickstream data for authentication. Elimination would impact not only businesses but also a large number of government enabled web applications." *See* The Office of the Privacy Commissioner, Guidelines for Federal and ACT Government Websites, Australia, providing guidance for the many government sites that use cookies and clickstream data technology.

[386] Article 29 Data Protection Working Party, *Opinion 1/2008*, *supra* note 207 at 6.

[387] Hal Varian, "Why data matters" (3 April 2008), online: Official Google Blog <http://googleblog.blogspot.com/2008/03/why-data-matters.html>.

[388] For instance, Google claims that it needs users data for improving security and fighting webspam. Web spam is junk that the user sees in search results when websites successfully cheat their way into higher positions in search results or otherwise violate search engine quality guidelines. See Matt Cutts, "Using data to fight webspam" (27 June 2008), online: Official Google Blog <http://googleblog.blogspot.com/2008/06/using-data-to-fight-webspam.html>: "The IP and cookie information is important for helping us apply this method only to searches that are from legitimate users as opposed to those that were generated by bots and other false searches. For example, if a bot sends the same queries to Google over and over again, those queries should really be discarded before we measure

users from *malware* or *phishing* attacks,[389] to detect and prevent advertising "click fraud", and for accounting requirements.[390]

Organizations may use cloud computing in order to achieve significant economies of scale by moving information (frequently personal information) across the globe between modular and reconfigurable data centres, often managed remotely.[391] Benefits also include positive environmental impacts because of the energy-saving effects of server consolidation.[392] Some may consider these reasons as legitimate ones.

Offline technology can also be used to collect information for legitimate purposes. For example, RFID tagging promises to deliver increased business efficiencies in every sphere of the retail industry from manufacturing, to pre- and post-sales applications, as well as payment and commercial transactions.[393] Commercial trucking companies and railways have long used RFID in tracking shipments, attaching RFID tags to pallets and containers, and even high-value parts which may be individually tagged because of their value.[394] In the pharmaceutical sector, the U.S. Food and Drug Administration has recommended RFID tagging of medications for safety purposes, arguing that by improving supply chain performance through widespread use of RFID technology,

---

how much spam our users see. All of this--log data, IP addresses, and cookie information--makes your search results cleaner and more relevant."

[389] Niels Provos, "Using log data to help keep you safe" (13 March 2008), online: Official Google Blog <http://googleblog.blogspot.com/2008/03/using-log-data-to-help-keep-you-safe.html>: "We analyze logs for anomalies or other clues that might suggest malware or phishing attacks in our search results, attacks on our products and services, and other threats to our users. And because we have a reasonably significant data sample, with logs stretching back several months, we're able to perform aggregate, long-term analyses that can uncover new security threats, provide greater understanding of how previous threats impacted our users, and help us ensure that our threat detection and prevention measures are properly tuned."

[390] For example, services such as clicks on sponsored links, where there is a contractual and accounting obligation to retain data, this data would be useful at least until invoices are paid and the period for legal disputes has expired. See Article 29 Data Protection Working Party, *Opinion 1/2008*, *supra* note 207 at 15-16.

[391] Cloud computing brings a new general architectural trend in the computer industry, moving from users doing computing on their own hardware using copies of software that they own, to users doing computing on other peoples' machines somewhere in the cloud, using software that they rent. See Mowbray, *supra* note 21 at 134.

[392] FTC, Preliminary Staff Report, *supra* note 372 at 24.

[393] In a manufacturing environment, RFID systems are routinely used for control of parts and logistics. Manufacturers track parts from the time they are produced until the assembled goods are to be sold. Hariton, Lawford & Palihapitiya, *supra* note 197 at 9.

[394] *Ibid*. at 10.

counterfeit drugs could be more easily prevented from reaching the market (since counterfeit drugs would not carry such records).[395] An analogy can also be made with the movement of "open data" which promotes the idea that certain data should be freely available to everyone to use and republish as they wish, without restrictions from copyright, patents or other mechanisms of control, which is being promoted by various academics including Danièle Bourcier.[396]

All of these examples illustrate that there are various legitimate reasons for the collection, use and disclosure of personal information or new types of data. Interestingly, in France, changes were recently made to the French DPL in order to allow for the processing of information for "legitimate" purposes without obtaining consent[397] and certain recent Canadian DPLs already provide for a "reasonableness" criteria.[398] These changes illustrate the necessity not to ignore the potential benefits of collecting and processing information, and further confirms the argument that individuals should not have absolute control of their personal information at all times.

2.1.1.1.3. Ignoring Countervailing Values

The concept of privacy as "control over all personal information" may end up placing the right to privacy over other important rights and values. The fact that the right to privacy is not an absolute right and that it may sometimes have to be balanced against other rights was already discussed back in the early 1970s:

> "We have also kept it constantly in mind that privacy cannot be an absolute right. A man's right to privacy has to be balanced against the rights of others; any additional protection which the law may afford to privacy may be found to impinge upon such other rights, in particular the right of free communication of the truth and of comment upon it, which are generally accepted as of great importance in a democratic society."[399]

---

[395] *Ibid*.

[396] Danièle Bourcier, *To Create Commons in order to Open Data* (CNRS and Creative Commons France, France).

[397] See *Loi informatique et liberté*, *supra* note 131, c. II; Conditions de licéité des traitements de données à caractère personnel s. 1: Dispositions générales art. 6, Modifié par la *Loi n° 2004-801 du 6 août 2004*, art. 2, J.O.R.F. 7 août 2004.

[398] See section 2.2.1.3.2(a)(i) entitled "Reasonableness or Legitimacy " which elaborates on this issue.

[399] *Report of the Committee on Privacy*, *supra* note 3 at 7, para. 23.

As Trudel states: "the right to privacy is not the only right relating to the Internet. It has to be weighed against other rights and freedoms".[400] When the right to privacy clashes with values that support restrictive treatment of the information flow, we then need to pursue trade-offs and balance.[401] There are at least a couple of values or rights (competing with privacy), which directly clash with the individual's right to control his or her personal information.[402] These include freedom of speech and the freedom of information or the public right to know.[403]

(a) Free Speech and Right to Speak about Others

While privacy can be useful in order to promote free speech (ideas and opinions being shared more openly), privacy can also compete against free speech, as illustrated by Trudel:

> "Clearly, as it is now applied, personal data protection law can oppose legitimate criticism of individuals with respect to their public activities and restrict circulation of information not related to an individual's private life. Yet, privacy protection on the Internet should reflect the social dimensions of activities that take place there, rather than favour an approach incompatible with transparency and public criticism. Human dignity is not protected by *de facto* prohibiting criticism of people's actions and behaviour."[404]

According to Trudel, when an individual engages in a public activity, he leaves his private life behind and unless we completely abandon freedom of expression, we cannot extend privacy protection to claim a veto over information relating to public

---

[400] Pierre Trudel, "La protection de la vie privée dans les réseaux: des paradigmes alarmistes aux garanties effectives" (2006) 61 *Annales des télécommunications* 950 at 957 [Trudel, "protection de la vie privée"], discussed in Trudel, "Privacy Protection", *supra* note 164 at 319-20.

[401] Nissenbaum, *supra* note 230 at 151.

[402] Conseil de l'Europe, *L'autodétermination informationnelle*, *supra* note 20 at 26: "Il arrive cependant que le souci de protection des données heurte le développement d'autres libertés." See also Karas, *supra* note 362 at 20: "The personhood rationale suffers from a certain high-minded focus on the value of privacy over other competing interests. (…) Similarly, where some see sale (i.e. publication) of personal information as a violation of dignity, others see an exercise of constitutionally enshrined First Amendment rights that are crucial to democratic society. (…) Needless to say, our society must the values of personhood and personal dignity. But it is sententious and imbalanced to define personhood rights so broadly that they trump other, equally legitimate social interests."

[403] For example, in the U.S., any restriction to the use of public information may run into First Amendment problems (free speech) and some difficult tradeoffs may have to be made between privacy and free expression (particularly in the form of commercial speech) as well as free access to public records.

[404] Trudel, "Privacy Protection", *supra* note 164 at 321 [footnotes omitted].

life.[405] One of the first governance tools that incorporated FIPs in the early 1980s, Convention 108, mentions the necessity to strike a balance between privacy and freedom of expression, but does not specifically provide the mechanisms needed to achieve it.[406] The difficulty in striking or addressing this balance was also discussed by the European Court of Justice in the 2003 *Linqvist* case.[407]

In the spring of 2010, the French government launched a public consultation on the "right to be forgotten" which would allow individuals to have information about them removed from the web;[408] as in many cases, information is stored potentially forever or at least with no specific time limit.[409] Google's CPO Peter Fleischer articulated the view that although the "right to be forgotten" is a great idea in theory, there is a thin line between the "right to be forgotten" and the "right of free speech" and that the former could be used to instead limit the scope of the latter (if used to censor information on the web*).*[410] Web 2.0 further complicates this issue, with blogs, OSNs and individuals sharing their opinions and thoughts online.[411] Trudel raises concern over DPLs being used by individuals to limit what can be said about themselves online, if they simply don't like it:

> "The right to privacy is sometimes depicted as an overriding right to be protected from an infinity of constraints flowing from social life. This has been taken to such an extreme that, in order to evade the requirements of balance that flow from the right to privacy, we have come to use the

---

[405] *Ibid*. at 323.

[406] Conseil de l'Europe, *L'autodétermination informationnelle*, *supra* note 20 at 17: "Il arrive cependant que le souci de protection des données heurte le développement d'autres libertés**.** En particulier, la protection des données doit être mise en balance avec les impératifs de protection de la liberté d'expression et d'opinion. Le préambule de la Convention le rappelle implicitement (…) sans qu'aucune disposition de la Convention n°108 ne consacre cependant explicitement la nécessité de cette mise en balance."

[407] See Flora J. Garcia, "Bodil Lindqvist: A Swedish Churchgoer's Violation of the European Union's Data Protection Directive Should Be a Warning to U.S. Legislators" (2005) 15 Fordham Intell. Prop. Media & Ent. L.J. 1206.

[408] RFI, "La France plaide pour le 'droit à l'oubli' sur internet" (15 November 2009), online : RFI <http://www.rfi.fr/contenu/20091115-droit-loubli-internet>.

[409] See section 1.2.5.2 entitled "Temporal Shift" which elaborates on this issue.

[410] Whitten & Fleischer, *supra* note 279 : "Peter Fleischer : Imaginer une charte sur le droit à l'oubli nous semble être une bonne approche. Nous sommes d'accord sur le fait qu'un effort important doit être fait en termes d'éducation. Là où nos points de vue divergent, c'est sur la frontière entre le droit à l'oubli et la liberté d'expression. Il est très difficile d'écrire une charte sur le droit à l'oubli sans que cela ne tourne à une possible censure. Si je mets en ligne une photo de quelqu'un, cette personne a-t-elle le droit de supprimer cette photo? Cela peut être évident dans certains cas, pas du tout dans d'autres."

[411] See section 1.2.1.2 entitled: "New Ways of Using the Internet: Web 2.0" which elaborates on this issue. See also Conseil de l'Europe, *L'autodétermination informationnelle*, *supra* note 20 at 26.

> notion of 'protection of personal life' to justify regulations inspired by people's desires to control information that displeases them."[412]

It was these issues (right to speak of others vs. privacy) which were at stake in the infamous French case of Note2be, in which the French Court ordered that a website on which students could rate their teachers stop processing personal (nominative) information.[413] Judge Richard Posner ("Posner"), who rejects the control-based paradigm as it would be fundamentally misguided (mainly because of its disregard for the economic efficiencies of data collection) suggests that we have no right to control other people's thoughts. Equally, we have no right to manipulate our public image by controlling information that is known about us.[414]

The "control" conception of privacy would also be challenged by the freedom of information, the freedom of the press as well as the right of the public to know, as discussed below.

(b) Freedom of Information and of the Press

Already in the beginning of the 1970s, it was acknowledged that the FIPs were potentially conflicting with other rights.[415] The 1973 Report of the Secretary's Advisory Committee on Automated Personal Data Systems (Scotland) raised that: "As a social value (…) privacy can easily collide with [other rights], most notably (…) freedom of the press, and the public's right to know."[416]

The protection accorded to privacy will vary. A certain piece of information of an "intimate" nature, may already be or, with time, become of public interest. The role and status of the individual in the society will play an important part in making this evaluation;[417] potentially creating a situation whereby the right to privacy of a public

---

[412] Trudel, "Privacy Protection", *supra* note 164 at 321.

[413] See: CNIL, "La CNIL se prononce : le site note2be.com est illégitime au regard de la loi informatique et libertés" (6 March 2008). See also: CA Paris, 25 June 2008, (2008) RG 08/04727 [CA Paris, RG 08/04727].

[414] Posner, *supra* note 356 at 408.

[415] *Report of the Committee on Privacy*, *supra* note 3 at 202-03, para. 653.

[416] See U.S. Department of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *supra* note 57.

[417] Trudel & Benyekhlef, *supra* note 367 at 7: "Le champ de protection de la vie privée varie principalement en fonction des personnes. En effet, comme les personnes ne jouent pas toutes le même rôle dans la

figure may be more limited than that of a random citizen.[418] Trudel and Benyekhlef take the position that by ignoring this potentiality, DPLs may become an obstacle to the free flow of information.[419] Trudel argues that the appreciation of the notion of public interest should therefore be at the core of the definition of privacy.[420] In order to address the need for some type of balance when facing conflicting rights (i.e. right to privacy vs. right of others to be informed) courts have developed the notion of the *expectation of privacy*.[421] Trudel and Benyekhlef believe that the legal system should acknowledge the public aspect of certain types of communications in cyberspace, while restricting the processing of personal information which would constitute a breach of privacy.[422]

***

As early as 1972, in the United Kingdom, the realization was made that striking a balance between privacy and freedom of speech/information was a difficult task[423] and that it was very doubtful whether a court was an acceptable arbiter to address an issue

---

société, ce qui est une information assimilable à un aspect de la vie privée pour l'une ne le sera pas forcément pour l'autre."

[418] See S.H. Abramovitch, "Publicity Exploitation of Celebrities: Protection of a Star's Style in Quebec Civil Law" (1991) 32 C. de D. 301; Jean-Marie Cotteret & Claude Emeri, "Vie privée des hommes politiques" (1979-80) 14 R.J.T. 335 ; Pierre Trudel, "Le rôle de la loi, de la déontologie et des décisions judiciaires dans l'articulation du droit à la vie privée et de la liberté de presse" in Pierre Trudel & France Abran, *Droit du public à l'information et vie privée : deux droits irréconciliables?* (Montréal : Éditions Thémis, 1992) 181 at 186, discussed in Trudel & Benyekhlef, *supra* note 367 at 7.

[419] *Ibid*. at 7.

[420] See Emmanuel Derieux & Pierre Trudel (eds.), *L'intérêt public, principe du droit de la communication* (Paris : Éditions Victoires, 1996).

[421] Trudel & Benyekhlef, *supra* note 367 at 9-10. See also Canada's Supreme Court in *Hunter v. Southam*, [1984] 2 S.C.R. 14 ; *Dyment*, *supra* note 107.

[422] Trudel & Benyekhlef, *supra* note 367 at 10: "Il faut donc un régime juridique des renseignements personnels qui reconnaît à la fois le caractère éminement public de certains contextes de communication dans le cyberespace mais qui en même temps balise les traitements d'informations personnelles qui sont constitutifs d'atteintes à la vie privée."

[423] *Report of the Committee on Privacy*, *supra* note 3 at 204, para. 658: "We have already referred to the need to balance the right of privacy against other and countervailing rights, in particular freedom of information and the right to tell the truth freely unless compelling reasons for a legal limitation of this right can be adduced. We have often found this balance difficult to strike. At every stage we have been conscious of differing judgments about the precise area of privacy which should be protected under each heading and about the considerations of 'public interest' which might be held in each case to justify intrusion and so on to override the right of privacy. These uncertainties are, no doubt, largely the consequence of the acknowledged lack of any clear and generally agreed definition of what privacy itself is; and of the only slightly less intractable problem of deciding precisely what is 'in the public interest' or, in a wider formulation, 'of public interest'."

of such public interest.[424] In order to partially address these issues, DPLs usually provide for an exception of the processing of personal information carried out solely for journalistic purposes or the purpose of artistic or literary expression.[425]

In this analysis, there will be no consideration regarding the proper method of striking a balance between privacy and various freedoms.[426] The approach which I propose in this thesis has to do with better targeting the information which is protected under DPLs, in order to ensure that information which was meant to be protected is in fact governed by DPLs. Therefore, any "balancing" of rights would take place only once we have determined that a certain piece of information actually qualifies as *personal information*. The present section simply illustrates how broad and potentially over-reaching the "control" conception of privacy actually is.

2.1.1.2. Notice and Choice Approach Challenged

The "control" conception of privacy is based on, among other things, disclosing the purpose of, and obtaining consent regarding the collection, use and disclosure of an individual's personal information. With such notice and consent, there would not be any violation of privacy.

DPLs usually require organizations to disclose to individuals their data protection practices and whether they are collecting personal information.[427] In Canada, PIPEDA states that the purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected[428] and that personal information shall only be collected by fair and lawful means.[429] In Quebec, an organization that collects personal information from an individual must inform them of the object of this collection.[430] There are similar notice requirements in Alberta[431] and in

---

[424] *Ibid*. at 11, para. 41.

[425] See for example, EC, *Directive 95/46/EC*, *supra* note 99 at art. 9; PIPEDA, *supra* note 63 at s. 4 (1) (c); Quebec DPL, *supra* note 110 at s. 1; B.C. DPL, *supra* note 115 at Part 1, s. 3 (2) (a) and (b);

[426] See section 2.1.1.1.3 entitled "Ignoring Countervailing Values" which elaborates on the fact that the right to privacy may sometimes come in conflict with other rights and freedom.

[427] See section 2.1.1.2.1 which elaborates on this issue.

[428] PIPEDA, *supra* note 63 at Schedule 1 (s. 5), principle 4.2 and principle 4.2.5.

[429] *Ibid*. at Schedule 1 (s. 5), principle 4.4.2.

[430] Quebec DPL, *supra* note 110 at s. 8.

[431] Alberta DPL, *supra* note 114 at Part 2, Division 3, s. 13 (1) (a) and see also s. 8 (3).

B.C.[432] Consistent with the Directive 95/46/EC on this issue, the French DPL mentions that personal data may be processed only if they have been collected in a licit and loyal manner.[433]

Certain Canadian or French DPLs have additional requirements. For instance, PIPEDA states that the disclosure must be in such a form that the individual can reasonably understand how the personal information will be collected, used and disclosed.[434] PIPEDA also requires that privacy policies provide information in a form that is generally understandable.[435]

Individuals usually also have to consent to the collection of their personal information under DPLs. For example, PIPEDA provides that the consent of individuals is required for the collection of personal information (except where inappropriate).[436] Under the Quebec DPL, consent to the collection of personal information must be manifest, free, and enlightened, and must be given for specific purposes.[437] The Alberta and the B.C. DPLs have similar consent requirements to the collection of personal information;[438] for instance, each forbids consent being obtained though deception.[439] France also has a consent requirement for the collection of personal data unless there is a legitimate interest on the part of the organization that does not violate the fundamental rights and liberties of the individual.[440] This consent has to be "express" when collecting sensitive data.[441]

---

[432] B.C. DPL, *supra* note 115 at Part 4, s. 10 (1).

[433] *Loi informatique et liberté*, *supra* note 131 at c. II, s. 1, art. 6 (1) and (2); EC, *Directive 95/46/EC*, *supra* note 99 at Whereas (28).

[434] PIPEDA, *supra* note 63 at Schedule 1, principle 4.3.2; Alberta DPL, *supra* note 114 at Part 2, Division 2, s. 8 (3).

[435] PIPEDA, *supra* note 63 at Schedule 1, principle 4.8.

[436] *Ibid*. at Schedule 1 (s. 5), principle 4.3.

[437] Quebec DPL, *supra* note 110 at s. 14.

[438] Alberta DPL, *supra* note 114 at Part 2, Division 2, s. 7 (1) (a); B.C. DPL, *supra* note 115 at Part 3, s. 6 (2) (a), (b), (c).

[439] Alberta DPL, *supra* note 114 at Part 2, Division 2, s. 8(2), s. 10 and Division 3, s. 11 (a); See also B.C. DPL, *supra* note 115 at Part 4, s. 11 and s. 12 (1) (a).

[440] *Loi informatique et liberté*, *supra* note 131 at c. II, s. 1, art. 6 (1), 7 (5).

[441] *Ibid*. at II, s. 2, art. 8 (I) and (II).

Paul Schwartz ("Schwartz") rightfully questions whether individuals are in fact able to exercise meaningful choices with regard to the handling of their personal information, given disparities in knowledge and power when bargaining over the transfer of their information.[442] Ryan Calo ("Calo") mentions that:

> "often, an individual has no idea that the information was even collected or, if she does, how it will be used. This fundamental tension plays out vividly in the context of online privacy. Many consumers have little idea how much of their information they are giving up or how it will be used."[443]

Michael Froomkin suggests that: "In theory, the parties to a transaction can always contract for confidentiality. This is unrealistic due because consumers suffer from privacy myopia: they will sell their data too often and too cheaply".[444]

I will first discuss how privacy policies are inadequate as a means to communicating choices to individuals. I will then elaborate on how the notion of consent is also challenged in light of the increase in the volume of players providing new products and services, of the dynamic aspect of privacy policies and business models, and due to the fact that technology is becoming increasingly sophisticated.

2.1.1.2.1. Inadequacy of Privacy Policies as a Means to Communicate Choices

Privacy policies are problematic as tools for protecting privacy for various reasons, namely the lack of understanding, among consumers, about the collection, use and disclosure of personal information.

(a) Policies are Overly Vague

Many privacy policies are vague about what information they collect, how the information will be used and how it will be disclosed.[445] In one French ruling, the privacy policy at stake was found to be inapplicable to consumers mainly for this

---

[442] See Schwartz, *Cyberspace*, *supra* note 355 at 1661.

[443] Ryan Calo, "The Boundaries of Privacy Harm" (2011) 86:3 Indiana Law Journal 1131 at 19 [Calo, "The Boundaries"].

[444] Froomkin, *supra* note 183 at 1502.

[445] Irène Pollach, "A Typology of Communicative Strategies in Online Privacy Policies: Ethics, Power and Informed Consent" (2005) 62:3 Journal of Business Ethics 221 at 228, 230-31.

reason.[446] Privacy policies often do not include sufficient information to allow for a truly informed decision on the part of the consumer.

Privacy policies are often ambiguous regarding the kind of data which is collected. Businesses managing personal information may capitalize on this ambiguity, by omitting to disclose the collection of IP addresses or other new types of data.[447] Alternatively, these businesses may disclose the collection but mention that the data in question is not *personal information* or refer to this data as "Non-PII". Given the general lack of awareness in the online community regarding new forms of behavioural tracking and targeting techniques, the lack of proper privacy disclosures becomes especially problematic.[448]

Privacy policies may also be very vague on the use which will eventually be made of the data. For example, online service providers may claim to use the data collected for broad purposes such as improving their products and services or enhancing the customer's experience.[449] The implication is that potential future uses of the information are too vast to enable individuals to make an adequate valuation.[450]

---

[446] See Trib. gr. inst. Paris, 1re chambre section sociale, 28 October 2008, Association Union Fédérale des Consommateurs Que Choisir vs. Amazon, available in French at <http://www.foruminternet.org/specialistes/veille-juridique/jurisprudence/IMG/pdf/tgi-par20081028.pdf>.

[447] See section 2.1.1.2.1(b) entitled: "Organizations Communicating their Practices in Conflict of Interests" and section 2.2.1.3.2(c) which elaborate on this issue.

[448] For instance, consumers are not always fully aware of the degree to which their online behaviour is tracked. See Article 29 Data Protection Working Party, *Opinion 2/*2010, *supra* note 191 at 22: "So far, the ways in which the industry has provided information and facilitated individuals to control whether they want to be monitored have failed. Notices provided in general terms and conditions and/or privacy policies, often drafted in rather obscure ways fall short of the requirements of data protection legislation." According to the PIAC, since consumers are unaware of the extent of behavioural targeting using their personal information, this precludes any real capacity to formulate a complaint. Their concern is that this would be a cruel catch-22 since certain DPLs such as PIPEDA is a complaints-driven regime. Public Interest Advocacy Centre, *2010 Consumer Privacy Consultations: Comments of PIAC on Behavioural Targeting* (15 March 2010) at 5, online: http://www.piac.ca/privacy/piac_comments_to_privacy_commissioner_of_canada_on_behavioural_targeting [PIAC].

[449] See Amazon.ca Privacy Notice, online: <http://www.amazon.ca/gp/help/customer/display.html/ref=footer_privacy?ie=UTF8&nodeId=918814> [Amazon.ca Privacy Notice]: "We use the information you provide for such purposes as (…) customizing future shopping for you, improving our stores (…)."; See Microsoft privacy policy, *supra* note 297, which states: "Microsoft collects and uses your personal information to operate and improve its sites and services. These uses may include (…) performing research and analysis aimed at improving our products, services and technologies". See Google privacy policy, *supra* note 297 which states: "Google only processes personal information for the purposes described in this Privacy Policy (…) such purposes include: (…) protect and improve our services; (…) and Developing new services". See Yahoo! Privacy

Finally, these privacy policies may also be nebulous when it comes to who the data will be shared with. Online businesses often sell or rent personal data about users to third parties or share this information with their marketing partners (as well as corporate affiliates and subsidiaries) in order to build more complete profiles about individual consumers; and often doing so quietly.[451] The KnowPrivacy report analysis of privacy policies found that while many businesses mention that they do not share data with third parties, what they mean by "third parties" is not clear.[452] They may be referring to companies which are not under the same corporate ownership or which are third party affiliates. Amazon and other online service providers may share customer data with "subsidiaries" or "affiliated businesses"[453] but rarely ever clarify who these parties are, and what kind of privacy business practices they follow.[454] Janet Lo shares similar concerns: "It is often unclear what a website means by the terms "affiliate," "third party" and "partner" as no definitions are provided."[455] The CPO of an organization operating a website claimed that they consider the advertising service company DoubleClick[456] to be a "marketing partner," and not a "third party".[457] Without providing a definitive distinction between the types of parties with whom data may be shared with,

---

Policy, *supra* note 228 which states: "Yahoo! uses information for the following general purposes: to customize the advertising and content you see, (…) improve our services (…)".

[450] Solove, "Privacy", *supra* note 1 at 1428: "The information remains in the control of the company, with no limitations on use". See also at 1452, Solove suggests that it is difficult, if not impossible, for an individual to adequately value her information because this value is linked to "uncertain future uses".

[451] For example, companies like Acxiom and Experian use cookies on their affiliate websites to gather data about users that surf their websites and sell this information to advertising networks to add to these networks' profiles about users. For example, data that these companies sell include income level, interests, age and gender. See Stephanie Clifford, "Your Online Clicks Have Value, for Someone Who Has Something to Sell" *New York Times* (25 March 2009), online: The New York Times <http://www.nytimes.com/2009/03/26/business/media/26adco.html>.

[452] Joshua Gomez, Travis Pinnick & Ashkan Soltani, *KnowPrivacy* (1 June 2009), online: <http://www.knowprivacy.org/report/KnowPrivacy_Final_Report.pdf>.

[453] See Amazon.ca Privacy Notice, *supra* note 449: "We share customer information only as described below and with subsidiaries (…) We work closely with our affiliated businesses."

[454] Solove, "Privacy", *supra* note 1 at 1428: "While the company insists that it will not share information with 'outsiders,' it does not explain who constitutes an 'outsider.' (…) Merely informing the consumer that data may be sold to others is an inadequate form of disclosure. The consumer does not know how many times the data will be resold, to whom it will be sold, or what purposes it will be used for."

[455] Lo, *supra* note 188 at 48.

[456] *DoubleClick* is an ad management and ad serving technology foundation for the world's buyers, creators and sellers of digital media. See online: <http://www.google.com/doubleclick/>.

[457] Gomez, Pinnick & Soltani, *supra* note 452 at 9.

consumers do not know the extent to which their personal information has been outsourced. [458]

In many instances, consent to data collection activities is granted despite the possibility, completely unbeknownst to the particular user in question, that personal information already on file may be correlated or aggregated with new data in order to form a more complete user profile. Julie Cohen ("Cohen") notes that "a comprehensive collection of data about an individual is vastly more than the sum of its parts."[459] Businesses can purchase more data about consumers in order to build better profiles.[460] For example, ChoicePoint has a business model focusing on the aggregation and sale of personal information by acquiring information from public records.[461] Therefore, the initial collection of data and the consent provided may not reflect the extent to which a given organization is "informed" about a given individual.

Similar issues can take place with RFID technology. For instance, with RFID chip systems, it is possible that a retailer will not think it necessary to include potential data matching capabilities in their notice to consumers; whereas RFID information may be matched against other personal information systems to produce a more detailed overall customer profile.[462]

The KnowPrivacy report[463] which discusses several reasons why privacy policies are ineffective, mentions the difficulty for consumers to understand policies.[464] Privacy polices would often be difficult to read and understand because of the use of legal jargon[465] and tiny font sizes.[466] Consumers may also overlook notices because they

---

[458] Lo, *supra* note 188 at 48.

[459] Julie E. Cohen, "Examined Lives: Informational Privacy and the Subject as Object" (2000) 52 Stan. L. Rev. 1373 at 1398 [Cohen, "Examined Lives"].

[460] In the KnowPrivacy report's analysis of privacy policies, they found that about a quarter of the websites expressly stated that they buy information about users from third parties to supplement data collected directly from their users. Gomez, Pinnick & Soltani, *supra* note 452 at 9.

[461] Lo, *supra* note 188 at 48.

[462] Hariton, Lawford & Palihapitiya, *supra* note 197 at 37: "Instead it is likely that the retailer may treat the RFID information as a discrete activity, although the ultimate goal is to combine it with information gathered from, for example, loyalty card programs or video surveillance footage."

[463] Gomez, Pinnick & Soltani, *supra* note 452.

[464] *Ibid*. at 11-12.

[465] Mark Hochhauser raises that: "a readability expert determined that, of sixty privacy notices examined, most were written at a third or fourth year college reading level, rather than the eighth grade level standard

are drafted in language that makes them appear to be marketing materials.[467] Policies may also be very long. For example, after the CIPPIC filed a complaint to the OPCC against Facebook in Canada, Facebook agreed to provide more details about its data handling practices and ended up with an extremely long policy.[468] Solove reports that "people will be given consent forms with vague fine-print discussions of the contractual default privacy rules that they are waiving, and they will sign them without thought."[469] The FTC, in its recent 2012 Report, articulated the view that: "privacy notices should be clearer, shorter, and more standardized to enable better comprehension and comparison of privacy practices."[470]

(b) Organizations Communicating their Practices in Conflict of Interests

Survey research shows that users falsely believe that privacy policies create strong legal protections and limits on data use.[471] Most consumers therefore do not bother to read them. Since organizations often draft very broad privacy policies regarding their use and sharing of the data collected, users end up granting a wide array of

---

typically used for notices to the general public". Mark Hochhauser, "Lost in the Fine Print: Readability of Financial Privacy Notices" (1 July 2001), online: Privacy Rights Clearinghouse <http://www.privacyrights.org/ar/GLB-Reading.htm>, discussed in Hoofnagle & Smith, *supra* note 82 at 5-6; FTC, Preliminary Staff Report, *supra* note 372. *See, e.g, 1st Roundtable, Remarks of Fred Cate, Indiana University Maurer School of Law*, at 280-81, at 6; Felicia Williams examined privacy policies of Fortune 500 companies and found that only one percent of the privacy policies were understandable for those with a high school education or less and thirty percent required a post- graduate education to be fully understood. See Felicia Williams, *Internet Privacy Policies: A Composite Index for Measuring Compliance to the Fair Information Principles* (2006) at 17, online: <http://www.ftc.gov/os/comments/behavioraladvertising/071010feliciawilliams.pdf>.

[466] Gautrais & Trudel, *supra* note 1 at 180-81: "Et la pratique quant à la manière de consentir est à cet égard déplorable. Car dans la mesure où le gestionnaire cherche à se protéger lui-même, sans considérer ni l'usager ni la finalité protectrice des lois vis-à-vis de ce dernier, il est différents travers quant au fond des consentements qui peuvent être trouvés. En premier lieu, de par les juridismes, de par la matière évoquée, les consentements sont d'une complexité remarquable qui rend la compréhension difficile au non spécialiste qu'est presque systématiquement l'usager. Une complexité découlant soit de la syntaxe, du choix des termes, tels que des adverbes imprécis, et d'autres choix linguistiques aussi. Ainsi, le résultat fait souvent que la lecture, qui est rendue fastidieuse, est en définitive inaccessible au commun des internautes."

[467] Hochhauser, *supra* note 465.

[468] See Facebook privacy policy dated September 2011, online: <http://www.facebook.com/about/privacy/>.

[469] See Solove, "Privacy", *supra* note 1 at 1454.

[470] FTC, *Recommendations* 2012, *supra* note 381 at viii, 61.

[471] Chris Jay Hoofnagle & Jennifer King, "What Californians Understand about Privacy Online" (3 September 2008), online: <http://ssrn.com/abstract=1262130 or http://dx.doi.org/10.2139/ssrn>; See Solove, "Privacy", *supra* note 1 at 1454. He discusses a study which found that consumers "do not read privacy policies because they believe that they do not have to; to consumers, the mere presence of a privacy policy implies some level of often false privacy protection".

permissions through a disclosure which they haven't read.[472] As disclosures become broader in scope, consent sometimes becomes a sweeping authorization. Solove posits that:

> "Consent is virtually meaningless in many contexts. When people give consent, they must often consent to a total surrender of control over their information."[473]

To make matters worse, organizations doing business online have every incentive to collect as much personal information as possible and be able to use this information as they wish.[474] With new business models based on "sponsored" services or greater customization, personal information is often viewed as a commodity.[475] Facebook is one example of a business model which has an economic incentive to gather as much information as possible about its users to help advertisers promote their goods and services. It was reported to have posted more banner ads than any other website in 2010.[476] This appetite for information leads to very nebulous disclosures and privacy policies attempting to entice people to relinquish information in exchange for a vague promise of little or no value.[477] Expanding on the idea of personal information as a

---

[472] Gautrais & Trudel, *supra* note 1 at 172-73: "Malheureusement, nous craignions que derrière la compréhension initiale du consentement, et afin de s'assurer que l'individu ait un contrôle sur les informations le concernant, il y ait dans la pratique actuelle un glissement vers une acceptation de l'individu à ce que les gestionnaire de renseignements personnels puisse utiliser comme il le souhaite, ou presque, lesdites informations." ; These authors refer to Steven I. Willborn, "Consenting Employees: Workplace Privacy and the Role of Consent" (2006) 66 Louisiana Law Review 975 at 979, discussed in Gautrais & Trudel, *supra* note 1 at 177: "Également, il est possible de s'interroger sur cette pratique qui veut que, via le consentement, on ne s'intéresse plus à la protection des renseignements personnels mais à la capacité dont dispose l'individu de refuser, mais plus souvent, d'admettre un certain usage de son espace personnel. Du consentement "protection" s'est donc opéré en pratique un glissement vers le consentement 'permission'. Un glissement qui parait aller à l'encontre de la raison d'être du consentement (…) Un glissement qui semble en violation des principes fondateurs derrière la notion de consentement en matière de protection des renseignements personnels voulant que l'individu dispose d'un certain contrôle, d'une certaine maîtrise, de ce qui le caractérise et de ce qui l'identifie."

[473] Solove, "Privacy", *supra* note 1 at 1426-27.

[474] Therefore, industry players may be viewed to be in a conflict of interest: they have every incentive to provide incomprehensible and broad privacy policies in order to keep as many business options open as possible.

[475] See section 1.2.4.1 entitled "New Business Models (Customization and Sponsored Services)" which elaborates on this issue.

[476] Crovitz, *supra* note 283.

[477] Malin, *supra* note 219 at 1: "In our driven society, there is an ever-increasing demand for the incorporation of new technologies to gather data on people for a variety of worthwhile endeavors. Concurrently, data collections have become commodities that can be shared, licensed, or sold for profit in many different communities. This is possible because both data subjects and data collectors consider these fragments innocuous. They often harbour the belief that their pieces of data are isolated and no one could systematically relate identity to them without a central registry to query."

commodity and online businesses being in a conflict of interest when preparing their privacy policies, Schneier states:

> "Here's the problem: The very companies whose CEOs eulogize privacy make their money by controlling vast amounts of their users' information. Whether through targeted advertising, cross-selling or simply convincing their users to spend more time on their site and sign up their friends, more information shared in more ways, more publicly means more profits. This means these companies are motivated to continually ratchet down the privacy of their services, while at the same time pronouncing privacy erosions as inevitable and giving users the illusion of control. (…)"[478]

To better illustrate his statement, Schneier suggests that we can see these forces in play with Google's launch of Buzz.[479] The privacy default settings were set so that Gmail users would follow the people they corresponded with most frequently, and this list of "followers" was made publicly available.[480] While users could change these options, the process was a difficult one and therefore, most people probably accepted the default settings.[481] In December 2009, Facebook changed its default privacy settings in order to make profiles more public.[482] While users could, in theory, keep their previous settings, it took an effort and many people clicked through the new defaults without even realizing it. Furthermore, in March 2010, Facebook announced new privacy changes that made it easier for location data to be collected and sold to third parties.[483] Finally, in June 2011, Facebook was criticized for launching its facial recognition feature through an "opt out" type consent instead of an opt-in consent,

---

[478] Bruce Schneier, "Google And Facebook's Privacy Illusion" (6 April 2010), online: Forbes.com <http://www.forbes.com/2010/04/05/google-facebook-twitter-technology-security-10-privacy.html> [Schneier, "Privacy Illusion"].

[479] Buzz is a Twitter-like chatting service. See online: <http://www.google.com/buzz>.

[480] Molly Wood, "Google Buzz: Privacy nightmare" *Cnet News* (10 February 2010), online: cnet.com. <http://news.cnet.com/8301-31322_3-10451428-256.html#ixzz1XIwhyWHP>; Nicholas Carlson, "WARNING: Google Buzz Has A Huge Privacy Flaw" (10 February 2010), online: Business Insider <http://www.businessinsider.com/warning-google-buzz-has-a-huge-privacy-flaw-2010-2#ixzz1XIxQ9N8V>.

[481] Schneier, "Privacy Illusion", *supra* note 478.

[482] Kevin Bankston, "Facebook's New Privacy Changes: The Good, The Bad, and The Ugly" (9 December 2009), online: The Electronic Frontier Foundation <https://www.eff.org/deeplinks/2009/12/facebooks-new-privacy-changes-good-bad-and-ugly>.

[483] Michael Richter, "Another Step in Open Site Governance" (26 March 2010), online: The Facebook Blog <http://blog.facebook.com/blog.php?post=376904492130>.

requiring once again some effort from users who did not want to use this new feature.[484]

These examples simply illustrate the shared incentive for businesses active on the web to collect as much data as possible and to disclose as little as possible (or at least to remain extremely vague in their privacy policies).

(c) High Volume of Privacy Policies are Not Read

As people make their way through their daily lives, they leave behind fragments of information in various databases.[485] Individuals may not even be aware they are shedding any information. This phenomenon is being exacerbated by our driven society, with an ever-increasing demand for the incorporation of new data gathering technologies.[486] To provide only a few examples: images of automobiles are recorded on various highway video cameras; the IP address of a personal computer is logged at multiple websites; and, a patient's DNA can be sequenced and recorded in numerous hospital databases.[487]

Vincent Gautrais ("Gautrais") and Trudel agree that online users are relinquishing too much control over their personal information.[488] Ostensibly, users are being flooded with privacy policies and are becoming increasingly complacent when faced with consent requests. A problem thus may arise if highly sensitive data is targeted by data collection or consent requests. Gautrais and Trudel's view is shared by other authors, such as Tholas Olsen and Tobias Mahler:

> "However, providing the user with a lot of information regarding the processing of personal data may paradoxically be a burden for the user because it encourages or requires the user to stop and reflect on the relevance of the information. Consequently, there seems to be a more general tension between the goal of providing a seamless user experience and information requirements to ensure the principles of self-determination. If seamlessness leads to a non-transparent service,

---

[484] Hamish Barwick, "Facebook facial recognition should be opt in, not opt out" (10 June 2011), online: Computerworld <http://www.computerworld.com.au/article/389810/facebook_facial_recognition_should_opt_opt/>.

[485] See Malin, *supra* note 219 at 1.

[486] *Ibid*.

[487] *Ibid*.

[488] Gautrais & Trudel, *supra* note 1 at 179-80.

> where the user does not know who can process his information and for what purposes, then it is questionable whether total seamlessness is at all desirable. From the perspective of data protection, a seamless integration of services should still ensure that the user can make informed decisions about how and by whom he or she wants personal information to be processed."[489]

The issue with a consent or choice-based approach is the fact that, with the volume of data exchanges and collections taking place in the modern society,[490] individuals would be faced with the prospect of constantly reviewing privacy policies and consenting to them throughout any given day.[491] It is not reasonable to expect the average person to devote large portions of their time in order to process and provide meaningful responses to consent requests. In a recent study performed by the University of California, only 14 per cent of participants said that they often read privacy policies on websites, 36 per cent said they read the policies sometimes, while 50 per cent read them rarely or not at all.[492] The FTC, in its recent 2012 Report, states that:

> "The "notice-and-choice model," which encouraged companies to develop privacy policies describing their information collection and use practices, led to long, incomprehensible privacy policies that consumers typically do not read, let alone understand."[493]

---

[489] Thomas Olsen & Tobias Mahler, "Identity Management and Data Protection Law: Risk, Responsibility and Compliance in 'Circles of Trust'" (2007) at 26-27, online: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1015006>.

[490] See section 1.2.1.1 entitled "Increase in Storage Capabilities, Number of Users and Exchanges" and section 1.2.1.2 entitled "New Ways of Using the Internet: Web 2.0" which elaborate on this issue.

[491] In the study by Aleecia McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies* (CyLab, Carnegie Mellon University, 2008) the study estimated that if users actually read privacy policies, it would take approximately 200 hours a year to read the policy for every unique website visited in a year, not including policy updates for sites visited on a repeating basis; Lawrence Lessig notes that our existing system of posting privacy policies and enabling consumers to opt in or out has high transaction costs because people do not have "the time or patience to read through cumbersome documents describing obscure rules for controlling data." See Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999) at 160; See also Hoofnagle & King, *supra* note 471.

[492] CBC, "Internet privacy attitudes shifting: report, Learning about privacy issues raises level of concern" (16 April 2010), online: CBC News <http://www.cbc.ca/consumer/story/2010/04/16/con-online-privacy.html>.

[493] See, e.g., 1st Roundtable, Remarks of Marc Rotenberg, Electronic Privacy Information Center, at 301; 1st Roundtable, Remarks of Leslie Harris, Center for Democracy & Technology, at 36-38; 1st Roundtable, Remarks of Susan Grant, Consumer Federation of America, at 38-39, discussed in FTC, *Recommendations* 2012, *supra* note 381 at 2.

Last but not least, authors have articulated the view that even if consumers could understand and had the time to read privacy policies, that there is not enough market differentiation for users to make informed choices.[494]

So, individuals don't read policies because they don't know that they are disclosing data or because they don't have the time or won't take the time to do so. Since they may be granting far-reaching permissions by approving consent requests, consumers can be said to have lost control over their personal information. Who can claim to have read every single privacy policy before signing up for a service on the Internet? All it takes is one click, and the individual may have lost this "control" forever as suggested by a U.K. blog which states that:

> "(…) if we are honest we have to recognise that we have lost control over our information, regardless of any data protection law that is passed or will be passed, the genie is out of the bottle, information replicates and strives to be free".[495]

Without proper notices and informed consents, individuals may not be in control over their *personal information*.

2.1.1.2.2. Consent Challenged by Technological Changes

The previous section illustrates how ineffective current privacy policies are, especially on the web, as these statements are rarely ever read, are often confusing and are incapable of capturing the complexity of modern data-handling practices. As a result, experts say, consumers typically have little meaningful choice about the online use of their personal information. As Cohen correctly notes: "freedom of choice in markets requires accurate information about choices and other consequences, and enough power—in terms of wealth, numbers, or control over resources—to have choices."[496] The FTC recently articulated the view that : "consumers generally lack full understanding of the nature and extent of (…) data collection and use and, therefore, are unable to make informed choices about it."[497]

---

[494] In the study by McDonald & Faith Cranor, *supra* note 491.

[495] Andres, "Information self-determination in the Google Age" (19 April 2010), online: Technollama Blog <http://www.technollama.co.uk/information-self-determination-in-the-google-age>.

[496] Cohen, "Examined Lives", *supra* note 459 at 1396.

[497] FTC, *Recommendations* 2012, *supra* note 381 at 2.

In order to claim a valid consent, the individual must be properly informed and understand what information is collected, how this information will be used and to whom it will be disclosed. The consent must also be freely given, specific and constitute an informed indication of the individuals' wishes. Due to lack of understanding about the collection, use and disclosure of their personal information, consumers are then incapable of making informed choices.

In certain cases, exercising choice also means losing certain benefits, such that the consumer in question may be in a lose-lose scenario. For instance, if a Google user "opts-out" of online behavioural tracking, they may still be tracked but will not gain the benefit of receiving targeted or customized ads.[498] Some are taking the position that consent obtained by Google for its behavioural marketing activities is not informed consent.[499] Others believe that there is "a need for a much higher original threshold of consent in privacy law than in contract law."[500] There are many situations in which people affirmatively give out information that should not be assumed to be consensual. Individuals must often disclose their personal information to gain employment, procure insurance, obtain a credit card, or otherwise participate like a normal citizen in today's economy.[501]

Another issue is the fact that too many choices create a similar burden for individuals, with a similar perverse effect. Facebook has been criticized for providing too many

---

[498] Chris Jay Hoofnagle, "The privacy Machiavellis" (25 May 2010), online: <http://www.sfgate.com/cgi-bin/article.cgi?f=%2Fc%2Fa%2F2010%2F05%2F24%2FED101DJPE1.DTL> [Hoofnagle, "Machiavellis"]: "Yet, you have no way to ask Google to stop this tracking. Instead, you can merely opt-out of the targeted advertising - the product recommendations. Exercising your privacy options creates a worst-case-scenario outcome: If you opt out, you are still tracked, but you do not receive the putative benefit of targeted ads."

[499] PIAC, *supra* note 448 at 5 [footnotes omitted]

[500] Ian R. Kerr et al., "Soft Surveillance, Hard Consent" (2006) 6 Personally Yours 1, discussed in Gautrais & Trudel, *supra* note 1 at p. 172-73.

[501] In the context of many online or offline services which would only be provided after sufficient personal data is released, with the consequence of the refusal of the providing of important services are denied if we are unwilling to supply that data, it is difficult to claim that individuals still have a real choice. See Robinson et al., *supra* note 151 at ix; See also Pomerance, *supra* note 233 at 284: "To make matters worse, it is impossible to sidestep this reality as a functioning member of society. Many daily activities require, as a condition precedent, that we surrender personal information about ourselves. For example, anyone who has tried to function without a credit card can attest to the difficulties they have encountered in accomplishing such basic tasks as booking a hotel room." See also Waldo, Lin & Millet, *supra* note 6 at 3: "To an unprecedented degree, making personal information available to institutions and organizations has become essential for individual participation in everyday life. These information demands have increasingly appeared in licensing; administration and conferring of government or private sector benefits to particular classes of people (e.g., veterans, the unemployed, those with low income, homeowners); providing of services; employment; and retailing."

choices.[502] Control of profile pages is becoming very complex due to complicated privacy settings. The 2010 Facebook privacy policy provided for 50 different settings and 170 different options.[503] As a matter of fact, by offering too many choices, individuals are likely to choose poorly.[504]

There are some DPLs (including certain Canadian and French DPLs), which employ a "reasonable test" (or some type of subjective test) in evaluating the notion of adequate disclosure and consent.[505] In Canada, Bill C-12, a new piece of federal legislation that would amend PIPEDA was introduced in 2011 and proposes to specify the elements of valid consent.[506] The following new provision was proposed, among many others, stating that: "the consent of an individual is only valid if it is reasonable to expect that the individual understands the nature, purpose and consequences of the collection, use or disclosure of personal information to which they are consenting".[507] Clearly then, the raison d'être of such a provision emerges from the fact that the notion of "consent" is now becoming obscured.

This obscurity is increased by the following three elements: the volume of players involved, the dynamic aspect of privacy policies and business models and the fact that technologies are becoming too sophisticated to enable individuals to properly evaluate the risks related to their consent to a given data handling activity.

---

[502] Hoofnagle, "Machiavellis", *supra* note 498.

[503] Asher Moses, "Facebook users 'don't want complete privacy': Zuckerberg" (24 May 2010), online: theage.com <http://www.theage.com.au/technology/technology-news/facebook-users-dont-want-complete-privacy-zuckerberg-20100524-w54g.html>.

[504] Hoofnagle, "Machiavellis", *supra* note 498: "Consider Facebook's privacy options. Regulators in the United States have long called for companies to give users choices to control personal data. Facebook can proudly proclaim that it offers these choices - more than 100 of them. Therein lies the trick; by offering too many choices, individuals are likely to choose poorly, or not at all."

[505] See section 2.2.1.3.2(a)(ii) entitled "Subjectivity in Type of Notices Provided and Method of Obtaining Consents " which elaborates on this issue.

[506] Bill C-12*, An Act to amend the Personal Information Protection and Electronic Documents Act*, 1st Sess., 41st Parl., 2011 [*Safeguarding Canadians' Personal Information Act*] aimed to amend PIPEDA, was re-introduced by the Government of Canada on September 29, 2011. This bill proposes amendments related to, among other things, breach notification, business transactions and disclosures to law enforcement. If enacted, this bill would require organizations governed by Canada's private sector data protection legislation to notify the federal Privacy Commissioner of any material privacy breaches involving personal information. This Bill is a copy of the previous Parliament's breach notification Bill C-29, which died on the order paper.

[507] Bill C-12 inserts a new section 6.1, clarifying that individuals' consent to collection, use or disclosure of their personal information is valid only if "it is reasonable to expect that the individual understands the nature, purpose and consequences of the collection, use or disclosure to which they are consenting" (clause 5).

(a) Increase in Volume of Industry Players Involved

Information and communication technologies and globalization have created structural and organizational changes which have influenced DPLs; including greater diversification within business groups and the growth of joint ventures, including loyalty programs. These developments are blurring the traditional boundaries between legal entities, such that it is becoming increasingly difficult to conclusively identify the owner or custodian of any particular piece of information. On this issue, Nigel Waters states:

> "In the course of conducting privacy reviews or audits it is often very difficult to get some managers to even understand the concept of custodianship of data, which is often seen as a shared, common resource to be used or 'mined' for different purposes and different beneficiaries."[508]

In the U.S., the *Gramm-Leach-Bliley Act*[509] ("GLBA") allows a broad spectrum of institutions to affiliate and operate under a single corporate umbrella, called a "financial holding company". This grouping has drawn criticism for the reason that financial institutions engage in a wide range of activities and compile vast amounts of information about their customers.[510] Affiliates may include banks, insurance companies, securities firms, as well as institutions that engage in significant financial activities, such as retailers that issue credit cards, auto dealerships that lease vehicles, and entities that appraise real estate. The GLBA allows all of these companies to merge their customers' data (which may include financial, medical and other sensitive information) into one comprehensive database. Some of these financial holding companies have thousands of affiliates making it very hard for consumers to know which organizations have access to their personal information let alone how their data is being used.[511]

If such organizations are not forthcoming about what kinds of data are being shared and who they are being shared with, individuals will have no way of knowing who may

---

[508] Nigel Waters, "Rethinking information privacy: a third way in data protection?" (2000) PLPR 6, online: <http://www.austlii.edu.au/au/journals/PLPR/2000/6.html>.

[509] Statute (*Public Law* 106-102, 15 U.S.C. § 6801, et seq.) enacted November 12, 1999.

[510] Hoofnagle & Smith, *supra* note 82 at 4-5.

[511] CitiGroup, Inc., for example, has over 2700 corporate affiliates. See US, *Financial Privacy and Consumer Protection Hearing Before the Senate Comm. on Banking, Housing and Urban Affairs*, 107th Cong. (2002) (statement of William H. Sorrell, Attorney General, State of Vermont); Bank of America has almost 1500 corporate affiliates.

have had access to their personal information. This is especially problematic if information is misused by an institution's affiliates or marketing partners since individuals may well have trouble identifying the offender.[512]

Personal information is constantly acquired, stored and disseminated by governmental and private agencies, often transferred without the owner's permission or knowledge. Even if an individual is aware of such a transfer, this does not always imply a full appreciation of the consequences. As noted in one report: "Citizens may be aware that they suffer harm from the circulation of computerized information about them, but they usually cannot reconstruct the connection between cause and effect."[513] Solove takes it a step further and articulates the view that even "opt-in" consent will not properly address this issue.[514]

The interaction between data controllers and data processors is essential in the application of certain DPLs (such as Directive 95/46/EC) since they influence who will be responsible for compliance with data protection rules and how individuals can exercise their rights. However, the increasing complexity of the environment in which these concepts are used has given rise to new and difficult issues. In February of 2010, the Article 29 Working Party issued an opinion emphasizing the need to allocate responsibility between data controllers and data processors so that compliance with DPLs is upheld sufficiently.[515] This problem may also be raised as an obstacle to the "Droit à l'oubli" (right to be forgotten) which has been proposed in certain jurisdictions such as France.[516] Under the *Droit à l'oubli*, an online user could request a website operator to delete his or her personal information posted online. Some could argue,

---

[512] Hoofnagle & Smith, *supra* note 82 at 5.

[513] Electronic Privacy Information Centre & Privacy International, *Privacy and Human Rights 2002: An international Survey of Privacy Laws and Developments* (Washington, D.C., London, U.K.; Electronic Privacy Information Center, Privacy International, 2002), discussed in Pomerance, *supra* note 233 at 278.

[514] Solove, "Privacy", *supra* note 1 at 1469: "Even with an opt-in system, steps must be taken to ensure that consent amounts to more than a "notice and choice" system, which as Marc Rotenberg argues, 'imagines the creation of perfect market conditions where consumers are suddenly negotiating over a range of uses for personal information.' This problem, which Julie Cohen terms the 'privacy-as-choice model' and which Paul Schwartz terms the notion of 'privacy-control,' emerges because of information inequalities between individuals and the bureaucracies that collect and use data, and because of an individual's lack of meaningful choices over the uses of her personal information."

[515] See Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of "controller" and "processor"*, [2010] 00264/10/EN, WP 169, online: <http://www.cbpweb.nl/downloads_med/med20100219_C.03%20DC-DP_Opinion_ADOPTED.pdf>.

[516] RFI, *supra* note 408.

however, that it may be very difficult for a user to track down all of the parties which have had access to their data.

Organizations may be sharing personal information collected from online visitors, especially those from jurisdictions which have no DPLs governing the transfer of personal information.[517] More organizations are now outsourcing part of their operations across multiple borders, and are partnering, off-shoring and entering into complex relationships with partners that are either collecting, using or storing the personal information on their behalf.[518] Globalisation and the constant drive for competitiveness means that personal data is moved where it is most efficient and effective for the organization, sometimes using cloud services.[519] In a paper published on information ownership "in the cloud", Chris Reed illustrates the new kinds of challenges that can arise in identifying the owner, controller or custodian of certain pieces of personal information, in light of new technologies and business models.[520] This represents yet another challenge to the concept of individuals having "control" over their personal information.

(b) Dynamic Aspect of Privacy Policies and Business Models

Many organizations and industry players may change their privacy policies, making it even more difficult to keep track (i.e. "control") of data handling practices.[521] They also often reserve the right to unilaterally change the terms and conditions of their privacy policy, at any time (so privacy policies are frequently modified with little or no warning). If consumers want to know the precise nature of the modification, it is often up to them to review the new version and "figure it out" for themselves; which can prove to be next

---

[517] For example, in the U.S., the *USA Patriot Act*, Public Law 107-56, Stat. 115 Stat. 272 (2001), which gives federal authorities much wider latitude in monitoring Internet usage and expands the way such data is shared among different agencies has brought many privacy concerns. See complaints files in Canada pertaining to these concerns: OPCC, *PIPEDA Case Summary #394, Outsourcing of canada.com e-mail services to U.S.-based firm raises questions for subscribers* (19 September 2008); OPCC, *PIPEDA Case Summary # 333, Canadian-based company shares customer personal information with U.S. parent* (19 July 2006); and OPCC, *PIPEDA Case Summary* #313, *Bank's notification to customers triggers PATRIOT Act concerns* (19 October 2005).

[518] Robinson et al., *supra* note 151 at 13.

[519] *Ibid*.

[520] Chris Reed, "Information 'Ownership' in the Cloud'" (2 March 2010), online: SSRN <http://ssrn.com/abstract=1562461>.

[521] For example, many privacy policies indicate that they may change from time to time and the users are requested to check back periodically.

to impossible for the average person. Certain authors suggest that changes made to a privacy policy should only affect the personal information collected going forward and that individuals should be notified of any changes.[522] All this to say that the business practice of unilaterally modifying privacy policies makes it even more difficult for individuals to keep control over their information. In the end, changes in privacy policies may create situations whereby personal information is transferred to unknown third parties without the knowledge or consent of interested parties.

Not only do privacy policies change, business models often do as well. For instance, Facebook and Google have changed their products ever so slowly and consumers are therefore less likely to perceive the change.[523] It is therefore even more difficult for online users to keep track of their personal data.

(c) Technology Becoming Increasingly Sophisticated

New types of data and new types of collection tools are becoming more complex, creating additional challenges. For example, the potential risks posed by online behavioural tracking and advertising practices are not known to most users. These users are also not aware of the type and amount of personal information collected by the websites they visit, nor the extent of tracking that companies and third party advertisers are engaging in when they surf the Internet.[524] For example, in a recent survey pertaining to whether Canadian consumers believe a "Do Not Track List" would be desirable, the first question asked respondents to identify their level of familiarity with the existence of tracking devices and techniques such as persistent cookies and web beacons. Overall, half of the respondents were not very familiar or not at all

---

[522] Gratton, *Internet and Wireless Privacy*, *supra* note 193: "A major concern about privacy policies is what happens to the information that has already been collected when the privacy policy is modified or the company is merged or acquired by another one that has different information practices. (…) Given that a privacy policy is a promise made to the online user, the e-Business cannot modify its terms without first notifying the online user and obtaining his/her consent. In the event that the user refuses to agree to the changes, the personal information already collected by the e-Business prior to the notice of change should be preserved under the prior policy terms. Hence, when a web site changes its privacy policy, the suggested approach is to ensure that the change will only apply to information that is collected from that point forward."

[523] Hoofnagle, "Machiavellis", *supra* note 498: "Facebook became a trusted brand by presenting itself as a private club of peers. Meanwhile, the site was changing settings and revealing more personal information to more people. Google used to tout its search engine advertising as privacy friendly, because it focused upon users' interests per-transaction, rather than through an analysis of past searches and browsing. But in 2007, Google quietly began behavioral profiling, tracking searches, and, with the acquisition of DoubleClick, nearly all browsing behavior."

[524] Lo, *supra* note 188 at 59.

familiar with the technologies.[525] In a complaint filed in the U.S. by three advocacy organizations with the FTC, demanding that it investigate and impose drastic requirements on entities involved in online data analytics and behavioral advertising, it was argued that the "compilation and analysis of data on users in real time involve highly sophisticated data mining technologies that few users—and likely regulators!—understand."[526]

Although individuals are aware that there are some risks involved with data collection when they are active on the web, these risks are only potential to them, not very visible, and not quite quantifiable. Therefore, individuals would not be motivated to refuse to sign up to online services or to stop disclosing their personal information on OSNs or other online blogs. Trudel suggests that a concern comes from the fact that the consequences of information circulation are often unbeknownst to stakeholders when information is initially put into circulation on the Internet.[527] It is often the agglomeration of information that may be viewed as problematic. Solove shares similar views and believes that it is difficult for a given individual to attribute a meaningful value to specific pieces of personal information.[528] In a recent article, Solove and Schwartz discussed the common myth about anonymity on the Internet as many people wrongly assume that anonymity is the norm in cyberspace.[529]

---

[525] The responses varied, with 20% of total respondents very familiar, 30% of respondents somewhat familiar, 19% not very familiar, and 31% not at all familiar with the technologies. *Ibid*. at 10.

[526] The U.S. Public Interest Research Group ("U.S. PIRG"), the Center for Digital Democracy and the World Privacy Forum target Google, Yahoo!, BlueKai, PubMatic, TARGUS info and others for allegedly participating in what the U.S. PIRG terms a "Wild West" of online collection and auctioning of data for marketing purposes. U.S., Federal Trade Commission, *In the Matter of Realtime Targeting and Auctioning, Data Profiling Optimization, and Economic Loss to Consumers and Privacy, Complaint, Request for Investigation, Injunction, and Other Relief: Google, Yahoo, PubMatic, TARGUSinfo, MediaMath, eXelate, Rubicon Project, AppNexus, Rocket Fuel, and Others* (Washington, D.C., 8 April 2010).

[527] Trudel, "Privacy Protection", *supra* note 164 at 330: "For example, a harmless piece of personal information can be published and then combined with other information and this can lead to disclosure of something private about an individual. In such a situation, the person concerned has consented to the disclosure or the public nature of the situation has brought the information out of the field of private information but there is nonetheless a violation of privacy."

[528] Solove, "Privacy", *supra* note 1 at 1452.

[529] Paul M. Schwartz & Daniel J. Solove, "The PII Problem: Privacy and a New Concept of Personally Identifiable Information" (2011) 86 N.Y.U. Law Review 1814 at 1836-1837: "There is common myth about anonymity on the Internet. Many people believe that anonymity exists for most situations when one surfs the Web or engages in behavior in cyberspace. The 'anonymity myth,' as we will call it, is this incorrect assumption that as long as one does not explicitly do something under one's actual name on the Internet, there will be safety from identification."

A 2005 survey entitled "RFID and Consumers" reported that awareness of RFID technology was low among both American and European consumers.[530] DPLs require retailers to obtain the informed consent of customers for the use or disclosure of shopping patterns revealed by RFID chips. Such "informed consent" will be difficult to achieve without extensive disclosure to the customer of the full implications of RFID surveillance and a positive indication of consent to the use and disclosure of RFID surveillance.[531] Some raise that it will also be difficult to formulate privacy policies that provide consumers with a meaningful opportunity to give consent to future uses of RFID (for example, with regards to RFID tags, fully "informed consent" would mean for an organization to reveal the 'dangerous' situation that the tag could be read by any external reader).[532] According to the Public Interest Advocacy Centre, a non-profit organization that provides legal and research services on behalf of consumer interests ("PIAC"), there are various issues with relying solely on simply posting a sign or statement on a tag noting the presence of RFID.[533] Consumers are not provided with a real opportunity to understand the proposed uses and disclosures of personal information via RFID.

To make matters worse, in many cases information is collected online and offline instantaneously and invisibly. For instance, when the consumer browses for products and services online, advertisers might collect and share information about the consumer's activity, search history, websites visited, etc. When participating in an OSN, third-party applications are likely to have access to the user's information pertaining to his posts. When using location-enabled devices, various third party application providers and entities might have access to the consumer's precise whereabouts. Apple has also drawn criticism for programming its iPhone to collect location data without proper consent.[534] While Apple's privacy policy was explicit on

---

[530] See BIGresearch, "Consumer Awareness of RFID Technology Now Stands at 42.4%, Up Dramatically From 28.2% Just One Year Ago" (15 November 2005), online: Marketwire <http://www.marketwire.com/press-release/consumer-awareness-rfid-technology-now-stands-424-up-dramatically-from-282-just-one-668531.htm>.

[531] Hariton, Lawford & Palihapitiya, *supra* note 197 at 3-4.

[532] *Ibid*. at 39.

[533] *Ibid*. at 36-37.

[534] Charles Arthur, "iPhone keeps record of everywhere you go" *The Guardian* (20 April 2011), online: The Guardian <http://www.guardian.co.uk/technology/2011/apr/20/iphone-tracking-prompts-privacy-fears>; Christopher Williams, "Apple under pressure over iPhone location tracking" *The Telegraph* (21 April 2011),

this kind of data collection, users did not understand the implications until much later.[535] If a consumer uses loyalty cards at a grocery store or sends in a product warranty card, his name, address, and information about his purchase may be shared with data brokers and combined with other data.[536] Most of these activities will take place without the knowledge of the consumer; as any potential warning contained within the privacy policy of the companies being dealt with (either directly or indirectly) are encrypted in legalese.

***

According to Janet Lo, without adequate notice and informed and meaningful consumer consent, consumers have no control over their personal information:

> "Because privacy policies are not effective in informing consumers about what information is collected by the website operator, how this information is used and the purposes for the collection and use of this information, consumers cannot be said to have provided informed and meaningful consent to these practices. Without adequate notice and informed and meaningful consumer consent, consumers have no control over their personal information."[537]

With recent technological changes, many believe that there are essentially no longer any proponents of the pure notice-and-choice model as it would no longer be adequate.[538] Privacy policies have become long and complicated documents, placing too high a burden on consumers to read, understand, and then exercise meaningful choices based on them.

While I don't completely reject the "control" concept of privacy and concurrently, the "notice and choice" model, I maintain that we need to limit the notices and choices to information which was meant to be protected by DPLs since users are currently "lost" in the volume of notices and choices which they receive on a daily basis. The focus on

---

online: The Telegraph <http://www.telegraph.co.uk/technology/apple/8466357/Apple-under-pressure-over-iPhone-location-tracking.html>.

[535] Apple, *supra* note 192.

[536] FTC, Preliminary Staff Report, *supra* note 372 at i.

[537] Lo, *supra* note 188 at 48.

[538] See comments made by Daniel J. Weitzner, a senior policy official at the National Telecommunications and Information Administration of the Commerce Department, discussed in Steve Lohr, "Redrawing the Route to Online Privacy" *The New York Times* (27 February 2010), online: The New York Times <http://www.nytimes.com/2010/02/28/technology/internet/28unbox.html> [Lohr, "Redrawing"].

"control over personal information" may be challenged in our contemporary society. Individuals generate massive amounts of information on a daily basis, online and offline, and may not be able to keep track of which organization collected, used or disclosed what piece of information and for which purpose. With the landscape of new technologies constantly increasing in complexity, I wonder if placing the "control" in the hands of users is the right thing to do in all situations, as it is forcing individuals to educate themselves on these ever-changing technologies.

In light of this, I believe that the approach which I propose in section 3 may be of guidance for any data protection system aiming at moving away from the current "notice and choice" model. Finally, I maintain that the type of notices to be provided and choices obtained should be directly linked with the sensitivity (risk of harm) of a given data handling activity, providing for a higher threshold of consent in the event that a given data handling activity creates a higher risk of harm for the individual concerned.

The changes detailed in section 1.2 are key drivers of the information society and highlight fundamental changes in how individuals and society grapple with privacy, business activities, social interaction, and information. These changes have various outcomes and consequences on the notion of *personal information*, as detailed in the next section.

2.1.2. Deconstructing the Efficiency of the Definition of Personal Information

As discussed earlier, the concept of privacy as "individuals in control of their personal information" is potentially too stringent since it would often ignore the societal importance of data flows and the legitimate reasons for the collection, use and disclosure of data by various organizations.[539] It would also place the right to privacy over and above countervailing values such as the freedom of speech and of information.[540] Section 2.1.1.2 discusses the issue with the "notice and choice" approach, which is included within the concept of privacy as "control". The present

[539] See section 2.1.1.1.1 entitled "Ignoring the Importance of Information Flow For the Society" as well as sectin 2.1.1.1.2 entitled "Ignoring Legitimate Reasons for Collecting, Using and Disclosing Information" which elaborate on this issue.

[540] See section 2.1.1.1.3 entitled "Ignoring Countervailing Values" which elaborates on this issue.

section will discuss the various challenges that relate to the definition of *personal information* in light of the various technological changes discussed in section 1.2.

This notion of *personal information* plays an important role and is crucial in the application of DPLs. As discussed in section 1.1.3, the definition has remained virtually unchanged since it was initially articulated in the early 1970s. Although most DPLs provide for certain exclusions, for example for journalistic or personal purposes,[541] employee or business contact information,[542] work product,[543] or for certain types of publicly available data,[544] the core of the definition has remained the same.

In Canada, PIPEDA defines *personal information* as *information about an identifiable individual*.[545] Other Canadian jurisdictions, namely Alberta,[546] British Columbia[547] and Quebec,[548] each have very similar definitions. In France, the definition is also very similar[549] and follows the definition of *personal data* provided by Directive 95/46/EC.[550]

---

[541] PIPEDA, *supra* note 63 at s. 4; Quebec DPL, *supra* note 110 s. 1; B.C. DPL, *supra* note 115 at Part 1, s. 3 (2) (a) and (b); EC, *Directive 95/46/EC*, *supra* note 99 at Whereas (12).

[542] PIPEDA, *supra* note 63 at s. 2 (1). PIPEDA does not apply to employees except of employees of federal works. Although it excludes from the definition the name, title or business address or telephone number of an employee of an organization. *Ibid*. at s. 2 (1); In the BC DPL, contact information is also excluded. "contact information" means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual: B.C. DPL, *supra* note 115 at Part 1, s. 1;

[543] The BC DPL excludes work product information from its definition of personal information. *Ibid*. at Part 1, s. 1.

[544] PIPEDA has *Regulations Specifying Publicly Available Information*, SOR/2001-7, which have been in force since 2001 and which exclude certain type of publicly available information. See also the Alberta DPL, *supra* note 114 at Part 2, Division 3, s. 14 (e) and Part 2, Division 4, s. 17. In BC, see B.C. DPL, *supra* note 115 at Part 4, s. 12 (1) (e), Part 5, s. 15 (1) (3) and Part 6, s. 18 (1) (a).

[545] Although it excludes from the definition the name, title or business address or telephone number of an employee of an organization. PIPEDA, *supra* note 63 at s. 2 (1).

[546] Alberta defines "personal information" as information about an identifiable individual. Alberta DPL, *supra* note 114 at s. 1(1) (k).

[547] BC uses the same definition than the Alberta DPL but with certain exclusion for contact information or work product information. It defines personal information as "information about an identifiable individual and includes employee personal information but does not include (a) contact information, or (b) work product information". "'contact information' means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual". See B.C. DPL, *supra* note 115 at Part 1, s. 1.

[548] Quebec DPL, *supra* note 110 at s. 2: "any information which relates to a natural person and allows that person to be identified".

[549] "Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro

The notion of *personal information* is one of the most important aspect of the "control" conception of privacy, since whether a piece of information is regulated by a DPL depends on whether it qualifies as *personal information*.[551]

In an article demonstrating how lawyers and legal scholars frequently comment on the law's inability to keep up with technological change, Lyria Bennett Moses ("Bennett Moses") suggests that over the course of history, the law has been observed to be in need of reform due to changes in transportation, computer, medical and communications technologies, among others. In all of these different contexts, the alleged reasons why the law needed to change were broadly similar: (i) **Over-inclusiveness and under-inclusiveness**, where existing legal rules were not formulated with new technologies in mind, resulting in those rules inappropriately including or excluding new forms of conduct; (ii) **Uncertainty**, where the law may be uncertain as it applies to new forms of conduct and it may not be clear whether a certain conduct is prohibited or authorized and therefore, existing legal rules may need to be clarified; and (iii) **Obsolescence**, where some existing legal rules may be justified, explicitly or implicitly, on the basis of a premise that no longer exists.[552]

In light of the technological changes discussed in section 1.2, I am of the view that using a literal interpretation[553] of the definition of *personal information* is no longer a viable option. This definition, at the heart of DPLs and the concept of privacy as "individuals in control of their personal information", plays an important role in the fact that DPL may be over-reaching or under-reaching. It also presents various uncertainties (especially with regards to new types of data). Finally, it is reasonable to

---

d'identification ou à un ou plusieurs éléments qui lui sont propres." *Loi informatique et liberté*, *supra* note 131 at art. 2.

[550] "any information relating to an identified or identifiable natural person". An indentifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. EC, *Directive 95/46/EC*, *supra* note 99 at art. 2(a).

[551] See section 1.1.2 entitled "Control over Personal Information and Fair Information Practices", section 1.1.2.2 entitled "Still about Control: Canadian and French", and section 1.1.3 entitled "Definition of Personal Information: Origin and Background" which elaborate on this issue.

[552] Lyria Bennett Moses, "Recurring Dilemmas: The Law's Race to Keep Up With technological Change" (2007) 7 University of Illinois Journal of Law, Technology and Policy 239 at 16. She also raises the fact that in certain cases there is a need for special laws and that there may be a need to regulate certain new forms of conduct using new, specially tailored, laws.

[553] An interpretation which is based on the exact wording. See Pierre-André Côté with the collaboration of Stéphane Beaulac and Mathieu Devinat, *Interprétation des lois* (Montréal: Éditions Thémis, 2009).

raise whether the concept of "identity" is still relevant in all cases (or whether it is obsolete), and whether pre-determined categories of "sensitive" data still make sense in today's Information Age.

2.1.2.1. Over-inclusiveness and Under-inclusiveness of the Definition

In order for a law to be efficient, it usually has to provide a result which adequately translates its goal or purpose.[554] I discuss in section 1.1.2.1 the fact that the FIPs were adopted in the specific context of computer development enabling automatic data processing. Many DPLs and data protection transnational policy instruments adopted for the last thirty or forty years (the OECD Guidelines, Convention 108, Directive 95/46/EC and the APEC privacy framework to name a few) claim to have been adopted for one of the main purposes of protecting the privacy of individuals.[555] I maintain, in section 2.2.2, that the ultimate purpose was in fact broader than protecting privacy and that it was the protection of individuals against the *risk of harm*, which may take place upon organizations collecting, using and disclosing their personal information. In this context, it is reasonable to wonder if the definition of personal information, *information that relates to an identifiable individual*, properly translates this main goal of DPLs.

The definition is extremely broad and may not allow for much flexibility. A literal interpretation of the definition triggers a situation under which certain data is either *personal information* or is not, without taking into account the context (whether a certain data handling activity may be harmful), which would allow for a more nuanced approach.[556] Many concerns have been raised over the lack of flexibility in the definition.[557] With new types of data, there have been contradicting positions rendered by courts in Europe using black or white literal interpretations when qualifying IP

[554] Bennett Moses, *supra* note 552 at 72.

[555] See OECD, *Guidelines*, *supra* note 11 at Preface; Convention 108, *supra* note 10 Preamble; EC, *Directive 95/46/EC*, *supra* note 99 at Whereas (1), (2) and (10); APEC, *Privacy framework*, *supra* note 363 at part. I, Preamble, s. 1.

[556] I am not proposing a contextual approach but instead, a more flexible approach under which information is evaluated in light of its underlying risk of harm to the relevant individual. I argue that only information which presents such risk should in fact be governed by the relevant DPL. See section 2.2.1.1 which elaborates on the differences between the approach which I propose and a contextual approach. See also, more generally, section 2.2.1 which elaborates on the proposed approach.

[557] See for example Waldo, Lin & Millet, *supra* note 6 at 22: "(…) the situational and contextual nature of privacy (…) depends on a number of specific factors that often do not cleanly and clearly overlap, rather than being identified by a sweeping universal calculus or definition".

addresses.[558] I maintain that this may well be in part due to the fact that the definition can be interpreted either strictly or broadly. The problem lies with the fact that each such literal interpretation, whether broad or strict, can lead to unwanted results.

It is my contention that a literal interpretation of the definition of *personal information* has in many instances either an over-inclusive outcome, or an under-inclusive one.

2.1.2.1.1. Potentially Over-Inclusive Definition

"Control over personal information" is a concept that can be over-reaching according to certain privacy experts.[559] In *Wyndowe v. Rousseau*,[560] the Canadian Court mentions that in light of the fact that "personal information is defined (…) as meaning *information about an identifiable individual* [t]he Act is therefore very far reaching."[561] As Paul Ohm ("Ohm") states:

> "No matter how effectively regulators follow the latest re-identification research, folding newly identified data fields into new laws and regulations, researchers will always find more data field types they have not yet covered. The list of potential PII will never stop growing until it includes everything."[562]

I maintain that the definition of *personal information* is at the heart of this issue and that, if interpreted too broadly, can end up covering too much information (all kinds of information), and trigger the situation of having DPLs translated into a very

---

[558] See section 2.1.2.2.1(b) entitled "At what costs and using what kind of efforts?" which elaborates on this issue.

[559] See section 2.1.1 entitled "Deconstructing the Concept of Privacy as Control" which elaborates on this issue. Solove, who has an issue with conceptualizing privacy as "control of information" as he believes the conception is too broad, suggests that one possibility is that the control-over information conception be limited in scope by including only intimate information. Although he is still concerned that it would still be too broad of a conception. See Solove, "Conceptualizing", *supra* note 23 at 1114. Stan Karas also suggests that the informational privacy approach to consumer data is inappropriate as it is too broad. See Karas, *supra* note 362 at 13: "Yet, despite this illustrious history, applying the tenets of the informational privacy approach to consumer data is inappropriate. The approach is simply too vague, broad and, as suggested above, this lacks proper attention to the context of the privacy invasion."

[560] 2008 FCA 39 (CanLII) [*Wyndowe*].

[561] *Ibid*. at para. 40.

[562] See Paul Ohm, "Broken Promises of Privacy" (2010) 57 UCLA l. Rev. 1701 at 1742.

cumbersome framework. Some observers have already complained about the onerous obligations outlined by certain DPLs[563] or the Directive 95/46/EC.[564] Ohm argues that:

> "The Directive's aggressive data-handling obligations might have seemed to strike the proper balance between information flow and privacy when we thought that they were restricted to "personal data," but once reidentification science redefines "personal data" to include almost all data, the obligations of the Directive might seem too burdensome. For these reasons, the European Union might want to reconsider whether it should lower the floor of its comprehensive data-handling obligations."[565]

It is interesting to note that, as far back as 1993, concerns were already being raised over excessively costly and burdensome data-handling requirements set forth by the Quebec DPL.[566]

(a) Definition Meant to be Broad

DPLs cover all information that relates to and can identify an individual, regardless of whether the information relates to an individual's privacy or private matters or is used in a harmful way towards the individual.

Section 1.1.3 entitled "Definition of Personal Information: Origin and Background" details the context of the elaboration of this definition of *personal information*. It is important to bear in mind that this definition was initially meant to be broad:

> "It needs to be noted that this definition reflects the intention of the European lawmaker for a wide notion of "personal data", maintained throughout the legislative process. The Commission's original proposal explained that "*as in Convention 108, a broad definition is adopted in order to cover all information which may be linked to an individual*". The

---

[563] In Quebec, Gautrais & Trudel, *supra* note 1 at 3: "De plus en plus souvent, émergent des situations selon lesquelles il est nécessaire – et non seulement utile – de se servir de ces derniers pour que le service soit tout simplement rendu. Le constat est simple : sans circulation, pas de service. Or, cette action de circulation est susceptible, au gré d'une interprétation par trop 'rigoureuse' des lois sur la protection des renseignements personnels, de donner lieu à un encadrement que nous croyons passablement 'lourd' quant au sens à donner à des termes tels que 'communiquer', 'collecter', 'transmettre', 'détenir', 'conserver', 'utiliser', etc."

[564] Doorthee Heisenberg is calling parts of Directive 95/46/EC "quite strict" and "overly complex and burdensome. See Dorothee Heisenberg, *Negotiating privacy: the European Union, the United States and personal data protection* (Boulder: Lynne Rienner Publishers, 2005) at 29, 30.

[565] Ohm, *supra* note 562 at 1763.

[566] See Quebec, Assemblée, *Les travaux parlementaires*, 34th lég., 2e sess. (March 19, 1992 to March 10, 1994), cahier no 73, 16 March 1993, pages 5357-77, at 13.

> Commission's modified proposal noted that "*the amended proposal meets Parliament's wish that the definition of "personal data" should be as general as possible, so as to include all information concerning an identifiable individual*", a wish that also the Council took into account in the common position."[567]

The breadth of the protection (i.e. all personal information) was initially motivated by the concern that small quantities of data of small computers could be connected with each other and with a central computer, thus forming a network in which all sorts of information could circulate.[568] The potential for correlation, coupled with the fact that the risks that these databanks involved for the rights and freedoms of individuals were found to be difficult to assess.[569] The FIPs (incorporated in DPLs) were also meant to remain relevant even in the face of continuous technological improvements; the definition of *personal information* was drafted in broad terms in large part to ensure this.[570] The conditions were ripe for the adoption of a very broad definition.

According to Trudel, it was also to circumvent problems involved in teasing out what has to remain secret in order to respect the right to privacy, that a notion was chosen that conflates "information that identifies an individual" with "information about an individual's private life" and DPLs were structured around the principle that the whole set is confidential:

---

[567] Article 29 Data Protection Working Party, *Opinion 4/2007*, *supra* note 100 at 4 [footnotes omitted].

[568] Council of Europe, *Report on data processing*, *supra* note 66 at 5, s. II, s. 3: "The present technical trend is towards the spread of small computers storing small quantities of data, but which may be connected with each other and with a central computer, thus forming a network in which all sorts of information circulate. From this point of view, control is necessary not only over the information stored, but also over its use and the means by which it is obtained, i.e. data processing control"; Also see s. II Explanatory Memorandum, s. 2 entitled "Reasons and objectives of the report", para. 1 entitled "reasons": "The growing number of files containing information on the health, the social, economic or penal situation and the opinions of individuals is reckoned as a threat in our societies (…) also because of the possibility of establishing interconnections between data banks and using the information obtained for undisclosed purposes."

[569] See *ibid* at s. II, s. 2 para. 1: "Although only thirty years old, data processing has become an essential feature of administration and management and is invading our daily lives. An increasing amount of information on almost every citizen is recorded in automated files whose capacity is much greater than that of manual files. These files offer obvious advantages to their users, but the risks they involve for the rights and freedoms of those about whom data are recorded are difficult to assess."

[570] Reports from the 70s that were published around the time of the elaboration of the definition of *personal information* suggest that this definition was meant to survive new technologies. For instance, Lindop articulated the view that their DPL should survive technology, and that it was necessary to ensure that the legislation would not need to be amended by reason of technical changes alone. See Lindop, *supra* note 96 at 13, para. 3.04.

> "While it is clear that some data concerning individuals is private, it is also clear that not all is. Apparently in the quest for standards guaranteeing fair personal data collection and processing practices, the nuances that had until then described the concept of privacy were left behind and instead measures were adopted that prohibit the circulation of any data on individuals." [571]

Even recently, governmental agencies and law makers still respect and take into account the fact that the definition was intentionally broad. For instance, in Canada, the OPCC recently concluded that *work product* should not be exempted from the definition of *personal information* in PIPEDA, one of the reasons being that the definition was intentionally broad, and it demonstrated a commitment to protecting individual privacy rights in all contexts.[572] Alberta has also declined to do so, reasoning that "the current contextual approach allows for greater flexibility than a categorical exclusion".[573]

The definition of *personal information* is so broad that almost any information can qualify as *personal*.[574] As a treatise on Canadian privacy law summarizes, "In essence, almost any information in any form that can be attributed to an identified individual is caught by this expansive definition."[575] The federal Privacy Commissioner plays a key role in deciding whether information is "identifiable". The general tendency has been expansionist. As the OPCC stated in his annual report to Parliament, 2001-2002:

> "The definition is deliberately broad, and in my findings I have tended to interpret it as broadly as possible. (…) I am inclined to regard

---

[571] Trudel, "Privacy Protection", *supra* note 164 at 319-20. See also Trudel, "protection de la vie privée", *supra* note 400 at 957.

[572] OPCC, *supra* note 135.

[573] See Alberta Select Special Personal Information Protection Act Review Committee, *Final Report: November 2007* (Edmonton: 2007) at 25-26.

[574] Boštjan Bercic & Carlisle George, "Identifying Personal Data Using Relational Database Design Principles" (2009) 17:3 International Journal of Law and Information Technology 233 at 235: "The criteria are met if it applies to a concrete individual, for example: the mere fact that an individual is wearing a red shirt can constitute an item of personal data."

[575] Barbara McIsaac et al., *The law of privacy in Canada* 4-7 (2011); See Jeffrey A. Kaufman, ed., *Privacy law in the private sector: an annotation of the legislation in Canada* (Aurora: Canada Law Book, 2007), at 15: "It is, therefore, important to note at the outset that the definition of 'personal information' [in PIPEDA] is extremely broad"; See also Stephanie Perrin et al., *The personal information protection and electronic documents act: an annotated guide* (Toronto: Irwin Law, 2001) at 54: "The definition in the Act is limitless in terms of what can be information about an identifiable individual."

> information as personal even if there is the smallest potential for it to be about an identifiable individual."[576]

In 2011, the OPCC published a handbook entitled "A Privacy Handbook for Lawyers, PIPEDA and Your Practice" in which states that: "as per relevant jurisprudence on the concept of "personal information," a broad and expansive interpretation is in order."[577] According to Canadian case law, information will be "about" an individual when it is not just the subject of that individual, but also relates to or concerns the individual.[578] Furthermore, an individual will be "identifiable" where there is a serious possibility that they could be identified through the use of that information, alone or in combination with other available information.[579] I maintain that this is overly broad.

Even the mere fact that an individual is wearing a red shirt can constitute an item of personal information. Boštjan Bercic and Carlisle George ("Bercic and George") are illustrating this excessive broadness with the following examples:

> "The fact that John Smith drives a car of XYZ brand is undisputedly personal data. A related question is whether the fact that this car has an engine capacity of 2000 cm3 can also be considered personal data. At first sight, the engine's capacity is not personal data (and it is not if taken by itself). Surprisingly, it becomes personal data as soon as we know that this car is driven or owned by an individual. (…) Similarly, the fact that a piece of land X that is owned by James Moore is worth €100.000 is also personal data. (…) the fact that the water on the piece of land is potable (or not) can become personal data if we know whose piece of land it is or who lives on it. Many other absurd examples like this can be constructed (e.g., the fact that Paris is the capital of France can become personal data if we relate it to John Smith who lives in Paris, the capital of France)."[580]

---

[576] Office of the Privacy Commissioner of Canada, *Annual Report to Canada 2001-2002* (Ottawa: Office of the Privacy Commissioner of Canada, 2003) at Part Two, "Report on the Personal Information Protection and Electronic Documents Act, The Definition of Personal Information". For important caselaw interpreting *personal information* under PIPEDA, see *Gordon v. Canada (Health)*, 2008 FC 258 (CanLII) [*Gordon*]; *Wyndowe*, *supra* note 560.

[577] Office of the Privacy Commissioner of Canada, *A Privacy Handbook for Lawyers, PIPEDA and Your Practice* (Ottawa: Office of the Privacy Commissionner of Canada, 2011) at 2 [OPCC, *Handbook for Lawyers*]: "Information will be 'about' an individual when it is not just the subject of that individual, but also relates to or concerns the individual."

[578] *Canada (Information Commissioner) v. Canada (Transportation Accident Investigation and Safety Board)*, 2006 FCA 157 (CanLII); *Dagg v. Canada (Minister of Finance)*, [1997] 2 S.C.R. 403.

[579] *Gordon*, *supra* note 576.

[580] Bercic & George, *supra* note 574 at 248.

In Europe, the Article 29 Working Party suggests that the concept of personal data includes data providing any sort of information including more general kinds of information[581] and that the term "any information" contained in Directive 95/46/EC clearly signals the willingness of the legislator to design a broad concept of *personal data* and that this wording calls for a wide interpretation.[582] At the same time, this Working Party, somewhat acknowledging that Directive 95/46/EC is potentially over-reaching in its scope, has suggested that the scope of this Directive 95/46/EC should not be overstretched and that "an undesirable result would be that of ending up applying data protection rules to situations which were not intended to be covered by those rules and for which they were not designed by the legislator."[583]

Referring to Richard Murphy's definition of *personal information*[584] (which is consistent with the definition of *personal information* discussed herein) Solove claims that it is too broad because there is a significant amount of information identifiable to us that we do not deem as private.[585] In his own words: "For example, the fact that a person is a well-known politician is identifiable to her, but is not private. Murphy's definition thus provides no reasonable limitation in scope".[586] According to Julie Inness ("Inness"), not all personal information is private as "it is the *intimacy* of this information that identifies a loss of privacy".[587] Trudel and Benyekhlef were mandated to evaluate the Quebec DPL in the context of the Internet a few years after its enactment. At that point, in 1997, it was already very clear to these authors that the definition of *personal information* was over-reaching in the context of the Internet and that the elusive balance between the

[581] Article 29 Data Protection Working Party, *Opinion 4/2007*, *supra* note 100 at 6: "From the point of view of the content of the information, the concept of personal data includes data providing any sort of information. This covers of course personal information considered to be 'sensitive data' in Article 8 of the directive because of its particularly risky nature, but also more general kinds of information."

[582] *Ibid*.

[583] *Ibid*. at 5.

[584] Richard S. Murphy, "Property Rights in Personal Information: An Economic Defense of Privacy" (1996) 84 Geo. L.J. 2381 at 2383.

[585] Solove, "Conceptualizing", *supra* note 23 at 1111.

[586] *Ibid*. at 1112.

[587] Julie C. Inness, *Privacy, Intimacy and Isolation* (New York: Oxford University Press, 1992) at 58.

protection of personal information and the free flow of information had yet to be reached.[588]

In 2009, the U.K. Information Commissioner's Office mandated a multidisciplinary international research team led by RAND Europe with time-lex and GNKS-Consult ("RAND Corporation") to review the strengths and weaknesses of Directive 95/46/EC and propose avenues for improvement. One of the main weaknesses identified by RAND Corporation was the fact that the link between the concept of "personal data" and real privacy risks was unclear.[589] This weakness has also been mentioned by various courts.

As a matter of fact, in certain cases, judges have come to the conclusion that the definition of personal information was to be interpreted more narrowly. For example, in the U.K. case of *Durant v Financial Services Authority,*[590] the Court of Appeal issued a landmark ruling narrowing the interpretation of what makes data "personal" (within the meaning of personal data under Directive 95/46/EC and the U.K. *Data Protection Act* 1998). More specifically, the Court ruled that personal data is information which: "is biographical in a significant sense; has to have the individual as its focus; and has to affect an individual's privacy whether in his personal family life, business or professional activity".[591]

In Europe, the Article 29 Working Party admits that a mechanistic application of every single provision of Directive 95/46/EC may lead to excessively burdensome or perhaps even absurd consequences, and that in the event that it does, it suggests that certain

---

[588] Trudel & Benyekhlef, *supra* note 367 at 3 : "La définition des notions de renseignements personnels des lois québécoises actuelles est trop large: elle empêche la circulation d'informations qui n'ont rien à faire avec la vie privée et du même coup, il en résulte une dilution de la protection des informations qui sont vraiment du domaine de la vie privée."

[589] Robinson et al., *supra* note 151 at ix; See also, *ibid*. at 27: "The scope of the Directive has been criticised because the relationship between privacy protection and data protection is vague: not all acts of personal data processing as covered by the Directive have a clear or noticeable privacy impact, and we must ask if this is a weakness in its focus. Should the impact on privacy be a relevant criterion for determining the applicability of data protection rules? The impact of the Directive is not defined in terms of situations with a privacy impact, but rather to acts of personal data processing. The Directive's approach is based strongly on a fundamental rights interpretation of data protection, where personal data is deemed inherently worthy of protection."

[590] [2003] EWCA Civ. 1746.

[591] Please note that the case has been taken before the European Court of Human Rights as a breach of Article Eight of the European Convention of Human Rights, article Eight which states that everyone has the right to respect to his private and family life, his home and his correspondence.

verifications should be made as to ensure that a given situation actually falls within the scope of Directive 95/46/EC.[592] In their own words: "It is a better option not to unduly restrict the interpretation of the definition of personal data but rather to note that there is considerable flexibility in the application of the rules to the data."[593]

Nissenbaum argues that the widely held conception of a right to privacy as a right to control information about oneself can also apply to protections even in categories of so-called public information, public spaces, and against non-governmental agents.[594] With more and more data available in cyberspace,[595] this definitely increases the potential for DPLs being over-reaching.

In recent years, certain Canadian DPLs have introduced notification obligations in the event of data security breaches. At the federal level, Bill C-12 was introduced in 2011[596] proposing a provision which would require organizations to notify the individuals involved if it is reasonable in the circumstances to believe that the breach creates "a real risk of significant harm to the individual". While it has been argued that this "real risk of significant harm" test is rather subjective,[597] it also goes a long way in demonstrating how DPLs are too broad in nature and that in many cases, a breach of security of random personal information may not necessarily imply any harm to the individuals concerned. Furthermore, this is a clear illustration of the fact that when legislators are attempting to limit the scope of the DPLs, they are inclined to focus on the notion of "risk of harm", probably, as I argue below, because this is the ultimate purpose of DPLs.[598]

---

[592] Article 29 Data Protection Working Party, *Opinion 4/2007*, *supra* note 100 at 5-6.

[593] *Ibid*.

[594] Nissenbaum, *supra* note 230 at 154.

[595] See section 1.2.1 entitled "Increase in Volume of Information" which elaborates on this issue.

[596] *Safeguarding Canadians' Personal Information Act*s, *supra* note 506 aimed to amend PIPEDA, was re-introduced by the Government of Canada on September 29, 2011.

[597] See comments by John Lawford, counsel with the Public Interest Advocacy Centre in Ottawa, in Michael McKiernan, "New federal privacy, anti-spam bills get mixed reviews" *Law Times* (31 May 2010), online: Law Times <http://www.lawtimesnews.com/201005316982/Headline-News/New-federal-privacy-anti-spam-bills-get-mixed-reviews>; See also David Canton, "Changes to privacy laws vague" (28 June 2010), online: elegal <http://canton.elegal.ca/2010/06/28/changes-to-privacy-laws-vague/>.

[598] See section 2.2.2 entitled "Determining Risk of Harm as Purpose Behind the Protection of Personal Information" which elaborates on this issue.

In many cases where organizations have been found to be in breach of a DPL, damages have not automatically been awarded by the courts.[599] Thus DPLs are often over-reaching in their effect, since a breach of the DPL doesn't mean that any kind of harm was necessarily done to an individual. I maintain that a literal interpretation of the very broad wording of the definition of *personal information* may well be at the heart of this over-inclusive outcome.

(b) Correlation Required to Identify an Individual

Personal information can be regarded as the set of all data that is associated with a specific individual, such as a date of birth, gender, home address, etc. In most cases, certain information "on its own" may not affect an individual's privacy or be potentially harmful, since it can almost always be associated with more than one individual. For example, many people have the same name, share the same birth date or share the same address. It is usually the correlation between two information elements that creates a privacy issue as this reduces the number of individuals from the group sharing the same information elements or ends up referring to a unique individual. *Personal information* therefore has meaning only so far as it associates or differentiates an individual from others.[600] Bercic and George illustrate the uncertainty surrounding the correlation and the notion of *personal information* as follows :

> "The Directive's definition does not define personal data in this way, hence it is unclear, for example, whether a unique identifier of a person (such as the UK National Insurance Number referred to as NINO, or US Social Security Number referred to as SSN) already constitutes personal data, whether only items of data related to this unique identifier would be considered personal data (for example, the fact that someone lives on Oxford street) or whether only a record that meets both criteria (inclusion of the unique identifier and data related to it) would be considered personal data (for example, the NINO of a person plus the fact that this person lives on Oxford street)."[601]

---

[599] See recent decisions rendered under by the Federal Court of Canada under PIPEDA, such as *Randall v. Nubodys Fitness Centres*, 2010 FC 681 (CanLII) [*Randall*]; *Stevens v. SNF Maritime Metal*, 2010 FC 1137 (CanLII) [*Stevens*].

[600] Waldo, Lin & Millet, *supra* note 6 at 39. In 1973, the *Records, Computers and the Rights of Citizens* Report (U.S.) suggested that data can be associated with identifiable individuals by means of some specific identification information, therefore implying the necessity for some type of correlation between two pieces of data. U.S. Department of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *supra* note 57 at s. IV.

[601] Bercic & George, *supra* note 574 at 236 [footnotes omitted].

Privacy is then a relative concept. An individual may feel that his or her privacy is adequately protected if they can be identified in a group of 10 people, for instance. While others may feel that their privacy is adequately protected if they can be identified within a group of 100 people.[602] In some cases, "unique identifiers" could be said to specify unique individuals.[603]

At the time that the principles of FIPs were initially formulated in working documents leading to Convention 108, privacy issues related to basic personal information that could be located in automated computer databases. Therefore, the concerns were that certain data concerning an individual, although by themselves inoffensive, could be correlated in such a way that their availability became a privacy threat to this individual,[604] especially given that certain databanks could be linked.[605] DPLs were meant to protect the privacy of individuals.[606] Instead of intervening at the point where the aggregation of information may breach the privacy of individuals, DPLs prohibit all circulation of information, in the event that this circulation may constitute a privacy breach. This illustrates how and why this concept is over-reaching and why the definition may often trigger an over-reaching outcome.

(c) Dealing with New Types of Data

The current definition of *personal information* can be challenged when attempting to qualify new types of data that have emerged on the Internet, as discussed in section 1.2.2. For instance, data may be linked to a device connected to the Internet (instead of a physical person) that may be used by one or more individuals and which can be

---

[602] Waldo, Lin & Millet, *supra* note 6 at 39.

[603] *Ibid*. at 40: "For example, ruling out the case of identical twins, an individual's complete genomic sequence (the specific sequence of all 3 billion DNA base pairs) could specify a unique individual. Barring errors and fraud, the Social Security number was originally intended to be a unique identifier. But in general, no one data elements specify a unique individual."

[604] See Council of Europe, *Explanatory Report: Resolution (73) 22*, *supra* note 56 at para. 3: "(…) data concerning him, which are by themselves inoffensive, may be correlated in such a way that their availability becomes a threat to his private interests".

[605] *Ibid*. at para. 14: "The resolution covers all data collections, irrespective of their size. It should be pointed out in this connection that computer technology makes it possible to link several small data banks into one big data bank."

[606] See OECD, *Guidelines*, *supra* note 11 at Preface; Convention 108, *supra* note 10 at Preamble; EC, *Directive 95/46/EC*, *supra* note 99 at Whereas (1) (2) and (10); APEC, *Privacy framework*, *supra* note 363 at part. I, Preamble, s. 1.

used to identify an individual only under certain circumstances (sometimes with the assistance of ISP log files or through data aggregation or correlation across services).

Support is growing for a broad interpretation of *personal information*, under which all new types of data are considered as personal information.[607] Proponents of this broad interpretation maintain that only the courts can decide for certain whether these new types of data amount to personal information and therefore, companies should exercise caution.[608] Furthermore, with respect to IP addresses, since ISPs would find it difficult to distinguish where identification is possible, Article 29 Working Party argues that all IP addresses should be treated as personal data, just "to be on the safe side".[609] This approach contributes to the potential over-reachingness of the definition.

(d) Consequences of Over–Inclusiveness

In the context of the Internet and new technologies, this over-inclusiveness (or the fact that DPLs are "over reaching") creates additional burdens for organizations and online service providers that hunger for data.[610]

---

[607] See Article 29 Data Protection Working Party, *Opinion 4/2007*, *supra* note 100 at 17. In France, early decisions from the CNIL pertaining to email addresses illustrate a very broad interpretation as well. In an early decision, for example, the CNIL appears to treat all e-mail addresses as nominative information whether or not the e-mail address uses a pseudonym or an anonymous re-mailer. See Délibération No. 97-051 du 30 juin 1997 concernant une demande d'avis présenté par la Mairie de Paris relative à un traitement d'informations nominatives mis en oeuvre dans le cadre du site Internet de la Ville de Paris. In another case, the CNIL granted permission to France Telecom to proceed with an e-mail service, Minitelnet, linking the Minitel to the Internet. See CNIL, Délibération No. 97-050 du 24 juin 1997 relative à une demande d'avis présenté par France Télécom concernant un traitement automatisé d'informations nominatives dénommé "Minitelnet". In this authorization as well, all email addresses were considered nominative.

[608] See for example Peter Scharr, German Federal Data Protection Commissioner and Chairman of the Article 29 Working Party, whose comments were the subject of various articles on the debate, has stated that all IP addresses should be treated by companies using them, as personal data. See Townsend & Jay, *supra* note 384.

[609] See Article 29 Data Protection Working Party, *Opinion 4/2007*, *supra* note 100 at 17: "So, unless the Internet Service Provider is in a position to distinguish with absolute certainty that the data correspond to users that cannot be identified, it will have to treat all IP information as personal data, to be on the safe side."

[610] Please refer to section 1.2.4.1 entitled "New Business Models (Customization and Sponsored Services)" for details on the online service providers that needs this data. For example, DPLs would apply to a website that collect and uses IP addresses even to determine the likely origin of a visitor for language customization purposes regardless of the apparent lack of risk of harm. Certain online service providers have in fact raised that the broadness of the definition is problematic for their business. See: Peter Fleischer, "Are IP addresses 'Personal Data'?" *Peter Fleischer: Privacy…?* (5 February 2007), online: <http://peterfleischer.blogspot.com/2007/02/are-ip-addresses-personal-data.html> [Fleischer, "IP addresses"]: "Personal data is very broadly defined in Article 2 of the Directive as 'any information relating to an identified or identifiable natural person'. Where this definition is applied unqualified then it may be interpreted in such a way that data will remain 'personal' and subject to the full remit of the law if

The fact that the definition is overly broad encourages a burdensome framework in which all data handling activities are governed by DPLs, regardless of the type of data or the type of activity at stake. Gautrais and Trudel point out that the provision of public services often requires a certain level of personal information.[611] They warn against elaborating strict interpretations of data collection, use and disclosure – as it would encourage the development of a burdensome framework. Trudel and Benyekhlef also claim that the over-reaching definition ("englobante") triggers the situation in which we may have to determine all kinds of exceptions to this definition, for the public good.[612] Trudel and Gautrais are suggesting that if we regulate too many situations, then organizations may be less and less inclined to comply with the law, if such law does not properly reflect the factual reality.[613]

Moreover, an over-reaching definition may trigger a system in which organizations and industry players will incur additional costs for complying with DPLs, which have nothing to do with the protection of individuals. According to Microsoft: "As data flows increase in volume and complexity, the application of blanket rules will not make sense in many circumstances -- they will increase costs without meaningfully enhancing the protections provided to data subjects."[614] Microsoft also does not believe that it is

---

individuals remain in any way identifiable. We believe that the concept of personal data should rather be defined pragmatically, based upon the likelihood of identification."

[611] Gautrais & Trudel, *supra* note 1 at 3: "la tendance grandissante est que la perpétuation des services gouvernementaux d'une façon diligente et efficace exige de plus en plus une circulation des renseignements personnels. De plus en plus souvent, émergent des situations selon lesquelles il est nécessaire – et non seulement utile – de se servir de ces derniers pour que le service soit tout simplement rendu. Le constat est simple : sans circulation, pas de service. Or, cette action de circulation est susceptible, au gré d'une interprétation par trop 'rigoureuse' des lois sur la protection des renseignements personnels, de donner lieu à un encadrement que nous croyons passablement 'lourd' quant au sens à donner à des termes tels que 'communiquer', 'collecter', 'transmettre', 'détenir', 'conserver', 'utiliser', etc."

[612] Trudel & Benyekhlef, *supra* note 367 at 11: "La notion de vie privée ne couvre pas toutes les informations qui touchent une personne. Comme nous vivons en société, il est des composantes de l'activité de chacun qui ont un caractère public. En ignorant cela et en persistant à promouvoir une définition englobante, telle la notion de 'renseignements personnels', on s'expose à inclure une kyrielle d'information dans le champ de la protection (en fait, tous les renseignements concernant une personne et permettant de l'identifier) et se retrouver dans l'obligation de multiplier les circonstances où il sera nécessaire, au nom du bien public, de déroger (par la multiplication des dispositions dérogatoires) aux protections pourtant essentielles à la préservation de la zone d'intimité de chaque personne."

[613] Gautrais & Trudel, *supra* note 1 at 43-44 : "(…) Mais outre le fait que cette insécurité soit pour le moins difficile à évaluer, il n'y a aucune preuve selon laquelle plus de contrôle a priori s'effectue et plus de protection est ainsi assurée. Au contraire. Si l'on souhaite trop encadrer des situations où un tel contrôle ne s'impose pas selon nous, il est un risque de voir le droit systématiquement violé, bafoué, les gestionnaires le considérant comme inadapté aux situations factuelles qui sont les leurs. Il est donc important que le droit soit en accord harmonieux avec les faits."

[614] Microsoft Corporation, *supra* note 358.

necessary to apply the full panoply of DPLs to every instance where personal data are processed and is positing that a more nuanced, or context-based, approach would enhance user privacy by ensuring that higher levels of protection are applied in situations where this is warranted.[615]

A broad literal interpretation of the notion of *personal information* may bring about a situation whereby even new types of data will be governed by DPLs, implying certain obligations for organizations managing this data which may be problematic in certain cases. For instance, Yves Poullet and his colleagues from the *Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel* (the "Comité consultatif") question how it would be possible to provide disclosure pertaining to the collection and use of these new types of data and obtain consent from individuals without actually identifying them.[616] They also raise that it may be difficult for an organization collecting new types of data to grant access if this data has not even been processed.[617] As a matter of fact, another negative consequence relates to an organization having to grant access to this so called *personal* information to individuals requesting it if they can be argued to be personal information relating to them.[618] The privacy issue with granting access to a website recording navigational or *clickstream* data (as an online user moves from page to page on its website) is that the data collected through these devices does not necessarily belong to one single individual. This entails that providing access to an online user to this data may breach the privacy of the other users of the same computer since the profile data, *clickstream* data and other data that could be collected might reveal information of intimate nature.[619]

---

[615] *Ibid*.

[616] Conseil de l'Europe, *L'autodétermination informationnelle*, *supra* note 20 at 34.

[617] *Ibid*.

[618] See Bercic & George, *supra* note 574 at 248.

[619] Gratton, "Personalization", *supra* note 16: "For instance, an employee at work sharing his/her workstation with other colleagues could be afflicted with a certain embarrassing disease. Should the data regarding this disease be disclosed to online users who request it, the employee in question would be terribly embarrassed and this would be in breach of his/her privacy."

2.1.2.1.2. Potentially Under-Inclusive Definition

The "control" conception of privacy can also be under-reaching by omitting to protect data which should be protected. For example, by failing to protect against profiling and behavioral marketing techniques in certain situations.

(a) Data not Identifying but Impacting on Individuals

In the event that certain data does not qualify as *personal information* (according to a strict literal interpretation), this data will not be subject to DPLs, although many raise that there may still be data protection or privacy issues surrounding certain data handling activities.

For example, the Comité consultatif raises the fact that a breach in human dignity can take place even in the absence of personal data processing.[620] The Comité consultatif then posited that a new approach, different from the notion of "control over personal information", may therefore be advisable.[621]

The uncertainty surrounding profiles raises another interesting issue. The definition of personal information focuses on information that relates to an individual that is "identifiable". Certain profiles may therefore be considered as anonymous and not covered under the definition if the name of the individual to which the profile belongs is unknown. But the profiles may still be used, for instance, to take decisions about an individual (or a profile).[622] For instance, Amazon was accused of practising *adaptative pricing* using cookies that would raise the price of certain items in accordance with the

---

[620] For instance, the Comité consultatif raises that a camera filming an anonymous individual trying on lipstick in a store may raise a privacy or a dignity issue even if this activity does not involve the processing of *personal information* (since the identity of the individual is unknown). Conseil de l'Europe, *L'autodétermination informationnelle*, *supra* note 20 at 25. See also section 2.2.2.1.1 entitled "Privacy is Broader than Data Protection" which elaborates on the fact that privacy is in fact broader than data protection (or of the concept of "control over personal information").

[621] Conseil de l'Europe, *L'autodétermination informationnelle*, *supra* note 20 at 23-24.

[622] See Roger A. Clarke, "Profiling : A hidden Challenge to the Regulation of Data Surveillance" (1993) 4 :2 J. of Law and Information Science 403 [Clarke, "Profiling"]; See also Conseil de l'Europe, *L'autodétermination informationnelle*, *supra* note 20 at 25 and see also at 28: "La possibilité de collecter des données relatives à des comportements présents ou passés, données personnelles ou anonymes, en quantités et qualités de plus en plus importantes et de les traiter de manière de plus en plus fine génère des risques de plus en plus grands de créer des profils et de prendre des décisions a priori par rapport à ces profils. Ainsi, la manière pour un internaute de naviguer sur le site d'une entreprise peut être caractérisée par quelques critères qui permettront après quelques visites de le ranger dans une catégorie ou une autre, d'afficher lors d'un contact une page de préférence à une autre, voire de lui refuser tel service."

profile of the potential purchaser.[623] In this case, although the identity of the individual impacted by this pricing decision is unknown, this individual may still be subject to some type of discrimination or other type of harm, which DPLs were meant to address.[624]

(b) Data Evaluated in Isolation vs. Full Picture

A strict literal interpretation of *personal information* may result in excluding new types of data since they relate to a device or an object (instead of an individual) or because the identity (name or contact information) of the individual to which they relate is unknown. Moreover, if a particular piece of data does not identify an individual on its own, it will often not qualify as "personal" under the strict interpretation.

Such literal interpretation could also encourage a piecemeal approach instead of looking at the big picture. As discussed under section 2.1.2.1.1(b) while every piece of information taken "on its own" may not qualify as *personal information*, when considering all the data together as a whole, the profile data may end up identifying an individual.[625] The same reasoning can apply if we consider data correlation[626] and data-mining techniques now available,[627] which trigger the situation whereby a single, insignificant piece of information may end up identifying an individual.

A strict literal interpretation of the notion of *personal information* may result in an under-inclusive outcome as it may trigger a situation where the privacy of online users are affected or where data handling activities which may be harmful to individuals are not

---

[623] *Ibid*. at 29.

[624] See section 3.2 and more specifically, section 3.2.2.1 entitled "Identifiability Replaced by Negative Impact (Objective Harm)" which elaborate of this issue.

[625] Pomerance, *supra* note 233 at 287: "it is by no means clear that data-mining would be found to offend section 8 of the Charter, given that: 1) any single piece of information, standing alone, might not be sufficiently intimate, personal or private to trigger section 8 protection; and 2) because much of the information that is accessed or 'mined' is within the public domain." Ian R. Kerr & Jenna McGill, "Emanations, Snoop Dogs and Reasonable Expectation of Privacy" (2007) 52:3 Criminal Law Quarterly 392 at 430-31: "In fact, as new and emerging information technologies continue to come before the courts, we predict that the current reductionist inclination which asks whether the intercepted data is, *on its own*, meaningless will and ought to give way to the very opposite approach, namely: whether the bundle of information that is made available by means of the search, *once assembled,* ought to attract a reasonable expectation of privacy. This latter approach recognizes the jigsaw nature of the data/information/knowledge/wisdom chain and the importance of each piece of the puzzle in telling a story despite the fact that no single piece could do so on its own."

[626] See section 1.2.3.1 entitled "Aggregation and Correlation of Data" which elaborates on this issue.

[627] See section 1.2.3.2 entitled "Extensive Data-mining Capabilities" which elaborates on this issue.

covered under DPLs. The data may end up identifying an individual, revealing private facts or intimate details in the process.[628] As it happens, the content of search queries have indeed been found to identify individual people in certain situations. In the AOL privacy scandal in which AOL Research published a compressed text file on one of its websites containing twenty million search keywords punched into AOL's search engine for over 650,000 AOL anonymous users over a 3-month period for research purposes, it was found possible to identify single users on the basis of the content of their combined search queries.[629] AOL ultimately apologized for the disclosure and recognized that it had violated the privacy of its users despite its attempts to anonymize the data.[630] Thus, although isolated pieces of information may not qualify as "personal", the context of such information, especially in light of profiling practices, may further bring the personal information within the meaning of the definition of "sensitive data".[631] The fact that there is a great volume of data easily available may further heighten the ability to trace personal information to an individual.[632]

A similar privacy concern can arise in the mobile space as discussed earlier. Location data may be anonymized by removing a phone number or other unique identifier of a specific mobile device, and instead replaced by a profile number (for example profile

[628] See Center for Democracy & Technology, *supra* note 204: "Use of the network, however, generates detailed information about the individual -- revealing where they 'go' on the Net (via URLs), who they associate with (via list-servs, chat rooms and news groups), and how they engage in political activities and social behavior"; Berman & Mulligan, *supra* note 204 at 554: "The data trail, known as transactional data, left behind as individuals use the Internet is a rich source of information about their habits of association, speech, and commerce. Transactional data, click stream data, or 'mouse droppings,' as it is alternatively called, can include the Internet protocol address ('IP address') of the individual's computer, the browser in use, the computer type, and what the individual did on previous visits to the Web site, or perhaps even other Web sites."

[629] While none of the records on the file were identifiable *per se*, certain keywords contain identifiable information by means of the user typing in their own name (ego-searching), as well as their address, social security number or by other means. Reporters from the *New York Times* quickly demonstrated that at least some of this information could easily be re-personalized. They were able to locate individuals from the released and anonymized search records by cross referencing them with phonebooks or other public records. This list, although quickly withdrawn by AOL recognising that it was an error, had by the time of the withdrawal reportedly been downloaded and re-posted many times, and made available in searchable form on a number of websites. See *Resolution on Privacy Protection*, *supra* note 177; See also Anderson, "AOL", *supra* note 178. See also Michael Barbaro & Tom Zeller, Jr., "A Face is Exposed for AOL Searcher No. 4417749", *New York Times* (9 August 2006) at A1.

[630] Anick Jesdanun, "AOL: Breach of Privacy Was a Mistake", *The Washington Post* (7 August 2006) at A1.

[631] See section 3.1.2.2 entitled "Risk of Subjective Harm: Revisiting the Sensitivity Criteria" which elaborates on the criteria to take into account when establishing the sensitivity of a given disclosure of information, namely the "identifiability" of the information, its "intimate" nature, as well as its "availability".

[632] See section 1.2.1.3 entitled "Easier Identification of Individuals" and section 1.2.3 entitled "New Identifying Methods" which elaborate on this issue.

ABC). If the location data collected is very accurate and collected over a long period of time, then one may be able to identify the identity of "profile ABC", spending every night at a specific location (i.e. place of residence) and spending the daytime at another location (i.e. work place).[633] A strict literal interpretation of the notion of *personal information* does not address these types of particular situations.

(c) Consequences of Under-Inclusiveness

The definition of *personal information*, if interpreted using a strict literal method, may prove to be under-inclusive. It may not cover certain information which, "on their own", do not qualify as such. It may also not govern certain profiles falling outside of the scope of the definition, although these profiles are otherwise used or disclosed, creating some type of privacy or other harm to the individuals behind the profiles. As further discussed in section 2.1.2.3.1, new technologies makes it possible to identify the behaviour of a machine (device, computer) and the behavior of the individual behind the machine. It may therefore be possible to recreate the personality of an individual in order to apply certain decisions to it without needing the identity (name and address) of this individual. There is always a face behind an online profile, even an anonymous one. The potential under-inclusiveness of the definition, with key forms of data outside the scope of protection, may lead to subjective or objective threats to individuals.[634]

***

In light of the above, the application of the definition of *personal information*, when using a literal interpretation, can lead to unpredictable or counterintuitive results. It can trigger over-reaching or under-reaching results. Any literal interpretation of the definition of *personal information* may create problems. A broad literal interpretation may create an undesired effect for online businesses or service providers that need this data but at the same time, a strict literal interpretation would trigger the situation where certain data that may not technically speaking be covered by the definition, may nonetheless breach the privacy of online users or cause other types of harm. It is

[633] See Gratton, "Personalization", *supra* note 16, which discusses this example.

[634] See section 3.1 and section 3.2 which discuss these subjective and objective harms. See also section 2.2.1.4.3(b)(i) entitled "Protecting Privacy is Important" which discusses the importance of protecting the privacy of individuals.

therefore dubious whether using a literal approach to interpreting the definition of personal information is the right approach.[635] In 2007, the Article 29 Working Group issued an opinion on the concept of "personal data" in which they propose a more relative interpretation of the definition.[636] In order to find that data *relates* to an individual, a *content* element, a *purpose* element or a *result* element should be present.[637] While the relative interpretation proposed by the Article 29 Working Group is more flexible than the literal one, the three criteria are still very broad, and this type of interpretation may definitely create over-inclusiveness with the problems already raised in section 2.1.2.1.1(d).[638]

2.1.2.2. Uncertainty Triggered by the Definition

Section 2.1.2.1 discussed potential over-reaching and under-reaching effects of DPLs when using a literal interpretation of the notion of *personal information*. In the present section, I will argue that the definition of *personal information* is also rather vague since it is not always clear at what point a piece of data can be said to be *identifying* an individual.[639] The OPCC has recently admitted that "It is not always straightforward to determine whether or not information is *personal information* for the purposes of PIPEDA."[640] Authors Patrick Lundevall-Unger and Tommy Tranvik ("Lundevall-Unger and Tranvik") rightfully articulate the view that:

---

[635] For instance, Google believes that nuanced analysis is required to apply the correct legal characterizations to IP addresses, rather than black-and-white labels. Google, *supra* note 280 at 6.

[636] Article 29 Data Protection Working Party, *Opinion 4/2007*, *supra* note 100.

[637] This means that data is personal data when it contains information about a specific person (content), when it is used or likely to be used to determine the treatment of a specific person (purpose), or when it is likely to have an impact on a specific person (result). See *ibid*.

[638] Certain authors have criticized these three criteria proposed by the Article 29 Working Party as they would be, in certain cases, over-inclusive, for instance with IP addresses which may eventually be assigned to vaious objects. Robinson et al., *supra* note 151 at 27: "Thus, IP addresses, user names or maps might not always be classified as personal data, the context within which the data is processed must be examined to determine whether one of the three criteria have been met. Determining what constitutes personal data becomes particularly acute in the context of mobile telecommunications, where a device with an IP address may easily be used by another entity. The problem is likely to get worse with IPv6, when IP addresses will become much more widely available and begin to be assigned to objects such as home appliances or cars."

[639] Bercic & George, *supra* note 574 at 235: "On the other hand, this definition is semantically also rather vague. Even if we accept the fact that content-wise every item of information can be considered personal data provided it can be related to an individual, the Directive's definition is still rather vague structurally since it is not always clear what kind of internal structure every 'record' of an individual has to have to be considered personal data."

[640] OPCC, *Handbook for Lawyers*, *supra* note 577 at 2.

> "The challenge for Fleischer, European data protection agencies and everybody else trying to determine which data are personal (and which are not), is to make sense of the Data Protection Directive's definition of what personal data is."[641]

Legal philosopher Jeroen van den Hoven ("van den Hoven") asks:

> "Personal data are and will remain a valuable asset, but what counts as personal data? If one wants to protect X, one needs to know what X is."[642]

First, the uncertainties relating to the notion of "identifiable" individual will be addressed, and then those relating to instances where data may instead relate to a device or an object instead of an individual.

2.1.2.2.1. Notion of Identifiable Individual

According to Canadian and French DPLs, *personal information* is generally any *information relating to an identified or identifiable natural person* (although it is to be noted that PIPEDA has dropped the notion of "identified" and only uses the notion of "identifiable").[643] The European definition of "personal data" is akin to that in PIPEDA. Under both definitions, personal information or personal data must be "in relation to" or "about" an "identifiable individual" or "natural person". This means that if the organization has information about an individual, and they know or can know who that individual is (for example, "a name and a face" has been associated with the information), then that information is personal information and is governed by the relevant DPL. On the other hand, if an organization has information about an individual, but it is impossible (or very difficult) for the organization to find out who that individual is, then the information is not personal information, and therefore not governed by DPLs.

---

[641] Patrick Lundevall-Unger & Tommy Tranvik, "IP Addresses: Just a Number?" (2011) 19:1 International Journal of Law and Information Technology 53 at 3.

[642] Jeroen van den Hoven, "Information Technology, Privacy, and the Protection of Personal Data" in Jeroen van den Hoven & John Weckert, eds., *Information Technology and Moral Philosophy* (New York: Cambridge University Press, 2008) 301 at 307 [Van den Hoven, "Information Technology"].

[643] See section 1.1.3 entitled "Definition of Personal Information: Origin and Background" which elaborates on this issue. EC, *Directive 95/46/EC*, *supra* note 99 at art. 2 (a) further states that "(…) an identifiable person is one who can be identified, directly or indirectly, in particular with reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity".

Bennett Moses suggests that with technological changes, the problem is often not with placing a new artifact, activity or relationship into a pre-existing category, but rather with the category itself and that some legal categories and concepts become ambiguous in light of technological change.[644] I maintain that this may well be the case with the definition of *personal information* that relates to an "identifiable individual".

In Canada, the OPCC has made several rulings affirming that *personal information* is information *about a particular individual*, not that the information must, at that time nor even in some realistically likely fashion in the future, ever be capable of, on its own or combined with other information, identifying that person.[645] The OPCC has therefore proposed a very broad interpretation of the term "identifiable", which may ultimately lead to an over-inclusive outcome. In Canada, there is no further guidance to assist organizations or courts to determine what needs to be taken into account when assessing if a certain piece of information is "identifiable" such as they have in Europe. As a matter of fact, recital 26 of the Directive 95/46/EC pays particular attention to the term "identifiable" and reads as follows:

> "whereas to determine whether a person is identifiable account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person."[646]

It is often unclear whether certain types of data that may be generated on the Internet or through new technologies are included under the current definition since the notion of "identifiable individual" can be interpreted in many different ways.[647] The Article 29

---

[644] Bennett Moses, *supra* note 552 at 46: "For instance, had bubble cars and hover cars been invented when the hypothetical 'no vehicles in the park' rule was enacted, the rule may have been worded differently. Technological change has the effect of upsetting the balance reached at the time of the rule's creation."

[645] See OPCC findings in OPCC, *PIPEDA Case Summary #2009-002, Realtor advertises purchase price of condominium in trade publication without buyer's consent* (20 February 2009); OPCC, *PIPEDA Case Summary #2008-390, Residential Property Appraisal Documents are Owners' Personal Information* (7 May 2008); OPCC, *PIPEDA Case Summary #2006-349, Photographing of tenants' apartments without consent for insurance purposes* (24 August 2006). In *PIPEDA Case Summary #2006-349*, the OPCCC mentioned that the individual must be "identifiable," not necessarily *identified*.

[646] See EC, *Directive 95/46/EC*, *supra* note 99 at recital 26.

[647] Robinson et al., *supra* note 151 at 27: "(…) the notion of personal data is extremely broad and subject to much debate. Some argue that any data that could be linked to a specific individual should be considered as personal data. Under this absolute interpretation, Internet Protocol (IP) addresses are personal data, regardless of whether the entity processing them has a realistic possibility of linking them to a given individual. (…) However, regardless of how rigorously the data is de-personalised, legally speaking under this absolute interpretation it remains personal data if there is a possibility of linking the data to an individual, however remote, difficult or complex that may be."

Working Party in Europe has conducted an analysis of the concept of "personal data" since they noticed that current practices in EU Member States suggested that there was some uncertainty on this issue and more specifically with the notion of "identity".[648] This uncertainty (whether certain types of data are covered by the definition) was raised back in 1998 by Joel Reidenberg ("Reidenberg") and Schwartz in their study addressing various key legal aspects of data protection and online services. According to Reidenberg and Schwartz, the determination of whether particular types of information related to an "identifiable person" in accordance with Directive 95/46/EC was unlikely to be straightforward.[649] More recently, Schwartz and Solove have suggested that the concept of "identifiability" is complex in part because of the changing landscape of technology.[650]

An illustration of the uncertainty raised by certain pieces of data can be made with IP addresses.[651] As a matter of fact, European privacy advocates don't even agree on whether IP addresses constitute personal data. While some argue that IP addresses should qualify as "personal data" under Directive 95/46/EC,[652] European officials are not consistent on the question. Courts and regulators in Sweden[653] and Spain[654] hold that IP addresses fall within Directive 95/46/EC. In Germany[655] and the U.K.,[656] the

---

[648] Article 29 Data Protection Working Party, *Opinion 4/2007*, *supra* note 100 at 3: "The Working Party is aware of the need to conduct a deep analysis of the concept of personal data. Information about current practice in EU Member States suggests that there is some uncertainty and some diversity in practice among Member States as to important aspects of this concept which may affect the proper functioning of the existing data protection framework in different contexts."

[649] Reidenberg & Schwartz, *supra* note 203 at 23.

[650] Schwartz & Solove, *supra* note 529 at 29-30.

[651] Lundevall-Unger & Tranvik, *supra* note 641 at 1.

[652] Article 29 Data Protection Working Party, *Opinion 4/2007*, *supra* note 100 at 21; Electronic Privacy Information Center, "Search Engine Privacy", online: <http://epic.org/privacy/search_engine>.

[653] John Oates, "Sweden: IP Addresses are Personal… Unless You're a Pirate" (18 June 2009), online: The Register <http://www.theregister.co.uk/2009/06/18/sweden_ip_law>.

[654] Agencia Española de Protección de Datos, Statement on search engines (2007), online: <http://www.samuelparra.com/agpd/canaldocumentacion/recomendaciones/common/pdfs/declaracion_aepd_buscadores_en.pdf>. The opinion of Spanish Data Protection Agency states that search engines process "personal data," relying in part on earlier rulings about IP addresses.

[655] Posting of Jeremy Mittma, "German Court Rules That IP Addresses Are Not Personal Data" (17 October 2008), online: Proskauer Privacy Law Blog <http://privacylaw.proskauer.com/2008/10/articles/european-union/german-court-rules-that-ip-addresses-are-not-personal-data>. At the same time, Peter Scharr, Germany's data-protection commissioner, has articulated the view in January 2008 that an IP address should be considered personal data. See: Aoife White, "IP Addresses Are Personal Data, E.U. Regulator Says", *Washington Post* (22 January 2008) at D01.

opposite position is favoured. Even within the same jurisdiction, certain courts don't always agree on whether IP addresses are *personal information*. French courts are not unanimous on the issue. The Cour d'appel de Paris in April and May 2007 took the position that IP addresses were not personal information.[657] In August 2007, the French CNIL issued a press release voicing concern over these two decisions and stating that IP addresses should be considered as *personal information*.[658] In May 2008, the Cour d'appel from Rennes decided that IP addresses were personal information.[659] In January 2009, the Cour de cassation reversed this decision, stating that IP addresses did not constitute personal information.[660] In June 2009, the Tribunal de Grande Instance from Paris took the position that IP addresses are indeed personal information.[661] In February 2010, the Paris Appeal Court, re-aligning with the position of the Cour de Cassation, took the position that IP addresses were not personal information.[662] An analysis of this case law shows that although these French cases all shared similar facts, it was the literal interpretation of the definition (either strict or broad) of *personal information* which was inconsistent throughout French courts and therefore triggered contrary decisions on the same issue, within the same jurisdiction.

---

[656] Information Commissioner's Office, *Personal Information online, Code of Practice,* U.K., July 2010, at 9-10.

[657] CA Paris, 27 April 2007, No. 06/02334 [CA Paris, No. 06/02334]; CA Paris, 15 May 2007, No. 06/01954 [CA Paris, No. 06/01954]: "L'adresse IP ne permet pas d'identifier le ou les personnes, qui ont utilisé cet ordinateur puisque seule l'autorité légitime pour poursuivre l'enquête (police ou gendarmerie) peut obtenir du fournisseur l'accès d'identité de l'utilisateur."

[658] Commission nationale de l'information et des libertés (France), "L'adresse IP est une donnée à caractère personnel pour l'ensemble des CNIL européennes" (2 août 2007), online : CNIL <http://www.cnil.fr/la-cnil/actu-cnil/article/article/ladresse-ip-est-une-donnee-a-caractere-personnel-pour-lensemble-des-cnil-europeennes/>.

[659] CA Rennes, 22 May 2008, No. 07/01495: "L'adresse IP de l'internaute, constitue une donnée indirectement nominative car, si elle ne permet pas par elle-même, d'identifier le propriétaire du poste informatique, ni l'internaute ayant utilisé le poste et mis les fichiers à disposition, elle acquiert ce caractère nommatif par le simple rapprochement avec la base des abonnés, détenue par le fournisseur d'accès à internet."

[660] Cass. crim., 13 January 2009, No. 08-84088: "L'adresse IP n'est donc pas une donnée à caractère personnel, car elle n'identifie pas une personne mais un ordinateur. Par contre il s'agit bien, au même titre que le numéro de la plaque d'immatriculation d'un véhicule, d'une donnée à caractère personnel indirecte."

[661] Trib. gr. inst. Paris, 24 June 2009, *Jean-Yves Lafesse et autres c. Google et autres*: "Le tribunal considère que l'adresse IP est une donnée personnelle puisqu'elle correspond à un numéro fourni par un fournisseur d'accès à internet identifiant un ordinateur connecté au réseau; elle permet d'identifier rapidement à partir de services en ligne gratuits le fournisseur d'accès du responsable du contenu qui délient obligatoirement les données nominatives du responsable du contenu, c'est-à-dire son adresse et ses coordonnées bancaires."

[662] CA Paris, 1 February 2010, *Cyrille S. c. Sacem*.

This legal uncertainty is problematic for organizations that manage personal information, since they do not know if the data that they are handling is personal information, in which case they would have an obligation to comply with the relevant DPLs. Section 2.1.2.1.1(d) discusses the challenges brought about by the over-inclusiveness of the definition for organizations that need this data. Similar consequences can take place when there are uncertainties around which piece of data are governed by the relevant DPL. Organizations will not know whether they should be incurring costs for complying with DPLs (invest in appropriate security measures to protect the data managed, etc.) since they will not know whether their activities are governed by DPLs. In the event that they are to comply with the applicable DPL, this implies certain obligations for an organization managing this data such as providing a privacy policy (disclosing their privacy practices) pertaining to the collection and use of these new types of data and obtaining consent from individuals.[663] They may also have to grant access to this data to individuals requesting it.[664] Also, organizations handling data have obligations regarding the retention, destruction or the anonymisation of the data in certain situations (i.e. when the data is no longer necessary for the purposes for which it was collected or further processed),[665] and therefore need to know at what point the data is in fact considered as being anonymised.

To illustrate these uncertainties, the following sections will address how it is not always clear what kind of resources should be expended by an organization in order to determine if certain data is "personal", where we should draw the line separating personal from anonymous data and whether the data should be evaluated by itself, or taking into account other readily available data.

(a) Identifiable Taking Into Account Illegal Means?

A important issue is whether we need to take into account the "possibility" of a security breach when evaluating the data, whether the data should be evaluated taking into account the possibility of an illegal act rendering certain pieces of data "identifiable",

---

[663] See section 2.1.1.2 entitled "Notice and Choice Approach Challenged" which elaborates on these obligations.

[664] See section 2.2.1.3.2(a)(v) entitled "Subjectivity in Access Rights and Data Quality" which elaborates on this issue.

[665] PIPEDA, *supra* note 63 at Schedule 1 (s. 5), principle 4.5.3; See Alberta DPL, *supra* note 114 at Part 3, Division 2, s. 34.1 (1); B.C. DPL, *supra* note 115 at Part 9, s. 35 (2) (a), (b); *Loi informatique et liberté*, *supra* note 131 at V, s. 1, art. 32 (IV); EC, *Directive 95/46/EC*, *supra* note 99 at art. 6 (1) (e).

whether the mere possibility–a third party giving illegal access to identifying information – be enough to qualify strings of non identifying numbers as personal data. Given that there is always a possibility, either technical (security breach) or illegal (illegal transfer of information that may allow the identification of additional information) this question is extremely relevant.

The Article 29 Working Party seems to take the position that illegal means should be taken into account when evaluating whether data is *personal* when it reasons that IP addresses should (almost) always and everywhere be regarded as personal data, "in order to be on the safe side".[666] In the context of IP addresses, this would mean that given that the ISP may illegally disclose the owner of the web account that can be associated with a certain IP address at a given time would be sufficient to make all IP addresses qualify as *personal information* which may create a very burdensome framework.[667] But various case law rendered in Europe, which were rendered evaluating article 2 of the Directive 95/46/EC (definition of *personal data*) with recital 26, also adhere to this view.

In a case argued before the District Court and the Regional Court of Berlin and pertaining to the legal status of IP addresses, the court emphasized that illegal means of linking "names and faces" to IP addresses should not be excluded from the decision-making process.[668] In a trial case in 2005, the Stockholm Lænsrætt landed on the same conclusion as the District Court and the Regional Court of Berlin did two years later: dynamic IP addresses in the hands of Internet portal or website operators are personal data and illegal means should not be excluded from the assessment.[669]

But the case law rendered on this issue in Europe is contradicting. As a matter of fact, the Paris Appeal Court, in two cases already discussed above, which concern the alleged infringement of copyright by members of a file-sharing network published in

---

[666] See Article 29 Data Protection Working Party, *Opinion 4/2007*, *supra* note 100 at 17: "So, unless the Internet Service Provider is in a position to distinguish with absolute certainty that the data correspond to users that cannot be identified, it will have to treat all IP information as personal data, to be on the safe side." See also the Article 29 Data Protection Working Party, *Working Document: Privacy on the Internet: An Integrated EU Approach to Online Data Protection*, [2000] 5063/00EN/FINAL, WP 37, at 21-23.

[667] See sections 2.1.1.1 entitled "Privacy as an Absolute Right" and section 2.1.2.1.1 entitled "Potentially Over-Inclusive Definition" which elaborate on this burdensome framework.

[668] District Court Berlin-Mitte, 27 March 2007, 5 C 314/06 [District Court Berlin-Mitte, No. 5 C 314/06].

[669] Stockholm Lænsrætt, 8 June 2005, No. 593-2005 [Stockholm Lænsrætt, No. 593-2005].

April and May 2007, rejected the complainants' arguments, and ruled that IP addresses are not *personal data* arguing that illegal means of unmasking the users of IP addresses should play no part in the "identifiability" assessment: The IP address does not allow the identification of the individuals using the computer since only the legitimate authority of investigation (the law-enforcement authority) may obtain the user identity from the ISP.[670] In a 2008 court case, the District Court of Munich also concluded that dynamic IP addresses are not *personal data*, on the basis that IP addresses are characterized by what the court called "intrinsic determinability", and because dynamic IP addresses are not personal data because Internet portal or website operators cannot link "names and faces" to IP addresses by employing "normally available tools".[671] The court mentioned that "normally available tools" does not encompass illegal methods of identification, or, more precisely, the possibility that a third party – such as an Internet Access Provider – gives portal or website operators access to information about the identity of customers that have been assigned IP addresses by that particular access provider.[672] Certain authors, arguing that the term "normally available tools" is similar to the phrase "all the means likely reasonable to be used" in recital 26 of Directive 95/46/EC, believe that this case may provide guidance on this issue of whether when assessing if a certain piece of data qualify as *personal information*, we should take into account potential security breaches or illegal means of making this link.[673]

In another recent case, when it came to the transfer from Europe of key-coded clinical trial data to the United States, this question arose – whether illegal means should be taken into account when determining whether the information, which was anonymized,

---

[670] CA Paris, No. 06/02334, *supra* note 657; CA Paris, No. 06/01954, *supra* note 657.

[671] i.e. "names and faces" cannot be revealed without investing a disproportionate amount of resources in the identification process. District Court of Munich, 30 September 2008, 133 C 5677/08, online: Medien Internet und Recht <http://medien-internet-und-recht.de/volltext.php?mir_dok_id=1769>. In this case, the portal operator registered and stored IP addresses in log files, for the duration of an individual browsing session and also after the end of a session. The plaintiff argued that this violated the *German Data Protection Act* because the log files contained personal data (the processing of which is regulated by German law) since the dynamic IP addresses and other information (like date and time of use and websites visited) could unmask the identity of individual users.

[672] The District Court excludes the use of illegal methods of identification, particularly the possibility of getting unlawful access to unique and identifying information from a third party.

[673] Lundevall-Unger & Tranvik, *supra* note 641 at 11.

was personal or not.[674] Some European agencies interpreted this as a transfer of personal information because the clinical trial data had been "reversibly anonymized" given that the European investigator could replace the numerical code with the original and identifying information or that the trial persons could be identified by the American pharmaceutical company by this company illegally contacting someone from the European clinical trial investigator.[675] Other agencies, however, disagreed that key-coded data could be classified as personal, since they took the position that seen from the U.S. company's perspective, they argued, the data was anonymous, especially since the forwarding of additional, unique and identifying information by the European investigator to the US-based company would be illegal.[676] According to the EC and the EU Member States, illegal means were not to be taken into account and the legal requirements regarding the processing of personal data specified in the Directive 95/46/EC do not apply to the clinical trial data held by the U.S. pharmaceutical company.[677]

Dr. Patrick Ho, Hong Kong's former Secretary for Home Affairs, has also taken the position that the possibility of using illegal means to "identify" the individual behind an IP address should not be considered in the context of evaluating the status of IP addresses.[678] Other authors such as Lundevall-Unger and Tranvik also argue that

---

[674] This example is discussed in *ibid*. at 15. See also EC, *Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce*, [2000] O.J., L 215/7 [EC, *Commission Decision 2000/520/EC*]. To illustrate the challenge, the European Union's Commission and the Member States had to address an issue concerning the out-of-Europe transfer of key-coded clinical trial data back in 2000.

[675] See Richard Morgan & Ruth Boardman, *Data protection Strategy. Implementing Data Protection Compliance* (London: Sweet & Maxwell, 2003) at 40, discussed in Lundevall-Unger & Tranvik, *supra* note 641 at 15.

[676] U.S. companies would not be subject to the requirements of the Directive 95/46/EC but because of article 25 of this Directive they need to provide an adequate level of protection.

[677] Patrick Lundevall-Unger and Tommy Tranvik suggest that this implies that the European Commission and the Member States performed a "legality test" meaning that the illegal means of linking "names and faces" to key-coded clinical trial data was identified and excluded from the assessment process, leading to the conclusion that no transfer of personal data to the United States had occurred. See Lundevall-Unger & Tranvik, *supra* note 641 at 16: "The Commission and the Member States argued along the same lines as the District Court of Munich and the Paris Appeal Court; the possibility that the European investigator illegally forwards identifying information to the US-based company is not sufficient to classify the information in question as personal data."

[678] In a debate in Hong Kong's Legislative Council in May 2006, he made the following statement: "(…) the Privacy Commissioner for Personal Data considers that an IP address does not appear to be caught within the definition of personal data under the Personal Data Ordinance (…) to trace an account-user or the physical address of the user's computer that has made use of a particular IP address at a particular point in time, one must have the IP address, the time of use of the IP address and the appropriate IP

illegal means of linking "names and faces" to "name and faceless" IP addresses should never be taken into account when assessing whether or not IP addresses are personal data.[679] They believe that only legal methods of identification should form the basis of these decisions, but the views are not unanimous on this issue.

(b) At what costs and using what kind of efforts?

What kind of costs and resources should be used by an organization to determine if certain data can "identify" an individual and is therefore covered under the definition? The FTC, in its recent 2012 Report, states that: "One industry organization asserted, for instance, that if given enough time and resources, any data may be linkable to an individual".[680] With new, sometimes sophisticated, technologies and the Internet, web 2.0, OSNs and the new trend towards increased cross-site profile linkage, certain data that could not identify an individual may now be able to.[681] The degree difficulty in identifying an unknown Internet user that should be taken into account when decisions about the identifiability of individuals are made is not clear.

In 1980, Convention 108 clarified in its Explanatory Report that "identifiable persons" refer to individuals who can be "easily" identified and that it did not cover identification of persons "by means of very sophisticated methods".[682] But this Report does not elaborate on what "sophisticated methods" may entail. Some argue that these methods must consist of an assessment of factors like time, money, expertise and manpower.[683] Similarly, the Council of Ministers of the Council of Europe adopted (in 1997) a Recommendation on the protection of medical data which states that natural persons

---

assignment logs kept by the ISPs; the provisions of the Personal Data Ordinance together with the relevant license conditions in the PNETS- license issued to the ISPs should therefore be sufficient to prohibit the unauthorized disclosure of information collected by ISPs." As quoted in Press Resleases, "LCQ17: IP addresses as personal data" (3 May 2006), online: <http://www.info.gov.hk/gia/general/200605/03/P200605030211.htm>.

[679] Lundevall-Unger & Tranvik, *supra* note 641 at 6.

[680] Comment of GS1, cmt. #00439 at 2, discussed in FTC, *Recommendations* 2012, *supra* note 381 at 19-20.

[681] See section 1.2.1.3 entitled "Easier Identification of Individuals" which elaborates on this issue.

[682] Council of Europe, *Explanatory Report: Convention for the Processing of Individuals with regard to Automatic Processing of Personal Data*, ETS no. 108 at art. 2, s. 28.

[683] See, for instance, Christopher Kuner, *European Data Privacy Law and Online Business* (Oxford: Oxford University Press, 2003) at 50; See also Lee Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits* (The Hague: Kluwer Law International, 2002) at 43; See also more generally the Article 29 Data Protection Working Party, *Opinion 4/2007*, *supra* note 100, On the Concept of Personal Data.

are not identifiable "(...) if identification requires an unreasonable amount of time and manpower."[684] Many DPLs provide that "identification" must be subject to a reasonableness standard. More specifically, certain European DPLs also share this approach, or at least a similar "reasonableness approach". For example, a definition such as that given in the *German Federal Data Protection Act* could be used as a basis for this interpretation:

> "Depersonalisation means the modification of personal data so that the information concerning personal or material circumstances can no longer or only with a disproportionate amount of time, expense and labour be attributed to an identified or identifiable individual."[685]

The U.K. DPL has also adopted a similar "reasonableness" test since data are deemed personal if the individual to whom they relate is identifiable "from those data and other information in the possession or likely to come into the possession of the data controller".[686] In Slovenia, the DPL also specifies a reasonableness standard: "where the method of identification does not incur large costs or disproportionate effort or require a large amount of time".[687]

Directive 95/46/EC states at recital 26 that to determine whether a person is "identifiable", account should be taken of "all the means likely reasonably to be used" either by the controller or by any other person to identify the said person.[688] The Article 29 Working Party suggests that the criterion of *"all the means likely reasonably to be used*" should in particular take into account all the factors at stake, namely:

> "The cost of conducting identification is one factor, but not the only one. The intended purpose, the way the processing is structured, the advantage expected by the controller, the interests at stake for the individuals, as well as the risk of organizational dysfunctions (e.g.

---

[684] Council of Europe, Committee of Ministers, *Recommendation No. R (97) 5, On the Protection of Medical Data* at art. 1.

[685] The definition of "Rendering anonymous" in §3(6) of the *German Federal Data Protection Act,* German Federal Data Protection Act, The Federal Ministry of the Interior, January 1, 2002.

[686] *Data Protection Act 1998* (UK), c. 29 at s. 1(1) (a) and (b) [*UK Data Protection Act*].

[687] The *Personal Data Protection Act of the Republic of Slovenia*, No. 001-22-148/04, Llubljana, 23 July 2004, art. 6 (1) and (2).

[688] See EC, *Directive 95/46/EC*, *supra* note 99 at Whereas 26: "(…) whereas, to determine whether a person is identifiable, account should be taken of all the means *likely reasonably to be used* either by the controller or by any other person to identify the said person; whereas the' principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; (…)".

> breaches of confidentiality duties) and technical failures should all be taken into account."[689]

Still, the challenge is then to determine which means should be deemed "likely and reasonable". Lundevall-Unger and Tranvik ask:

> "Should sophisticated, cutting-edge and expensive means be included, or only off-the-shelf and inexpensive tools and methods (like cookies or super-cookies)? Moreover, should illegal means (for gathering additional and identifying information) be taken into account, or must the tools or methods used observe the letter of the law?"[690]

In Canada, jurisprudence on the concept of *personal information* mentions that an individual will be "identifiable" where there is a serious possibility that they could be identified through the use of that information, alone or in combination with other available information.[691] Unfortunately this jurisprudence offers no further guidance on what kind of efforts should be undertaken by an organization to determine this notion of "serious possibility" or evaluate whether the information at stake qualifies as *personal information* in light of "other data available".

Certain other jurisdictions (such as France and Belgium) have interpreted *personal data* to mean that data will remain "personal" and subject to the full remit of the law if individuals remain in any way identifiable.[692] A few European courts have looked into this issue. In a case argued before the District Court and the Regional Court of Berlin, the court concluded that dynamic IP addresses must be considered *personal data* under the *German Data Protection Act* since all means of identification, regardless of whether these means are controlled by a third party (an Internet Access Provider) or by the portal operator himself, must be taken into account when making decisions about the identifiability of address-holders.[693] Thus, the only relevant criteria for evaluating the status of IP addresses according to them was the effort (or costs) involved in the

---

[689] Article 29 Data Protection Working Party, *Opinion 4/2007*, *supra* note 100 at 15.

[690] Lundevall-Unger & Tranvik, *supra* note 641 at 4 [footnotes omitted]

[691] See *Gordon*, *supra* note 576.

[692] This interpretation is discusses in Reidenberg & Schwartz, *supra* note 203 at 29.

[693] District Court Berlin-Mitte, No. 5 C 314/06, *supra* note 668. The plaintiff claimed that an Internet portal operator, by storing dynamic IP addresses, did not comply with the *German Data Protection Act* since these addresses had to be regarded as *personal data* especially since the portal operator's log files could reveal information about the Internet users' political or religious beliefs.

identification process.[694] In a trial case in 2005, the Stockholm Lænsrætt landed on the same conclusion: dynamic IP addresses in the hands of Internet portal or website operators are personal data, since portal or website operators could, without investing too much effort, contact a third party (an Internet Access Provider) and get illegal access to identifying billing information controlled by that third party.[695] In both these cases, the issue of identifiability is reduced to a "likely reasonable" test and it is the amount of effort or costs needed to link "names and faces" to IP addresses that is used as the sole criteria for separating personal from anonymous data.[696]

In the context of online services, this would mean that the traceability of any information back to an individual can qualify that information as *personal*, even if the entity processing that information does not actually know the identity of the data subject. No distinction is made between information that can easily be linked to an individual and information that can only be linked with extraordinary means or with the cooperation of third parties.[697]

Under this interpretation, every organization doing business on the Internet collecting or using these new types of data would have to be sure that there is no conceivable method, *however unlikely in reality*, by which the identity of individuals could be established. This may be a highly impractical approach, usually requiring considerable resources to be implemented.[698]

For instance, in the case of *clickstream* data, since it may ultimately be traced back to an individual, it will be covered by the definition regardless of the practical difficulties and incentives inhibiting actual traces of *clickstream* data back to particular

---

[694] According to Patrick Lundevall-Unger and Tommy Tranvik, this implies, for instance, that since the illegal transfer of identifying data from an Internet Access Provider to a portal operator would not strain the resources of either party (a telephone call or an exchange of e-mails is enough), then the "name and faceless" IP addresses stored by that portal operator are personal data (even if the portal operator has no interest in finding out the identity of individual address-holders). Lundevall-Unger & Tranvik, *supra* note 641 at 12.

[695] See Stockholm Lænsrætt, No. 593-2005, *supra* note 669.

[696] There are also a few other cases where the IP-addresses-as-personal-data issue has been addressed. See Lundevall-Unger & Tranvik, *supra* note 641 at 13.

[697] Reidenberg & Schwartz, *supra* note 203 at 29.

[698] Fleischer, "IP addresses", *supra* note 610.

individuals.[699] Some claim that it is not a realistic possibility in many cases that the party holding the IP address could obtain the information needed to link the IP address with an individual.[700] But that possibility still exists. We can't help but wonder if this translates into *anonymized data* being also covered by the definition of *personal information*.

In a time where it is often possible, with a lot of resources and sophisticated technologies, to be able to link certain data to an individual, additional guidance is necessary in order to be in a position to determine how the notion of "identifiable" should be interpreted in the context of the Internet and new technologies. More specifically, it will become increasingly important to quantify the requisite efforts and resources needed to determine whether certain types of data qualify under the definition of *personal information*.[701]

(c) At what point is data anonymized?

This issue of identification is closely linked to the issue of anonymisation of personal information. Data rendered anonymous is usually no longer subject to substantive rights and obligations elaborated by DPLs. But more and more, there is a blurring of the distinction between personal and anonymized information. In Canada, in *PIPEDA Case Summary #2009-018*, the OPCC took the position that the Psychologist's

---

[699] Without the assistance of extra information-gathering devices (like cookies) or soliciting the help of a third party, it is impossible (at least for now) for Internet portal and website operators to identify individuals on the basis of IP addresses alone. Lundevall-Unger & Tranvik, *supra* note 641 at 7. As expressed by the United Kingdom's former Information Commissioner, Elisabeth France: "(…) it is hard to see how the collection of IP addresses without other identifying information would bring a website operator within the scope of the Data Protection Act of 1998." as quoted online: <http://www.out-law.com/page-8060>. See also Geaham J. H. Smith, *Internet Law and Regulation* (London: Sweet and Maxwell, 2007) at 694-97; Kuner, *supra* note 683 at 49-55.

[700] Even if identifying information collected by cookies, super-cookies and browser fingerprinting often make third party assistance unnecessary, business representatives, like the Business Software Alliance (<http://www.bsa.org>), highlights that this is far from always the case: "(…) there is not a realistic possibility in many cases that the party holding the IP address could obtain the information needed to link the IP address with an individual". The Business Software Alliance, "Online Security, Traffic Data and IP addresses" (2008) Review of the Regulatory Framework for Electronic Communications at 2, online: <http://www.statewatch.org/news/2008/oct/eu-datret-bas.pdf>; Robinson et al., *supra* note 151 at 27: "Anonymity in large datasets is also complicated. Healthcare research is one area that uses large sets of anonymised clinical data for statistical analysis, data mining etc. However, regardless of how rigorously the data is de-personalised, legally speaking under this absolute interpretation it remains personal data if there is a possibility of linking the data to an individual, however remote, difficult or complex that may be."

[701] I suggest that we need a set of additional criterias to provide guidance on this notion of "identifiability", which I will elaborate on in section 3.1.2.2.1.

anonymized peer review notes were the *personal information* of the patient.[702] While the psychologist argued that the notes did not contain sufficient information to identify the complainant to anyone receiving the information and considered them "anonymized" (and therefore, the complainant had no right of access to them), the OPCC disagreed since: "(…) de-identified data will not constitute "truly anonymous information" when it is possible to subsequently link the de-identified data back to an identifiable individual."[703] In Europe, according to the Article 29 Working Party, "anonymous data" in the sense of the Directive 95/46/EC would also be anonymous data that previously referred to an identifiable person, but "where that identification is no longer possible."[704] In the U.S., the FTC recently commented that "the traditional distinction between PII and non-PII continues to lose significance due to changes in technology and the ability to re-identify consumers from supposedly anonymous data"[705] and that "the traditional distinction between PII and non-PII has blurred and that it is appropriate to more comprehensively examine data to determine the data's privacy implications."[706]

Organizations may employ various techniques to "anonymize" (or de-identify) the personal information they collect before using the data or selling it to third parties. As a matter of fact, marketers and market researchers often attempt to quell privacy concerns by stating that they anonymize the data in their databases. To anonymize the data, details such as name, phone number and e-mail address may be stripped from the database. Data may be linked to a certain customer's name or IP address, which could in turn be directly linked to an individual. It may also be assigned a unique randomized number such as customer "ABC" who spent X amount of time on a certain website and purchased certain kinds of products. By omitting the name, address and

---

[702] OPCC, *PIPEDA Case Summary #2009-018, Psychologist's anonymized peer review notes are the personal information of the patient* (23 February 2009).

[703] *Ibid*.

[704] Article 29 Data Protection Working Party, *Opinion 4/2007*, *supra* note 100 at 21.

[705] See FTC Staff, *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising* (February 2009) at 25, online: <http://www.ftc.gov/os/2009/02/P0085400behavadreport.pdf>.

[706] See Comment of AT&T Inc., cmt. #00420, at 13-15; Comment of Center for Democracy & Technology (Feb. 18, 2011), cmt. #00469, at 3-4; Comment of CTIA - The Wireless Ass'n, cmt. #00375, at 3-4; Comment of Consumers Union, cmt. #00362, at 4-5; Comment of Electronic Frontier Foundation, cmt. #00400, at 1-4; Comment of Google Inc., cmt. #00417, at 7-8; Comment of Mozilla, cmt. #00480, at 4-6; Comment of Phorm Inc., cmt. #00353, at 3-4, discussed in FTC, *Recommendations* 2012, *supra* note 381 at 19.

IP address of the customer, the data may be considered to be non-personal according to DPLs.

A challenge is that anonymisation methods can vary. For example, Google and the Article 29 Working Party recently disagreed on what anonymisation of data actually means. After Google revealed its anonymisation process,[707] the Article 29 Working Party clarified that such a process must be "completely irreversible" for Directive 95/46/EC to no longer apply.[708]

Various studies have challenged the reliability of anonymization, demonstrating that by using publicly available data, anonymized information about a user's online history can be "de-anonymized" to identify users. For example, a few attempts to re-identify individuals through de-identified data have brought into question the effectiveness of current data de-identification techniques.[709] A recent case in point, further discussed in section 1.2.3.2, involves the identification of Netflix customers using anonymized data. This anonymized information, generally related to movie preferences, combined with digital trails left on blogs, chat rooms and Twitter were used to positively identify Netflix customers.[710] Yet another example is the work of former Apple engineer Warden who has spent some time harvesting and analyzing data (names, fan pages, and lists of friends) from some 215 million public Facebook profile pages,[711] which he analysed at

---

[707] Google, *Letter to the Article 29 Working Party in answer to their Letter dated May 16, 2007* (10 June 2007) at 5: "We are putting significant resources into creating processes for reliably anonymizing data. Although we are still developing our precise technical methods and approach, we can confirm that we will delete some of the bits in logged IP addresses (i.e., the final octet) to make it less likely that an IP address can be associated with a specific computer or user. And while it is difficult to guarantee complete anonymization, the network prefixes of IP addresses do not identify individual users. Logs anonymization will not be reversible. We will intentionally erase, rather than simply encrypt, logs data so that no one (not even Google) can read it once it has been anonymized. Finally, logs anonymization will apply retroactively and will encompass all of Google's search logs worldwide."

[708] Article 29 Data Protection Working Party, *Opinion 1/2008*, *supra* note 207 at 20: "Even where an IP address and cookie are replaced by a unique identifier, the correlation of stored search queries may allow individuals to be identified. (…) Anonymisation of data should exclude any possibility of individuals to be identified, even by combining anonymised information held by the search engine company with information held by another stakeholder (for instance, an internet service provider). Currently, some search engine providers truncate IPv4 addresses by removing the final octet, thus in effect retaining information about the user's ISP or subnet, but not directly identifying the individual. The activity could then originate from any of 254 IP addresses. This may not always be enough to guarantee anonymisation."

[709] For more examples of the process of re-identification, see the Electronic Privacy Information Center's webpage: <http://epic.org/privacy/reidentification/>.

[710] The 2006 Netflix case already discussed in section 1.2.3.2 is one of them.

[711] He was exploiting a flaw in Facebook's architecture to access public profiles without needing to be signed in to a Facebook account, effectively avoiding being bound by Facebook's Terms of Service preventing such automated harvesting of data. Warden, "harvest Facebook profiles", *supra* note 242.

an aggregate level.[712] When it was time to release the results of his researches, many claimed that this release may be harmful since individuals were still potentially identifiable or worse, there was the potential that this data could be used to help re-identify *other* datasets, ones that might contain much more sensitive data.[713] As a matter of fact, since restrictions on the collection and use of data become more lax once the "personal" aspect of the data is removed, the problem worsens as more and more data about online activity is collected, which once aggregated and analyzed, can serve to re-identify individuals quite accurately.[714]

Thus, even a small amount of de-identified data on an individual, once combined with another dataset available either publicly or privately through sale, may still serve to re-identify the individual. The 2006 AOL case already discussed in sections 1.2.1.3 as well as discussed in section 2.1.2.1.2(b) is another example of data (three-month record of 20 million web searches belonging to 657,000 U.S. subscribers), which could be identifiable because of the volume of data disclosed. While AOL attempted to protect its users' privacy by removing their screen names and IP addresses from the dataset, researchers were still able to identify individuals solely by analyzing the searches tied to their unique randomized customer identification number.[715] With the volume of data available, it is more easy than ever to identify individuals. A 2009 study by AT&T Labs and Worcester Polytechnic Institute found that OSNs leak personal information, raising the possibility that third party aggregators can potentially link social

---

[712] Warden, "split the US", *supra* note 244.

[713] Zimmer, "Pete Warden", *supra* note 245 : "(…) Warden's release of this dataset — even with the best of intentions — poses a serious privacy threat to the subjects in the dataset, their friends, and perhaps unknown others. Warden claims to be sensitive to the privacy of the subjects in the database, and in response he has removed the identifying URLs that are unique to each profile, but the dataset retains the subjects' names *(really!)*, locations, Fan page lists and partial Friends lists (I'm not sure what is meant by a 'partial' list of friends). So, obviously, individuals can be easily identified within the dataset. But that's not the greatest threat with the release of this data. What is most dangerous is its potential use to help re-identify *other* datasets, ones that might contain much more sensitive or potentially damaging data."

[714] See section 1.2.3 entitled "New Identifying Methods" which elaborates on this issue.

[715] Dolin, *supra* note 371 at 137: "Search queries may reveal quite sensitive information about the querier. One can imagine the potentially compromising nature of queries and result clicks: a spouse looking up STD's; a student seeking free copyrighted music or video downloads; someone inquiring about nuclear bomb or other WMD technology; a citizen posing questions about a political group within a country that disfavors or forbids it. Even though most queries are not directly associated with a particular person, corresponding identifying information can often be sufficient to figure out who the querier is, which can create a trail of sensitive information."

network identifiers to past and future website visits, thereby tracking a user's online activities.[716]

Ohm has recently published an article entitled "*Broken Promises of Privacy*" in which he articulates the view that we should abandon the very concept of PII since it is a fatally-flawed concept given that so much non-PII can be re-identified.[717] Although PII is not an identical notion to *personal information*,[718] this illustrates the kind of similar concerns that the U.S. notion of *personal information* is triggering. Amongst other things he refers to a landmark study by Latanya Sweeney entitled *Uniqueness of Simple Demographics in the U.S. Population*, which suggests that for 87 percent of the American population, no individual shares their specific combination of ZIP code, birth date (including year), and gender with any other individual.[719] Therefore, these three pieces of often easily accessible information would uniquely identify an individual.

With technologies that are becoming more and more sophisticated and may enable to link an individual to certain data, the notions of "identification" and "anynomisation" of data are being challenged. Experts claim that there is always a risk of re-identification with new technologies,[720] and that as the semantic web continues to evolve and tools become more sophisticated, re-identification arguably could become easier.[721]

---

[716] Lo, *supra* note 188 at 43, referring to: Thomas Claburn, "Social Networks Leak Personal Information" *InformationWeek* (24 August 2009), online: <http://www.informationweek.com/news/internet/social_network/showArticle.jhtml?articleID=219401268>. The study examined twelve social networking sites: Bebo, Digg, Facebook, Friendster, Hi5, Imeem, LinkedIn, LiveJournal, MySpace, Orkut, Twitter, and Xanga.

[717] Ohm, *supra* note 562 at 1742.

[718] PII stands for personally identifiable information and, in the U.S., PII is the term used in sectoral DPLs instead of *personal information* or *personal data*.

[719] Latanya Sweeney, "Uniqueness of Simple Demographics in the U.S. Population" (2000) Laboratory for Int'l Data Privacy, Working Paper LIDAP-WP4.

[720] Yet, as Joel Reidenberg and Paul Schwartz suggest, anonymity in a network environment is not necessarily absolute. The mapping functions that render data anonymous are not always irreversible. Reidenberg & Schwartz, *supra* note 203 at 34.

[721] Many authors including Khaled El Emam suggest that there is indeed evidence showing that it is often possible to re-identify data sets. He suggests that de-identification should be part of an overall risk management approach. He suggests that it should also be noted that the only way to have an absolute guarantee that no one will be re-identified in a database is not to disclose it, so the key issue is to decide what probability of success is acceptable risk. De-identification is probabilistic - it can ensure that the probability is below a certain value but cannot eliminate the risk to zero. According to him, if one's objective is (an unrealistic) zero risk, then that is rightfully a dead end. See Khaled El Emam, *De-identification Risk Assessment Model* (30 May 2009), online: www.healthinformation.ca; and Khaled El Emam, *De-identifying Health Data for Secondary Use: A Framework*, available at: <http://www.ehealthinformation.ca/documents/SecondaryUseFW.pdf>.

(d) Identifying alone or in correlation with other data?

The fact that there is a huge volume of data available that can be used to make a link between a piece of data and an individual[722] triggers a debate as to how certain pieces of data should be treated and what kind of correlation is needed between data and an individual in order for this data to qualify as *personal information*. In the U.S., the FTC has raised the issue as follows:

> "Another question is whether applying the framework to data that can be "reasonably linked to a specific consumer, computer, or other device" is feasible, particularly with respect to data that, while not currently considered "linkable," may become so in the future. If not feasible, what are some alternatives? Are there reliable methods for determining whether a particular data set is linkable or may become linkable?"[723]

As more pieces of *personal information* become available, it may become easier to link this data to other data since there will likely be more common data elements. As Paul Ohm notes : "The accretion problem is this: Once an adversary has linked two anonymized databases together, he can add the newly linked data to his collection of outside information and use it to help unlock other anonymized databases." [724]

Although the definition of *personal information* doesn't discuss correlation of data, the fact that it has to be able to "identify" an individual clearly suggests that a correlation is needed as further discussed in section 2.1.2.1.1(b). Older documents and reports including the 1978 Lindop Report and the 1973 U.S. Report on *Records, Computers and the Rights of Citizens* mention the necessity for correlation.[725] Therefore, the "correlation" between at least two pieces of data is an underlying criteria necessary for the data to be able to "identify" an individual.

In a recent complaint, the Hong Kong Privacy Commissioner took issue with Yahoo!'s disclosure of information about a journalist to Chinese authorities; taking the position that an IP address *per se* does not meet the criteria of *personal data* since it refers to

---

[722] See section 1.2.1 entitled "Increase in Volume of Information" which elaborates on this issue.

[723] FTC, Preliminary Staff Report, *supra* note 372 at 43.

[724] Ohm, *supra* note 562 at 1746.

[725] Lindop, *supra* note 96 at 154, para. 18.27. See also U.S. Department of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *supra* note 57 at s. IV.

an inanimate computer, not an individual.[726] This Commissioner articulated the view that and IP address alone can neither reveal the exact location of the computer concerned nor identify the user of the computer.[727] Nevertheless, he suggested that in the hands of an ISP, an IP address can become personal data when combined with other information that is held by the ISP (customer's name and address) and in the hands of a website operator, it can become personal data through user profiling. This type of reasoning rightfully implies that data should be evaluated taking into account the other data any given IP address may be easily correlated with.

The definition as it stands now does not provide clear guidance as to whether correlation is needed between two pieces of information when evaluating them and, if so, whether the correlation should be made taking into account third party data.[728] If one was to take the position that correlation needs to be taken into account, then we must determine what kind of correlation is necessary in order for the information to qualify as *personal*. Some believe that only the data actually available to the data controller should be taken into account.[729] Others such as U.K. privacy expert Chris Pounder ("Pounder"), Reidenberg and Schwartz suggest that the data "likely to become available" to the data controller should be taken into account.[730] Finally, some such as the Article 29 Working Party take the position that data in the hands of third

---

[726] Office of the Privacy Commissioner for Personal data, Hong Kong, *Report Published under Section 48 (2) of the Personal Data (Privacy) Ordinance (Cap. 486), Report Number R07-3619* (14 March 2007) at 30-31, para. 8.11: "In order to constitute 'personal data' under the Ordinance, the data must satisfy three criteria laid down in the Ordinance, namely, that (a) it relates directly or indirectly to a living individual; (b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and (c) in a form in which access to our processing of the data is practicable. The word 'practicable' is further defined under section 2(1) as 'reasonably practicable'."

[727] *Ibid*. at 30, para. 8.10.

[728] Lundevall-Unger & Tranvik, *supra* note 641 at 4. These authors ask: "which third parties, possessing potential means of identification, should be included when determining the question of identifiability?".

[729] CPO of Google seems to suggest that only the data available to the data controller should be taken into account. See Fleischer, "IP addresses", *supra* note 610.

[730] For example, in the U.K., personal data means data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, "or is likely to come into the possession of, the data controller": *Data Protection Act 1998*, *supra* note 686 at s. 1(1) (a) and (b). According to Chris Pounder, this would mean for example, in the context of the IP address, that the question is whether the individual is identifiable not from the IP address but rather "from other information in the possession of Google" (e.g. a history of transactions). See Chris Pounder in answer to blog: Alma Whitten, "Are IP addresses personal?" (22 February 2008), online: Official Google Blog <http://googlepublicpolicy.blogspot.com/2008/02/are-ip-addresses-personal.html>. See also Reidenberg & Schwartz, *supra* note 203 at 41-42. These authors mention how the U.K. treats telephone numbers, how these are generally viewed as personal information when they refer to an individual subscriber but that work numbers can become personal information depending on the circumstances depending on whether a it is attributed to a specific person, etc.

parties should be taken into account as well.[731] Peter Fleischer, CPO of Googe Inc. disagrees with this last interpretation.[732]

We can also wonder if illegal ways of obtaining additional information (to be used to correlate with other data in order to be able to identify an individual) should be taken into account when determining whether certain data qualify as *personal*. This issue of illegal means is further discussed in section 2.1.2.2.1(a). Therefore there are still various unresolved uncertainties on the notion of "identifiable individual".

2.1.2.2.2. Identifying a Device or an Object

In some situations, information may be considered to be *personal* regardless of whether or not the person associated with that information has actually been identified. As a matter of fact, according to the definition of personal information, it is usually sufficient that the individual be "identifiable". The fact that information may be linked to a device or an object therefore raises various uncertainties since it is not always clear at what point this data identifies an individual using the device or object.

To illustrate this uncertainty, this section will first discuss the fact that it is not always clear if new types of data are or should be regulated as *personal information* under DPLs. Then, this section will discuss issues pertaining to at what point information linked to a device (which device may be used by more than one individual) should qualify as *personal information.* Finally, I will discuss the uncertainty regarding the need for an "accurate" link between a piece of data and an individual in order for this data to qualify as *personal information*.

---

[731] Article 29 Data Protection Working Party, *Opinion 4/2007*, *supra* note 100 at 17: "So, unless the Internet Service Provider is in a position to distinguish with absolute certainty that the data correspond to users that cannot be identified, it will have to treat all IP information as personal data, to be on the safe side." These considerations will apply equally to search engine operators. See: Article 29 Data Protection Working Party, *Opinion 1/2008*, *supra* note 207 at 8. Article 29 Data Protection Working Party, *Opinion 2/2002: The Use of Unique Identifiers in Telecommunications Terminal Equipments: the Example of IPv6*, [2002] 10750/02/EN/Final, WP 58, at 3, footnote 4: "As recital 26 of Directive 95/46 specifies, data are qualified as personal data as soon as a link can be established with the identity of the data subject (in this case, the user of the IP address) by the controller or any person using reasonable means. In the case of IP addresses the ISP is always able to make a link between the user identity and the IP addresses and so may be other parties, for instance by making use of available registers of allocated IP addresses or by using other existing technical means."

[732] Fleischer, "IP addresses", *supra* note 610: "The Working Party have assumed that if an IP address is identifiable by one company (e.g., an ISP) it is personal data as far as all other companies are concerned, even if they have no access to the information that permits an association to the individual. But this assumption is very questionable."

(a) Dealing With New Types of Data

In the context of the Internet, new types of data or collection tools may relate to an inanimate object. Part of the uncertainty therefore results from the fact that these new types of data or tools are more and more divorced from a unique and identifiable individual. They may relate to a machine (clickstream data or data collected from cookies), to an Internet connection (IP address) or a web account. Other types of data relating to ambient technologies may relate to a wireless device (ex: location data) and an object (ex: RFID).[733] These devices or objects may be used by one or more individuals. Also, some of this new data, or profiles derived from this data, are not created only by individuals. For instance, web-browsing information is created from the interaction between users and websites.[734] The market value of this information often results in the third party compiling the information.[735]

In the debate on the status of IP addresses, we can note the stance taken by certain French courts. In determining that IP addresses did not qualify as *personal information*, these courts did not take the correlation of information into consideration – only the IP address in and of itself was evaluated.[736] Since this data merely identified a machine, it did not qualify under the definition. In July 2009, a Seattle court also took the position that IP addresses are not personal information based on the same premise, since they can only identify a computer.[737]

---

[733] Article 29 Data Protection Working Party, *RFID technology*, *supra* note 196.

[734] See Jerry Kang, "Information Privacy in Cyberspace Transactions" (1998) 50 Stan. L. Rev. 1193 at 1202, 1246.

[735] See Miller, *supra* note 57 at 213. For example, Solove suggests that the value of personal information for advertisers and marketers emerges in part from their consolidation and categorization of that information. Solove, "Conceptualizing", *supra* note 23 at 1113.

[736] See section 2.1.2.2.1 entitled "Notion of Identifiable Individual" which elaborates on this issue.

[737] In the context of a class-action lawsuit brought by consumers against Microsoft stemming from an update that automatically installed new anti-piracy software, consumers alleged that Microsoft violated its user agreement by collecting IP addresses in the course of the updates. The consumers argued that Microsoft's user agreement only allowed the company to collect information that does not personally identify users. Microsoft argued that IP addresses do not identify users because the addresses don't include people's names or addresses. The company also said that it did not combine IP addresses with other information that could link them to individuals. See: Wendy Davis, "Court: IP Addresses Are Not 'Personally Identifiable' Information" (6 July 2009), online: Online Media Daily <http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=109242>. The Seattle judge stated: "In order for 'personally identifiable information' to be personally identifiable, it must identify a person. But an IP address identifies a computer."

A current tendency from the industry is to consider that unique identifiers, and basic biographical information pertaining to these unique identifiers, do not refer to identifiable individuals.[738] The notion of "identity" is therefore being interpreted restrictively by the industry. For example, the potential merging of databases between Abacus and DoubleClick in 2000 was aborted due to public pressure.[739] It was initially surprising that such a merger of databases was even technically possible. The database from Abacus consisted of biographical information and Double Click claimed to collect anonymous profile information.[740] Authors suggest that Double Click was still collecting some type of unique identifiers, probably the identifying cookie installed on millions of PCs, that enabled them to make a link between the data collected and an individual.[741]

New types of data may, in certain cases, identify an individual, especially with new identification tools that exist today[742] or with the volume of data available.[743] While this new data may be used and processed in some cases without technically speaking being covered by the definition of *personal information*, the processing of such data may result in obtaining sensitive information pertaining to a given profile. For this reason, the OPCC has taken the position that information involved in online tracking and targeting for the purpose of serving behaviourally targeted advertising to individuals should generally constitute *personal information.*[744] It is also possible to

---

[738] Conseil de l'Europe, *L'autodétermination informationnelle*, *supra* note 20 at 31.

[739] Macavinta, *supra* note 229. See also, online: <http://www.privacilla.org/business/online/doubleclick.html>.

[740] Conseil de l'Europe, *L'autodétermination informationnelle*, *supra* note 20 at 31 : "DoubleClick does not collect any personally-identifiable information about you, such as your name, address, phone number or email address."

[741] *Ibid*.

[742] See section 1.2.3 entitled "New Identifying Methods" for details.

[743] See section 1.2.1 entitled "Increase in Volume of Information" which elaborates on this issue.

[744] OPCC, *Online Behavioural*, *supra* note 275: "PIPEDA defines personal information as 'information about an identifiable individual'. Information will be about an identifiable individual where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information. A prominent strategic element of online behavioural advertising comes from the tailoring of advertisements based on an individual's browsing activities, which could include purchasing patterns and search queries. Given the scope and scale of information collected, the powerful means available for aggregating disparate pieces of data and the personalized nature of the activity, it is reasonable to consider that there will often be a serious possibility that the information could be linked to an individual. As such, we take the position that the information involved in online tracking and targeting for the purpose of serving behaviourally targeted advertising to individuals will generally constitute personal information."

recreate the personality of an individual behind a given profile in order to apply certain decisions to it without needing the identity (name and address) of this individual.[745] Therefore, the interpretation of the notion of *personal information* should take this into account.

(b) Device Used by a Group: At What Point is it Identifiable?

An issue comes from the fact that the same information can be *personal* to more than one individual.[746] Solove suggests that personal information rarely belongs to just one individual; it is often formed in relationships with others.[747] This may be especially true with new types of data, for example those collected by cookies or IP addresses, which do not independently identify any particular user as they pertain to the use of a particular device rather than use by a particular person. Data generated through the use of such a device may be the result of interventions by a number of individuals; perhaps the members of an extended family each making use of a home PC, a whole student body utilising a library computer terminal, or potentially hundreds of people purchasing from a networked vending machine. At what point should the data collected by cookies or pertaining to IP addresses be qualified as *personal*?

In certain cases, the cookies or IP addresses will be linked with additional information such as a web user account. The data collected would therefore identify an individual since there can logically be an assumption that the data relates to a specific individual, the owner of the web account.[748] As for other cases, the interpretation to be given to

---

[745] See section 2.1.2.3.1 entitled "Notion of Identity Obsolete in Certain Situations" for details on this issue.

[746] See *Wyndowe*, *supra* note 560 at para. 50; See also *Canada (Information Commissioner) v. Canada (Minister of Ctizenship and Immigration)*, 2002 FCA 270 (CanLII) at para. 8.

[747] Solove, "Conceptualizing", *supra* note 23 at 1113: "An example of the difficulty in assigning ownership to information is illustrated by *Haynes v. Alfred A. Knopf, Inc.* 8 F.3d 1222 (7th Cir. 1993) (Posner, J.). This case involved Nicholas Lemann's highly praised book about the social and political history of African Americans who migrated from the South to northern cities. The book chronicled the life of Ruby Lee Daniels, who suffered greatly from her former husband Luther Haynes's alcoholism, selfishness, and irresponsible conduct. Haynes sued the author and the publisher under the public disclosure of private facts tort, claiming that he had long since turned his life around and that the disclosure of his past destroyed the new life he had worked so hard to construct.(…)" According to Solove, although it did not hinge on the shared nature of the information, this case illustrates that personal information rarely belongs to just one individual; it is often formed in relationships with others.

[748] Joel Reidenberg and Paul Schwartz suggest that, to be able to identify a particular user, the information in the cookie file must be linked with other data such as a registration entry at the web site, which is increasingly a typical practice for websites. See Part II, New York Times case study and see: Reidenberg & Schwartz, *supra* note 203 at 31. In Canada, the Commissioner was satisfied In PIPEDA Case Summary No 2003-162 that the information stored by the temporary and permanent cookies qualified as *personal information* for the purposes of PIPEDA as it pertained to a website customer's profile, which was created

the definition is not clear. For instance, during the hearing which came against the backdrop of the European Commission's ongoing investigation into the merger of Google and DoubleClick, Peter Scharr acknowledged that IP addresses for some computers, such as those in Internet cafes, may not be linked to an individual – and thus may not be *personal information*, but that if an individual uses the same computer on a regular basis, then the IP address could be used to associate the individual with the computer.[749] This implies a "case by case" methodology, which requires some type of flexibility and guidance which is not offered by the current definition of *personal information*, at least when using a literal interpretation.

Some have interpreted the definition of *personal information* to mean that an identifiable individual exists when the information in question relates to this person and only to this person.[750] This interpretation implies that information needs to be unique in order to be *personal*. In the context of the Internet, with new types of data belonging in certain cases to a device that may be used by more than one individual, it may be a challenge to demonstrate that they are unique to a certain individual. For *clickstream* data associated with a group of individuals, will the information be considered anonymous if the aggregation is small?

Certain authors take the position that if an object or device is linked to a small number of individuals, it should be treated as *personal data*.[751] In France, the CNIL rejected a proposed intelligent transport system in part because of the reliance on collecting and tracking data matched by license plate numbers.[752] The CNIL felt that while a license

---

when the customer signs in. See OPCC, *PIPEDA, Case Summary #2003-162, Customer complaints about airline's use of cookies on its Web site* (16 April 2003) [OPCC, *PIPEDA, Case Summary #2003-162*]; Article 29 Working party has taken a similar approach as they believe that when a cookie contains a unique user ID, this ID is clearly *personal data*. See Article 29 Data Protection Working Party, *Opinion 1/2008*, *supra* note 207 at 9.

[749] European Parliament, *Seminar Data protection*, *supra* note 164.

[750] In Germany, the BDSG, § 3 states: "'Personal data' means information concerning the personal or material circumstances of an identified or identifiable individual (data subject)." According to the data protection treatise by Spiros Simitis et al., an identifiable individual exists in the sense of BDSG, § 3 when the information in question "relate to this person and only to him". See Spiros Simitis, Ulrich Dammann et al, Kommentar zum Bundesdatenschutzgesetz, § 3, 11. This issue is discussed in Reidenberg & Schwartz, *supra* note 203 at 37.

[751] Lundevall-Unger & Tranvik, *supra* note 641 at 3. See also Bercic & George, *supra* note 574 at 235-46.

[752] Délibération no. 96-069 du 10 septembre 1996 relative à la demande d'avis portant création à titre expérimental d'un traitement automatisé d'informations nominatives ayant pour finalité pincipale la lecture automatique des plaques d'immatriculation des véhicules en mouvement par la société des autoroutes Paris-Rhin-Rhône (SAPR).

plate number identifies the owner of the car, and not the actual person driving the car at any given time, the information is nonetheless linked to a small group of people (possible drivers of a particular car) and therefore it had to be covered by the definition of *personal data*.[753] Still, it is debatable whether the same reasoning should apply when evaluating a computer's IP address or new types of data and if so, what constitutes a "small" enough group to make certain data qualify as *personal*.

Some have taken the position that in the event that a computer is registered against a number of individuals through an IP address, then it is not personal data within the meaning of the definition because a single individual cannot be identified from such use.[754] Lee Bygrave states: "The chance of an IP address (and other clickstream data registered against that address) constituting personal data will be diminished if a multiplicity of persons are registered against that address".[755] At the same time, some have raised that while there may be difficulties in determining whether clickstream data correlates with a specific individual, the technologies have become so sophisticated that it is possible to extract personal information from clickstream data and identify specific individuals through this process,[756] therefore further illustrating how the notion of "identifying" data is changing with the Internet and new technologies.

(c) How Accurate Must the Link Be in Order to be Identifying?

Aside from the fact that certain data may be linked to more than one individual (this would be the case for example with clickstream data collected from cookies, if more than one person is using the same device), another issue is the degree of accuracy needed to be able to consider the data collected as being "identifying" and therefore covered under the definition of *personal information*?

Some claim that IP addresses are not precise enough in many instances to qualify as *personal information* for at least two reasons which are: multiple users and multiple

---

[753] See Reidenberg & Schwartz, *supra* note 203 at 32.

[754] See Bygrave, *supra* note 683 at 317.

[755] *Ibid*. at 318.

[756] See Daniel B. Garrie, "The Legal Status of Software" (2005) 23 J. Marshall L J. Computer & Info. L. 711 at 727. See also Wong & Garrie, *supra* note 187 at 580.

locations.[757] Many individuals may use the same computer, and thus share the same IP address and without an actual username/password login, no actual identification is facilitated. Also, an individual may be using the same device accessing the Internet (laptop) from different locations, for example, making queries across multiple IP addresses. There could be more than one machine using the same Internet facing IP address *at the same time*. For example, neighborhood members could be using a neighbor's wireless router without this person's knowledge.[758] These individuals would all technically appear to be under the same IP address. The Canadian Federal Court in *BMG Canada Inc*. v. *John Doe*[759] recognised the fact that given the unreliability of the evidence matching IP addresses and pseudonyms to account holders, it would be irresponsible to order disclosure of the identity of an account holder and expose that individual to a lawsuit.[760] Many authors have acknowledge this possibility, raising for instance that in order to link an IP address to a subscriber, an ISP must cross-reference several different databases.[761] The older the information is, the more difficult it is to retrieve, and the more unreliable are the results that will be produced.[762] Another issue is the fact that an IP address with the assistance of the ISP can identify the account holder, which may not be the individual who was using the computer. To complicate matters further, it is common for an account holder to set up a Local Area Network ("LAN") using a router to share the Internet connection between multiple computers.[763] In the event that a certain Internet user is surfing off a neighbour's

---

[757] Dolin, *supra* note 371 at 149: "The first reason, the case of multiple users of the same IP address, is exemplified by a public computer, say at a library. There, many people use the same computer, and thus share the same IP address. A new cookie may be generated each time the web browser is re-opened after a prior user closes it, allowing the search engine to detect a possible change in user. However, without an actual username/password login, no actual identification is facilitated. The second reason that an IP address alone may be insufficient to track a user's queries, multiple locations for the same user, is exemplified by someone using the same laptop from different locations. A user may scatter his queries across multiple IP addresses, some of which he may own, some not. Again, without cookie information, and, in particular, an actual login, the user would not have access to his complete search history via IP address data alone. IP addresses are still informative, however, as they can often be mapped to a small geographical region such as a county or zip code without requiring any non-public information."

[758] Comment in answer to blog. Whitten, *supra* note 730.

[759] *BMG Canada v. John Doe*, 2004 FC 488 (CanLII), aff'd 2005 FCA 193 (CanLII) [*BMG Canada*].

[760] *Ibid*. at para. 20.

[761] See Min-Chee Fong, *supra* note 382. This author raises that matching subscribers to IP addresses is an onerous, time-consuming task. In order to illustrate this, she refers to the fact that several employees of Rogers had to work for four days to locate nine IP addresses. See *BMG* Canada, *supra* note 759 at paras. 8-10.

[762] *Ibid*. at para. 34.

[763] *Ibid*. at para. 23.

unsecured wireless LAN, this may create additional uncertainties since an ISP can only identify the IP address of the router, not the actual computer that was responsible for a particular online activity.

An IP address is not necessarily sufficient information to determine the identity of an individual actually using a computer at a particular time. In the case of a LAN, only one of several computers could be responsible for certain online activities. In BMG Canada,[764] a public interest intervener submitted that if the court granted an order to disclose Internet users' identities on a low threshold test, then there could be a chilling effect on legitimate activities in cyberspace.[765] Disclosure of an Internet user's IP address, identity, and online activities could reveal highly personal information about his or her preferences and lifestyle that go beyond the scope of the copyright owners' allegations.[766] Although subscriber data pertaining to an IP address can be helpful to law enforcement agents, sometimes mistakes are made. In the fall of 2006, an ISP mismatched a customer and an IP address, resulting in a guns-drawn raid by a child-porn squad on a farmer in rural Virginia.[767] This illustrates how the quality of the identifying method will play an important role when linking certain data to an individual.

2.1.2.3. Obsolescence

Bennett Moses raises the fact that some existing legal rules may be justified, explicitly or implicitly, on the basis of a premise that no longer exists.[768] The definition of personal information focuses on information that relates to an "identifiable" individual. It is debatable whether the notion of identity is still relevant in the context of the Internet.

This section discusses how the notion of "identity" may be obsolete in certain situations and when and why pre-determined categories of "sensitivite" data are challenged in light of the Internet and new Internet technologies and may need to be revisited.

---

[764] *Ibid*.

[765] *Ibid*. See Factum of the Intervener Canadian Internet Policy and Public Interest Clinic at para. 31.

[766] CIPPIC Factum in *BMG* Canada, *supra* note 759 at para. 18.

[767] Ellen Nakashima, "The Legal Tangles Of Data Collection" *The Washington Post* (16 January 2007) at A09, online: The Washington Post <http://www.washingtonpost.com/wp-dyn/content/article/2007/01/15/AR2007011501301_pf.html>.

[768] Bennett Moses, *supra* note 552 at 16.

2.1.2.3.1. Notion of Identity Obsolete in Certain Situations

Profiles of individuals, although they may be anonymous and not covered under the definition of *personal information* in all cases, may still be used, for instance, to take decisions about an individual (or a profile).[769] There are a growing number of cases where information about an individual may not be directly personally identifiable, but where the individual has some interest based on the use of the information.[770]

Behavioural advertising may often involve the collection of IP addresses and the processing of unique identifiers (through the use of cookies). The use of such devices with a unique identifier allows the tracking of users of a specific computer even when dynamic IP addresses are used. In other words, such devices enable data subjects to be targeted or "singled out", even if their real names or contact information are not necessarily known.[771] Similar concerns can take place in the offline world, using location data or RFID technology to profile individuals.[772] New technologies make it

---

[769] See Clarke, "Profiling", *supra* note 622 at 403; See also Conseil de l'Europe, *L'autodétermination informationnelle*, *supra* note 20 at 28: "La possibilité de collecter des données relatives à des comportements présents ou passés, données personnelles ou anonymes, en quantités et qualités de plus en plus importantes et de les traiter de manière de plus en plus fine génère des risques de plus en plus grands de créer des profils et de prendre des décisions a priori par rapport à ces profils. Ainsi, la manière pour un internaute de naviguer sur le site d'une entreprise peut être caractérisée par quelques critères qui permettront après quelques visites de le ranger dans une catégorie ou une autre, d'afficher lors d'un contact une page de préférence à une autre, voire de lui refuser tel service."

[770] Certain have raised that RFID tracking without additional identifiers should not be governed by DPLs, while the Article 29 Working party disagrees on the basis that individuals may have some interest based on the use of the information. See Article 29 Data Protection Working Party, *Results of the Public Consultation*, *supra* note 380: "Another very controversial point, connected to the issue mentioned in the above bullet point, is whether the Working Party 29 paper is based on an overstretched definition of personal data, which goes beyond the definition contained in the data protection Directive and which is used to support the application of the Directive in cases where the Directive should not apply. In particular, a number of respondents think that the various hypotheses described in point 3.3 of the Working Party 29 paper do not entail a processing of personal data."

[771] Article 29 Data Protection Working Party, *Opinion 2/*2010, *supra* note 191 at 9. See online: <http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm>.

[772] See for example Profilium Inc.'s business model which was based on targeting individuals with relevant advertising messages based on their historical location data profile which would in no event reveal the identity of the individuals. See Profilium business model, 2001. This business model based on analyzing anonymous information is further discussed and illustrated in Gratton, *Internet and Wireless Privacy*, *supra* note 193 at 315-17. See also Article 29 Data Protection Working Party, *RFID technology*, *supra* note 196 at 7: "A further example could be where the use of RFID tags can lead to the processing of personal data, even when RFID technology does not involve the use of other explicit identifiers. Take the hypothesis where person Z walks into Shop C with a bag of RFIDtagged products from Shops A & B. Shop C scans his bag and the products in it (more likely a jumble of numbers) are revealed. Shop C keeps a record of the numbers. When person Z returns to the shop the next day, he is rescanned. Product Y, that was scanned yesterday, is revealed today – the number is for the watch he always wears. Shop C sets up a file using the number of product Y as a 'key'. This allows them to track when Person Z enters their shop, using the RFID number of his watch as a reference number for him. This allows shop C to set up a profile of

possible to identify the behaviour of a machine (device, computer) and the behavior of the individual behind the machine. It may therefore be possible to recreate the personality of an individual in order to apply certain decisions to the profile (so to the individual behind the anonymous profile) without needing the identity (name and address) of this individual. On this issue, the FTC in its recent 2012 Report states that:

> "commenters pointed to studies demonstrating consumers' objections to being tracked, regardless of whether the tracker explicitly learns a consumer name, and the potential for harm, such as discriminatory pricing based on online browsing history, even without the use of PII."[773]

We can recall the accusations made against Amazon of practising *adaptative pricing* to readjust and raise the price of certain items in accordance with the profile of the potential purchaser.[774] The United Kingdom's Office of Fair Trading ("OFT") has expressed a concern that consumers could suffer if their personal web usage is used to set the price they are offered for a particular service or product, especially if consumers are unaware of this practice.[775] The Comité consultatif takes the position that for these reasons, online profiles, even if potentially anonymous, should be covered by the definition of *personal information*.[776]

European privacy expert Pounder suggests that "identifying" an individual does not necessarily involve correlating certain data (such as an IP address) to someone's

---

Person Z (whose name they don't know) and to track what he has in his shopping bag on subsequent visits to Shop C. By doing this, Store C is processing personal data and data protection law will apply."

[773] Center for Democracy & Technology, Comment #00469 at 3, citing Edward C. Baig, "Internet Users Say, Don't Track Me" (14 December 2010), online: USA TODAY <http://www.usatoday.com/tech/news/2010-12-14-donottrackpoll14_ST_N.htm>; Scott Cleland, "Americans Want Online Privacy: Per New Zogby Poll" (8 June 2010), online: The Precursor Blog <http://www.precursorblog.com/content/americans-want-online-privacy-new-zogby-poll>; Consumers Union, Comment #00362 at 4 (discussing the potential for discriminatory pricing and citing Annie Lowery, "How Online Retailers Stay a Step Ahead of Comparison Shoppers" *The Washington Post* (12 December 2010), online: The Washington Post <http://www.washingtonpost.com/wp-dyn/content/article/2010/12/11/AR2010121100143.html>), discussed in FTC, *Recommendations* 2012, *supra* note 381 at 18.

[774] See section 2.1.2.1.2(a) entitled "Data not Identifying but Impacting on Individuals" which elaborates on this issue. See also Conseil de l'Europe, *L'autodétermination informationnelle*, *supra* note 20 at 29.

[775] See Office of Fair Trading, "OFT launches market studies into advertising and pricing practices" (15 October 2009), online: OFT <http://www.oft.gov.uk/news/press/2009/126-09>.

[776] Conseil de l'Europe, *L'autodétermination informationnelle*, *supra* note 20 at 29 : "Il est donc important qu'indépendamment du caractère personnel des données traitées, certaines règles soient posées à propos de l'établissement de profils (première étape), indépendamment de leur application ultérieure dans une seconde étape à des personnes physiques."

name.[777] He suggests that identifiablity can involve something where there is a focus on a particular characteristic. For example, this could mean that the user from a certain IP address is likely to be interested in advertisement pertaining to a certain area of interest because he/she has visited certain key websites.[778] It is interesting to note that in Sweden, the *Personal Data Act 1998* defines personal data as *"all kinds of information that directly or indirectly may be referable to a natural person who is alive".*[779] This definition does not refer to the fact that the data needs to "identify" an individual. For example, a website that would propose life insurance policies online, could conclude, rightfully or not, that a particular online visitor is homosexual and is afflicted with AIDS, based on the profile information collected by cookies.[780] The Swedish DPL would therefore apply if the notion of "gay person who probably has AIDS" relates, at the time of connection, to a physical person alive, even if such a person is not identifiable by name. In light of this, it is reasonable to wonder if the notion of "identity" is still relevant in the context of the web or if the definition should be re-evaluated in light of the above.[781]

2.1.2.3.2. Pre-determined Categories of Sensitivite Data Challenged

The Lindop Report from the 1970s discussed the aspect of data "sensitivity". While a number of users and trade unionists urged that special restrictions should be imposed on particular classes of information, especially information about an individual's race, religion or politics,[782] they had concluded that the notion of data "sensitivity" was a subjective issue and that it was not possible to either simply put together a complete list of what kind of data is "sensitive" or put together objective standards of "sensitivity":

> "We do not believe that any list of categories of information could ever be complete. Nor do we believe that there are any objective standards of "sensitivity": some people are sensitive about their age, and others are not; some are sensitive about their finances, and other boast about

[777] Comment from Chris Pounder in answer to blog. Whitten, *supra* note 730.

[778] Comment from Chris Pounder in answer to blog. *Ibid*.: "Identifiablity does not need a name - it can involve something where there is a focus on a particular characteristic (e.g. the user from the IP address 330.09.08.07 is likely to be interested in XYZ because he/she has visted web-sites P, Q and R)."

[779] Swedish *Personal Data Act* (1998:204), s. 3.

[780] Conseil de l'Europe, *L'autodétermination informationnelle*, *supra* note 20 at 33-34.

[781] See section 3.2.2.1 entitled "Identifiability Replaced by Negative Impact (Objective Harm)" which elaborates on this issue.

[782] Lindop, *supra* note 96 at 45-46, para. 5.34.

> them; and the same is true for sexual activities, medical history, and a host of other classes of personal information. Even names and addresses could in some circumstances be highly sensitive – as for example a list of names headed "suspected members of subversive political party", or "inmates not suitable for release because of danger to public" – or simply "trouble-makers" or "bad risks"."[783]

To illustrate this subjectivity, they referred to a survey carried out at the request of the Younger Committee Report on Privacy which indicated that no fewer than 35% of the respondents regarded it as an infringement of their privacy that their names and addresses could be found in the electoral register at the public library, and most of those thought that this should be prohibited by law.[784]

Certain DPLs, notably in France, have followed this trend (of having categories of sensitive data) and similar to article 8 of Directive 95/46/EC, acknowledge that certain types of personal data are more privacy sensitive and more likely to harm the data subject in cases of unauthorised processing. These include certain categories of data which are "sensitive" by nature, which are "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life".[785]

Many believe that pre-determined categories of sensitive data make no sense since sensitivity is dependant on the context. The PIAC shares this view and takes the position that the listing approach leaves room for companies to collect and use data not properly falling within an excluded class and that there are a number of potential harms regarding profiling and social sorting that will not be resolved by relying upon the "sensitivity" criterion.[786] These special categories of sensitive data may also contain

---

[783] *Ibid*. at 153-54, para. 18.25.

[784] *Ibid*.

[785] *Loi informatique et liberté*, *supra* note 131 at c. II, s. 2, art. 8 (II) (1): "Il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci."

[786] PIAC, *supra* note 448 at 9: "(…) there are decisions on the scope of 'sensitive' information (health information in particular) from the Ontario Information and Privacy Commissioner: see OIPC's recent HO-007 and its discussion of s. 4(1) of PHIPA of Ontario. Nevertheless, this listing approach leaves room for companies to collect and use data not properly falling within an excluded class. In addition, there are a number of potential harms regarding profiling and social sorting (detailed below) that will not be resolved by relying upon the 'sensitivity' criterion."

certain omissions, for instance financial and location data,[787] which data (location) may raise privacy concerns.[788]

Also, in the context of the Internet, with the increase in the volume in data exchanges[789] and the social changes through web 2.0 and OSNs under which online users voluntarily disclose and share their personal information,[790] this principle (of pre-determined categories of sensitive data) may be challenged. For example, images posted online (for example on OSNs) often reveal racial origin, and names may be typical to certain ethnicities and/or religions.[791] A photograph showing the ethnic origin of an individual would be regarded as sensitive data irrespective of the context or purpose in which the photograph was published.[792]

The current categorization of sensitive data in Directive 95/46/EC is not adequate as it is only based on the actual nature of the data. The publication of any personal data on the Internet may, under particular contexts, constitute the processing of sensitive data.[793] The 2002 Proposals for Amendment to Directive 95/46/EC[794] suggested redefining the scope of this provision in terms of acts of data processing that include any kind of "discriminatory practice". Many authors including Rebecca Wong ("Wong"), Yves Poullet (member of the Comité consultatif), Spiros Simitis, Schwartz and Reidenberg are proposing more contextual-based approaches in order to determine

---

[787] Robinson et al., *supra* note 151 at 28.

[788] Location data collected via mobile devices are useful for organizations that wish to provide location-based services. These services are already seen as a growth market but raise important privacy concerns. See Gratton, *Internet and Wireless Privacy*, *supra* note 193.

[789] See section 1.2.1.1 entitled "Increase in Storage Capabilities, Number of Users and Exchanges" which elaborates on this issue.

[790] See section 1.2.1.2 entitled "New Ways of Using the Internet: Web 2.0" which elaborates on this issue.

[791] Robinson et al., *supra* note 151 at 28.

[792] See Wong & Garrie, *supra* note 187 at 582.

[793] See Bygrave, *supra* note 683 at 69. Lee A. Bygrave is commenting on the context approach and sensitive data; See also generally Spiros Simitis, "Revisiting Sensitive Data" (1999) Review of the answers to the Questionnaire of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108). Spiros Simitis is discussing the context oriented approach to personal data as sensitive data.

[794] The *2002 Proposals for Amendment of the Data Protection Directive (95/46/EC),* made by Austria, Finland, Sweden and the United Kingdom - Explanatory Note, online: <http://www.dca.gov.uk/ccpd/dpdamend.htm> [*2002 Proposals for Amendment*].

the sensitivity of the data.[795] Interestingly, in Canada, PIPEDA has taken a more flexible position under which any data can be sensitive, "depending on the context".[796]

Guidelines may be useful to assist in evaluating new types of data given that the issue of qualifying data - such as clickstream data or profile data - as being sensitive raises additional issues. Reidenberg and Schwartz suggest that data profiles may frequently approach the categories of sensitive data that are subject to processing prohibitions under Directive 95/46/EC.[797] Assuming that clickstream data is person specific (i.e. relating to an identifiable individual), data revealing an individual's ethnic origin or religious opinion would qualify as sensitive data. Wong suggests that there is one flaw with this argument, as it is not always possible to draw an inference of an individual's sensitive data based on the fact that he or she has visited a particular website:

> "For example, if a user visited a Christian website, it is not necessarily true that the user was doing so for his or her religious beliefs rather than for research purposes. Certainly, repeated visits to a particular website or websites of a similar nature may indicate that the user holds particular religious beliefs. But it does not always follow that a website will necessarily correlate with a user's sensitive data as defined under Article 8(1). The DPD does not draw a distinction in ascertaining the user's intention when he or she visits a website".[798]

There have been various discussions in the U.S. about whether location information should be given the same privacy protections as medical data.[799] Some are suggesting that location data should be as sensitive as medical data, or that treating this data the same way makes no sense because location information is sensitive but it is sensitive

---

[795] Wong & Garrie, *supra* note 187 at 582; Conseil de l'Europe, *L'autodétermination informationnelle*, *supra* note 20 at 44-45; Rebecca Wong, "Data Protection Online: Alternative Approaches to Sensitive Data?" (2007) 2:1 J. Int'L Com. L. & Tech at 3; Simitis, *supra* note 793; Reidenberg & Schwartz, *supra* note 203 at 9: "Yet, the creation of special protection is also understood as requiring attention not only to whether information identifies particular aspects of a person's life that are sensitive, but how data will actually be used. The ability of information technology to combine and share data makes impossible any abstract, noncontextual evaluation of the impact of disclosing a given piece of personal information. The impact of bureaucratic use of personal information, whether merely personal or highly sensitive, depends on the means of processing, the kinds of databases linked together, and the ends to which information will be used."

[796] PIPEDA, *supra* note 63 at Schedule 1 (s. 5), principle 4.3.4.

[797] See Reidenberg & Schwartz, *supra* note 203 at 84. See also EC, *Directive 95/46/EC*, *supra* note 99 at art. 8.

[798] Wong & Garrie, *supra* note 187 at 581.

[799] Erica Newland, "Should all sensitive data be treated the same?" (26 February 2010), online: CDT <http://www.cdt.org/blogs/erica-newland/should-all-sensitive-data-be-treated-same#sf40182>.

"in different ways than medical data" and that therefore location information deserves special protections, but different protections than medical data does.[800]

I maintain that we may need to rethink the notion of pre-determined categories of so-called "sensitive" data in light of the fact that this information may already be widely "available" with new Internet technologies, new types of data, new data-mining techniques and the fact that individuals may disclose their personal information for anyone to see while using OSNs or other public blogs.[801]

[800] Marshall Kirkpatrick, "Location Data Sensitive Like Medical Information, Says Congressional Witness" *The New York Times* (25 February 2010), online: The New York Times <http://www.nytimes.com/external/readwriteweb/2010/02/25/25readwriteweb-location-data-sensitive-like-medical-inform-75294.htm> [Kirkpatrick, "Location Data"]: "But treating location data like medical data sounds like a recipe for shrouding it in complete privacy by default. Not allowing information about our activities in public (...) to be public (...) would be a real blow to the location service ecosystem."

[801] In section 3.1.2.2 entitled "Risk of Subjective Harm: Revisiting the Sensitivity Criteria", I elaborate on the criterias which should be relevant when determining if certain information is "sensitive", meaning if it creates a risk of subjective harm upon being disclosed. More specifically, section 3.1.2.2.3 elaborates on the fact that whether the information is in fact available is a criteria which should be taken into account in assessing this risk of subjective harm.

2.2. Reconstruction Taking into Account Underlying *Risk of Harm*

The notion of *personal information* is central to DPLs, as it defines the object of protection.[802] Although the all encompassing nature of the definition initially allowed the difficulties emerging from the contextual nature of privacy to be sidestepped, new challenges have arisen with the Information Age and recent technology developments.[803] I maintain that if we want to address the over-reaching outcome of the notion of *personal information*,[804] the under-reaching outcome,[805] the uncertainties as to which information qualifies as *personal information*[806] and ensure that certain situations which are obsolete are no longer covered by DPLs,[807] that we should adopt certain new sub-criteria (which may or may not include the notion of "identifiable" individual) in order to provide guidance on which kind of data qualifies as *personal*.

Van den Hoven, as are many others, is of the view that the current legal definition of *personal information* (or *personal data* in Europe) provides no guidance on which data should be governed by DPLs.[808] He suggests that it is essential to the ethics, law, and technology of data protection to identify the parcels of information that actually warrant protection.[809] I maintain that an interpretation of the notion of *personal information*, which will take into account the purpose behind DPLs, will simplify this process.

Rather than proposing a redrafting of the current definition or worse, as suggested by Ohm, to completely abandon it,[810] a possible alternative would be to discard the literal method of interpreting *personal information* which has led to so many unwanted

---

[802] See section 1.1.3 entitled "Definition of Personal Information: Origin and Background" which elaborates on this issue.

[803] See section 1.2 entitled "Technological Background Affecting Personal Information" which elaborates on this issue.

[804] See section 2.1.2.1.1 entitled "Potentially Over-Inclusive Definition" which elaborates on this issue.

[805] See section 2.1.2.1.2 entitled "Potentially Under-Inclusive Definition " which elaborates on this issue.

[806] See section 2.1.2.2 which elaborates on this issue.

[807] See section 2.1.2.3 entitled "Obsolescence" which elaborates on this issue.

[808] Van den Hoven, "Information Technology", *supra* note 642 at 309.

[809] *Ibid*.

[810] Ohm argues that the concept of PII or personal identifiable information (the U.S. counterpart of *personal information*) is unworkable and unfixable. See Ohm, *supra* note 562 at 1742.

outcomes and contradictory results.[811] I maintain that a method of interpretation, which is consistent with the original goals of DPLs, should be favoured.

2.2.1. Using a Purposive Approach to Interpreting Personal Information

Using a literal approach to interpret *personal information* has created unwanted outcomes in many cases, including unnecessary compliance costs. I maintain that data collected, used or disclosed that provides no *risk of harm* to individuals should not be protected under DPLs (and therefore, not considered *personal information*). A more relative approach is the proper way to ensure that the interpretation of *personal information* stays true to the ultimate goal or purpose behind the adoption of DPLs.

2.2.1.1. A New Interpretation of Personal Information as a Solution

The definition of personal information as: "data pertaining to an identifiable individual" (or similar definitions)[812] which can be found in most DPLs across the globe, can be viewed as a legal category or construct; one, which began to emerge several decades ago.

The 1970s saw an increase in the capacity of computers and electronic databases. As public and private sector use of computers began to increase so did the concern that individuals would ultimately lose control over their personal information, as further detailed in section 1.1.2. It was in this context that the current definition of *personal information* was established.

Reports from the 1970s suggest that the definition was meant to remain relevant even in the face of new technologies.[813] Nonetheless, in light of recent unprecedented and exponential technological advancements, which have increased the overall volume of

---

[811] See section 2.1.2.2 which elaborates on this issue.

[812] See section 1.1.3 entitled "Definition of Personal Information: Origin and Background" which elaborates on the origin of the definition of "personal information" or "personal data" found in Canadian and French DPLs.

[813] For instance, Lindop wanted their DPL to survive technology, and suggested that the legislation should not need to be amended by reason of technical changes alone. See Lindop, *supra* note 96 at 13, para. 3.04: "Because the lifetime of the legislation on which we are asked to advise will be substantial, we have informed ourselves both about the current state of the art and about foreseeable developments in it, to ensure that the legislation will not need to be amended by reason of technical changes alone."

available information that can be linked to an identifiable individual,[814] the definition evidently needs to be revisited. To echo van den Hoven's arguments, given the prominence of new technology, including RFID, profiling and data mining technologies, the dominant referential interpretation of *personal information* must be reconsidered.[815]

Adopting a new interpretation of *personal information* is important for two reasons. To begin with, DPLs may provide for the necessary flexibility of the definition (or at least they were initially supposed to). Second, providing for an interpretation instead of proposing a new wording to the definition may avoid having to completely reopen the "control" conception of privacy, which is the basis of DPLs which have been adopted all over the world.

As Ohm cautions, we should avoid getting caught in semantics, in other words trying to determine exactly what "identifiable" individual actually means.[816] He argues that this would prove to be an exercise in futility, especially in light of modern technologies where almost any data could technically qualify *as personal information*.[817] At the same time, I agree that it is important to do this exercise (of determining how "identifiable" should be interpreted) when evaluating the "sensitivity" of certain data, in the context of assessing the risk of subjective harm triggered by the disclosure of this data (in order to determine if this data should qualify as *personal information*).[818]

In contrast with this flawed strategy (trying to determine exactly what "identifiable" individual actually means), consider a decision tree that would take into account the context of the information, for instance whether it is being collected, used or disclosed.[819] This decision tree would provide for sub-criteria which would be very useful in determining whether or not certain data should be governed by DPLs, the

---

[814] See section 1.2.1 entitled "Increase in Volume of Information" and more specifically, section 1.2.1.3 entitled "Easier Identification of Individuals" and section 1.2.3 entitled "New Identifying Methods" which elaborate on this issue.

[815] Van den Hoven, "Information Technology", *supra* note 642 at 310.

[816] Ohm, *supra* note 562 at 1761: "Regulators need to shift away from thinking about regulation, privacy, and risk only from the point of view of the data, asking whether a particular field of data viewed in a vacuum is identifiable. Instead, regulators must ask a broader set of questions that help reveal the risk of reidentification and threat of harm."

[817] See section 2.1.2.1.1 entitled "Potentially Over-Inclusive Definition" which elaborates on this issue.

[818] See section 3.1.2.2 entitled "Risk of Subjective Harm: Revisiting the Sensitivity Criteria" which elaborates on this issue.

[819] See the decision tree which is detailed at note 247.

appropriate extent of protection and, above all, whether it actually qualifies as *personal information*.

2.2.1.1.1. Sufficient Flexibility for Interpretation

Does the definition of *personal information* leave any room for interpretation? In other words, how flexible is it? Pierre-André Côté suggests that once we determine that a new technology was meant to be governed by a given law, then we need to determine if the text was drafted in terms general enough to allow new cases to be submitted; including those that could not have been foreseen at the time that the text of law was adopted.[820] If a literal interpretation is favoured to interpret *personal information*, the flexibility of the definition becomes quite limited. An interpretation, which takes into account the purposes behind DPLs, on the other hand, leaves much more room for interpretation.

A general principle of lawmaking is that the law should be sustainable. It is obvious that nowadays, technology develops much more quickly than the law does.[821] Laws should be sustainable enough to cope with technological development over a sufficiently long period of time. If a law is too technology-specific, it is not likely to cover future technological developments, and it will therefore have to be amended often.[822] Bert-Jaap Koops ("Koops") raises another interesting point:

> "(…) On the other hand, eminently sustainable laws may also contain the risk that over the years, the interpretation of the law will diverge for different technologies and hence will lead to unintended technology specificity. (…) Another and more important risk with sustainability is that, in order to create sustainability, laws are formulated that are so technology-neutral that they become meaningless."[823]

---

[820] Pierre-André Côté, *Interprétation des lois*, 3rd ed. (Montréal : Éditions Thémis, 1999) at 333-34. "Dans chaque cas, il s'agit de savoir d'une part, si la finalité de la disposition en justifie l'application à la nouvelle invention et, d'autre part, si le texte est rédigé d'une manière suffisamment générale pour que l'interprète puisse y soumettre des cas d'espèces inconnus à l'époque de l'adoption."

[821] Bert-Jaap Koops, "Should ICT Regulation be Technology-Neutral?" in Bert-Jaap Koops et al., eds., *Starting points for ICT regulation: Deconstructing prevalent policy one-liners*, coll. IT & Law Series, vol. 9 (The Hague: TMC Asser, 2006) 77.

[822] *Ibid*. at 10.

[823] *Ibid*. at 10-11.

With a literal interpretation of *personal information*, the manner in which DPLs are applied towards different technologies may vary.[824] DPLs may also become to a certain extent meaningless or marginalized.[825] Thus, the way in which the notion of *personal information* is understood may fluctuate based on the interpretation. Ultimately, in order for DPLs to be applied more uniformly across the board and avoid unintended technological specificity, I maintain that a new interpretation is needed.

Since DPLs were designed to remain relevant in the face of technological change, I believe that proposing more precise regulations to address the new technological reality may not be the best solution. The definition of *personal information* should remain broad enough to allow for flexibility when applying the FIPs to different technologies. Following this approach, the effects of DPLs will remain technology neutral as much as possible.[826]

According to the Article 29 Working Party, unduly restrictions must not be imposed on the interpretation of *personal data*.[827] More recently enacted DPLs, such as PIPEDA or the Alberta and British Columbia DPLs, contain "reasonableness tests" which dictate the limits of their applicability.[828] These tests illustrate that having some type of flexibility has become a necessity; especially true in the context of the Information Age.

According to the OPCC, the current broad definition of *personal information* in PIPEDA has enabled the OPCC to develop a fine-tuned and balanced approach in its decision-making, which implies that it provides for the proper flexibility:

---

[824] See section 2.1.2.2.2 entitled "Identifying a Device or an Object" which elaborates on this issue and more specifically, section 2.1.2.2.1(b) entitled "At what costs and using what kind of efforts?" on the various contradicting positions rendered (when using a literal interpretation) on whether an IP address qualifies as *personal information*.

[825] See sections 2.1.2.1.1(d) entitled "Consequences of Over–Inclusiveness" and section 2.1.2.1.2(c) entitled "Consequences of Under-Inclusiveness" which elaborate on this issue.

[826] Althought I realize that it might be in many cases impossible to acheive perfect "technology neutrality". See Vincent Gautrais, *Neutralité technologique: Rédaction et interprétation des lois face aux technologies* (Montréal : Éditions Thémis, 2012) [Gautrais, *Neutralité technologique*].

[827] Article 29 Data Protection Working Party, *Opinion 4/2007*, *supra* note 100 at 5-6: "It is a better option not to unduly restrict the interpretation of the definition of personal data but rather to note that there is considerable flexibility in the application of the rules to the data."

[828] For example, there would be in certain situations no need to disclose the collection of certain data and obtain consent for their use or disclosure. See section 2.2.1.3.2(a)(i) entitled "Reasonableness or Legitimacy Tests" which elaborates on this issue.

> "The few cases that have considered the scope of "personal information" have also provided opportunities to consider what information is protected by PIPEDA and, more specifically, when it is appropriate to claim that information is *not about* an identifiable individual and therefore not protected by PIPEDA. A review of these findings shows that the OPCC has developed a balanced approach that enables decision-making to be tailored to the context." [829]

In Europe, the Article 29 Working Party has also suggested that the National Data Protection Supervisory Authorities "should endorse a definition that is wide enough so that it can anticipate evolutions and catch all "shadow zones" within its scope, while making legitimate use of the flexibility contained in the Directive."[830] More specifically, this group argues that the text of Directive 95/46/EC invites the development of a policy that combines both a wide interpretation of *personal data* and an appropriate balance in the application of Directive 95/46/EC's rules.[831]

The Article 29 Working Group issued an opinion on the concept of *personal data* in 2007 in which they suggest that the ultimate purpose of the rules contained in the European Directives – to protect the fundamental rights and freedoms of natural persons and in particular their right to privacy, with regard to the processing of personal data – should be taken into account in the interpretation and application of the Directive 95/46/EC's rules.[832] More specifically, it suggests that such an interpretation should restrict the applicability of Directive 95/46/EC to a number of situations where the rights of individuals are not at risk. The group also cautions against any interpretation that would deprive individuals of protection:

> "As a general consideration it has been noted that the European lawmaker intended to adopt a broad notion of personal data, but this

---

[829] OPCC, *supra* note 135. The OPCC states that: "The OPC's total context approach also means that the OPC has retained jurisdiction to assess the introduction of new technologies that could be highly intrusive if not used in a controlled way – for example, biometrics, global positioning systems and radio frequency identification. In sum, the OPC has achieved a delicate balancing of powers and rights, consistent with the balance attained in PIPEDA itself."

[830] Article 29 Data Protection Working Party, *Opinion 4/2007*, *supra* note 100 at 5-6.

[831] *Ibid*.

[832] *Ibid*. at 4: "Articles 1 of Directive 95/46/EC and of Directive 2002/58/EC states the ultimate purpose of the rules contained therein is to protect the fundamental rights and freedoms of natural persons and in particular their right to privacy, with regard to the processing of personal data. This is a very important element to take into account in the interpretation and application of the rules of both instruments. It may play a substantive role in determining how to apply the provisions of the Directive to a number of situations where the rights of individuals are not at risk, and it may caution against any interpretation of the same rules that would leave individuals deprived of protection of their rights."

> notion is not unlimited. (…) These rules were therefore designed to apply to situations where the rights of individuals could be at risk and hence in need of protection. The scope of the data protection rules should not be overstretched, but unduly restricting the concept of personal data should also be avoided."[833]

In the 1970s, as the FIPs were being established and DPLs began to emerge in certain jurisdictions, it was already very clear that a certain flexibility was required and necessary in the application of FIPs. For instance, the Lindop Report explained that the FIPs were drafted in broad terms, specifically in order to provide some type of flexibility.[834] Too much specificity in defining the objectives of the FIPs could lead to a loss of flexibility and DPLs incorporating these FIPs were therefore to be as flexible as possible.[835]

As early as the 1970s, businesses and various organizations were already raising warning flags over potential restrictions to their data processing activities, if the objectives of the FIPs were to be given a strict, literal interpretation.[836] In answer to these concerns, certain documents from the 1970s generated from European jurisdictions illustrate that the FIPs and their underlying obligations on users were to be imposed only "as far as reasonably practicable".[837] Clearly, the original intention of DPLs was not to ensure that every conceivable data handling activity be covered:

> "We believe that regulation should be as light and as flexible as possible, and exercised with any stringency only where there is a special need to overcome substantial risks for the citizen's privacy. Our recommendations for the scope of the statute, for the powers of the DPA and for the form of the statutory guidelines are therefore deliberately cast widely. This is not because it is our intention that every conceivable data handling activity should be capable of accommodating the changes in

---

[833] *Ibid*. at 25.

[834] Lindop, *supra* note 96 at 199, para. 21.04. See also *ibid*. at 148, para. III.04.

[835] This is now the case with certain DPLs such as PIPEDA which is more flexible, as it is based on a standard. See section 2.2.1.3.2(d) entitled "Certain Jurisdictions Have Already Adopted a Flexible Interpretation" which elaborates on this flexibility under PIPEDA.

[836] Lindop, *supra* note 96 at 200, para. 21.05: "The great majority of users who commented on the objectives set out in paragraph 34 of the White Paper were concerned to explain to us the problems which would be imposed on their data processing activities if those objectives were to be strictly applied, across the board, to everyone and with literal adherence to their wording."

[837] *Ibid*. at 199, para. 21.04.

> the automatic handling of personal information which will occur during its foreseeable lifetime."[838]

More specifically, great importance was attached to flexibility in the application of the principles of FIPs as evidenced by a certain document dating back from this period which mentions that: "the appropriate level of compliance with each applicable principle will vary for different information systems which handle personal data in different ways and for different purposes."[839]

The main purpose of adopting a very broad yet flexible legislation (DPLs) was therefore initially meant to ensure that the law would keep up with technological developments.[840] The interpretation of the FIPs was crucial and would largely determine the effect of the objectives of the FIPs as implemented.[841]

The definition of *personal information* was drafted to be intentionally broad.[842] Instead of redefining *personal information*, I maintain that we should be seeking an interpretation that is consistent with the original goals of DPLs.

2.2.1.1.2. Underlying Benefits of Interpretation as a Solution

Proposing an interpretation has various benefits. It is always less disturbing to provide a solution which will be incorporated within the current legal framework (DPLs), such as a proposed interpretation, than proposing something completely new.[843] Many jurisdictions are aligning their practices with one another in an attempt to promote some type of global consistency in the data protection arena.[844] Many industry players

---

[838] *Ibid*. at 147, para. III.04.

[839] *Ibid*. at 202, para. 21.15.

[840] *Ibid*. at 13, para. 3.04: "Because the lifetime of the legislation on which we are asked to advise will be substantial, we have informed ourselves both about the current state of the art and about foreseeable developments in it, to ensure that the legislation will not need to be amended by reason of technical changes alone."; See also *ibid*. at 18, para. 3.21: "We took these considerations into account when deciding upon our recommendations for data protection legislation. An approach which would have been appropriate in 1970 and 1975 would not be suitable for the technology of 1980 and 1985. Technological developments are happening with increasing speed and economy; this requires flexibility in the mechanics of control to allow new potential threats to be contained."

[841] *Ibid*. at 45-46, para. 5.34.

[842] See section 2.1.2.1.1(a) entitled "Definition Meant to be Broad" which elaborates on this issue.

[843] Gautrais & Trudel, *supra* note 1 at 2: "Le doyen Carbonnier considérait qu'il 'fallait légiférer en tremblant'".

[844] See section 1.1.2.2 which elaborates on the fact that Canadia and European countries have adopted similar DPLs.

are also vouching for global privacy standards.[845] The FTC, in its recent 2012 Report, states that :

> "Many commenters cited the value to both consumers and businesses of promoting more consistent and interoperable approaches to protecting consumer privacy internationally. These commenters stated that consistency between different privacy regimes reduces companies' costs, promotes international competitiveness, and increases compliance with privacy standards."[846]

As already mentioned, the OPCC recently concluded that *work product* should not be exempt from the definition of personal information in PIPEDA, one of the reasons being that the current definition of personal information is based on known Canadian and "International precedent and consensus":

> "PIPEDA defines the information it protects to be information "*about* an identifiable individual." This definition was selected because it had a known and stable history in Canadian law and jurisprudence. It also paralleled definitions in other jurisdictions, particularly those in Europe, that were also addressing private sector privacy protection in a rapidly developing technological environment. A key goal in drafting the definition of personal information in PIPEDA was to ensure that Canadian law was harmonized with European law. This would prevent impediments to trade based on differing data protection schemes."[847]

More specifically, the OPCC was concerned that the introduction of a *work product* exemption would mean that Canada would be taking a position different from that taken in other jurisdictions, particularly in Europe.[848] While this concern (promoting

---

[845] See Jose Vilches, "Google proposes global privacy standard" (14 September 2007), online: Techspot <http://www.techspot.com/news/27032-google-proposes-global-privacy-standard.html>; See also Microsoft Corporation, *supra* note 358 at 8-9: "As the Commission considers if, and how, the Data Protection Directive should be reformed, we encourage examination of regulatory developments in other jurisdictions and movement towards a more harmonised global regime. As the patchwork of worldwide data protection laws has become increasingly difficult to navigate, Microsoft has repeatedly called for a comprehensive, workable global privacy framework that is consistent, flexible, transparent and principles-based. We welcome, for example, efforts made by the Spanish Data Protection Agency to develop a global standard. We would encourage the Commission to align EU rules and practices to the extent possible with international standards, provided that they ensure strong protections for users and are consistent with the principles of the Data Protection Directive."

[846] See Comment of AT&T Inc., cmt. #00420, at 12-13; Comment of IBM, cmt. #00433 at 2; see also Comment of General Electric, cmt. #00392, at 3 (encouraging international harmonization), discussed in FTC, *Recommendations* 2012, *supra* note 381 at 9.

[847] OPCC, *supra* note 135.

[848] While the OPCC admitted that it had not investigated whether a change in PIPEDA's definition of personal information would affect the perception that PIPEDA was sufficiently harmonized with European law, it noted that during a recent review of the Directive 95/46/EC, the EC was asked to add a "work

consistency across jurisdictions) makes even more sense in today's world, with the web and related technologies, we can note that this concern has been around for a while. Even back in the 1970s, certain legislators or committees in charge of analyzing data protection issues such as the Lindop Committee in the U.K., were very cautious about ensuring the cross-jurisdictional consistency of how *personal information* was defined:

> "Accordingly, we have come to the conclusion that the only feasible definition of "personal information" for this purpose is any information which relates to any data subject who is, or can be, identified – including the information whereby he can be identified, as for example his name, address, date of birth, or telephone number (…). Here again, we are reinforced in our conclusion by the fact that the foreign statutes all adopt similar definitions. The US privacy Act, for example, uses "any information about an individual that contains his name…or identifying particulars", the Swedish Acts speaks of "information concerning an individual" and the Norwegian Bill defines it as "information and assessments, which are directly or indirectly traceable to identifiable individuals, associations or foundations". France, Austria, Denmark and West Germany all use similar terms in their proposed or enacted legislation."[849]

There is no magic cure to be found (when addressing the current outcome of DPLs) as many potential solutions entail great challenges as well. Proposing a jurisdiction-specific solution will not be sufficient. Nor should we completely overhaul the "control" definition of privacy. There may be a lot of resistance, since many countries are attempting to have a similar approach to facilitate inter-jurisdictional exchanges.[850] It

---

product" exemption to the Directive 95/46/EC's definition of personal information and that in general, the EC advised against modifying it. See IMS Health, *supra* note 135. See EC, Commission, *Report from the Commission: First Report on the Implementation of the Data Protection Directive (95/46/EC)*, COM (2003) 265 (Brussels: EC, 2003), discussed in OPCC, *supra* note 135.

[849] Lindop, *supra* note 96 at 154, para. 18.27.

[850] The threat of loss of trade as a result of the Directive 95/46/EC and its adequate protection requirements was a strong motivating factor for the Canadian Government's decision to enact PIPEDA. See Coughlan et al., *supra* note 112 at 12; See also Gilbert Parent, *supra* note 112; The Quebec parliament debates which led to the adoption of the Quebec DPL in 1993 confirm that the main concern at such point was to ensure that Quebec would have a DPL which would be in line with the OECD Guidelines. Various references are made on the fact that Quebec is "behind" on the data protection front since it has not yet adopted a DPL in line with the OECD Guidelines although Canada is a member of the OECD and that it needs to adopt a DPL in order to have a law in line with data protection efforts made at the international level, especially with efforts made in Europe. See *Les travaux parlementaires*, 34th législature, 2nd session, Commission permanente de la culture, cahier no 11 (February 23,1993), at p. 2, 5, 12, 27, 57, 58, 66; *Les travaux parlementaires*, 34th législature, 2nd session, Commission permanente de la culture, cahier no 12 (February 24, 1993), at p. 38, 41, 49; *Les travaux parlementaires*, 34th législature, 2nd session, Commission permanente de la culture, cahier no 13 (March 1, 1993), at p. 2, 6 and 8; *Les travaux parlementaires*, 34th législature, 2nd session, Commission permanente de la culture,

would definitely go against the reality of the Internet and related technologies, and the current trend of globalization.

I already discuss in section 2.1.1 the issues that I have with the concept of privacy as "control". I also elaborate on the fact that while I am not completely against this concept, I do not believe that having individuals in "absolute" control of their personal information is realistic in the Information Age or that it is the right way to address the concerns that we have with organizations collecting, using and disclosing personal information. I discuss in section 2.1 how many believe that conceptualizing privacy as "control over personal information" can be too vague, too broad, or too narrow, that the "control" conception of privacy may be outdated or that the control-based paradigm may be fundamentally misguided. At the same time, many others believe that this conception is still relevant nowadays. The latter group argues that in the Information Age, with so much data available, "control over personal information" is still relevant and that privacy is about "control".[851] Bruce Schneier articulates the view that contrary to the older generation for which privacy was about secrecy, nowadays privacy is quite simply about "control":

> "Privacy is about control. When your health records are sold to a pharmaceutical company without your permission; when a social-networking site changes your privacy settings to make what used to be visible only to your friends visible to everyone; when the NSA eavesdrops on everyone's e-mail conversations -- your loss of control over that information is the issue. We may not mind sharing our

cahier no 14 (March 2, 1993), at p. 6, 25, 36, 38, 40, 43 and 65; *Les travaux parlementaires*, 34th législature, 2nd session, Commission permanente de la culture, cahier no 16 (March 4, 1993), at 35 and 55; *Les travaux parlementaires*, 34th législature, 2nd session, Assemblée, cahier no 73 (March 16, 1993), at 2, 3, 9, 23, 27; *Les travaux parlementaires*, 34th législature, 2nd session, Assemblée, Motion, cahier no 73 (March 16, 1993), at 1-2; *Les travaux parlementaires*, 34th législature, 2nd session, Commission permanente de la culture, cahier no 23 (May 13, 1993), at 9, 11, 14; *Les travaux parlementaires*, 34th législature, 2nd session, Assemblée, cahier no 112 (June 14, 1993), at 2; and *Les travaux parlementaires*, 34th législature, 2nd session, Commission permanente de la culture, cahier no 32 (June 8, 1993), at 4 and 12.

[851] Fleischer, "The data deluge", *supra* note 143: "There's no doubt that the Information Age is doing a lot of great stuff with this data deluge. It's also true that this data deluge is posing unprecedented challenges to privacy. (…) I don't think there's a better solution than trying to create maximum transparency and putting control over data back into people's hands, as best as possible. Trying to stop the data deluge is either Sisyphean or chimerical. But trying to decide on behalf of people also undermines the fundamental dignity and choice that each individual should be able to exercize over his/her own data. Of course, not all people can or will exercize responsible control over their own data. But putting transparency and control into users' hands is much like democracy. It fundamentally empowers the individual to make choices and trade-offs about data: making choices between data benefits and privacy."

> personal lives and thoughts, but we want to control how, where and with whom. A privacy failure is a control failure."[852]

Various online services mention having developed the technology to allow individuals to "control" their personal information. These are often referred to as "privacy settings" and are found on websites such as Facebook. In the words of Facebook founder Mark Zuckerberg : "we have focused on giving you the tools you need to share and *control your information*. (…) We're adding something that many of you have asked for — the *ability to control* who sees each individual piece of content you create or upload."[853]

Therefore, proposing a new interpretation of the notion of *personal information*, while maintaining the "control" conception of privacy, may be the ideal way to move forward.[854] This approach will be especially effective if it addresses the current concerns with the "control" definition of privacy,[855] as well as the concerns relating to the definition of *personal information*.[856] This approach would also be in line with the initial intent of lawmakers at the time of the adoption of DPLs (incorporating the FIPs).[857]

In Canada, the OPCC has often chosen not to implement a literal interpretation of the notion of *personal information* and instead favours an approach they refer to as the "total context approach".[858] Ostensibly, the OPCC has implemented what it sees as a more practical and logical approach, at least when evaluating information produced in the context of an individual's employment.[859] In Europe, the Article 29 Working Group suggests that it is important to keep the ultimate purpose of Directives 95/46/EC and

---

[852] Schneier, "Privacy and Control", *supra* note 83.

[853] Zuckerberg, *supra* note 165.

[854] Although I believe that my analysis may still be useful for a system which would reject this "control" conception.

[855] See generally, section 2.1 entitled "Deconstructing the Definition of Personal Information" which elaborates on this issue.

[856] See section 2.1.2 "Deconstructing the Efficiency of the Definition of Personal Information" which elaborates on this issue.

[857] For example, Lindop had raised the fact that the interpretation of the FIPs was crucial and would largely determine the effect of the objective as implemented. See Lindop, *supra* note 96 at 45-46, para. 5.34.

[858] See section 2.2.1.3.2(d) entitled "Certain Jurisdictions Have Already Adopted a Flexible Interpretation " which elaborates on this "total context" approach. Please note that the interpretation which I propose is different than a contextual approach and section 2.2.1.2 elaborates on this issue (the difference between a contextual approach and the approach proposed in this thesis).

[859] OPCC, *supra* note 135.

Directive 2002/58/EC[860] in mind when interpreting and applying the rules of both instruments.[861] In light of this, while the proposed approach is different than a contextual approach, I maintain that an interpretation of *personal information*, which takes into account the ultimate purpose of DPLs, should be the preferred approach. This purposive approach to interpretation, which I propose, is detailed below.

2.2.1.2. Proposed Interpretation: Purposive Approach (vs. Contextual Approach)

In his book entitled "Purposive Interpretation in Law", leading judge and legal theorist Aharon Barak ("Barak") argues that while legal philosophers and jurists apply different theories of interpretation to statutes and rules, a purposive interpretation would probably be more beneficial.[862] He suggests that this method would allow jurists and scholars to approach all legal texts in a similar manner, while remaining sensitive to important differences.

Barak explains the purposive interpretation as follows: All legal interpretation must start by establishing a range of semantic meanings for a given text, from which the legal meaning is then drawn. In a purposive interpretation, the text's "purpose" is the criterion for establishing which of the semantic meanings yields the legal meaning. Establishing the ultimate purpose (and therefore, the relevant legal meaning) would depend on the relationship between the subjective and objective purposes; that is, between the original intent of the text's author and the intent of a reasonable author and of the legal system at the time of interpretation.[863] Barak contrasts his approach

---

[860] EC, *European Parliament and Council Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*, [2002] O.J., L 201/37 [EC, *Directive 2002/58/EC*].

[861] Article 29 Data Protection Working Party, *Opinion 4/2007*, *supra* note 100 at 4: "Articles 1 of Directive 95/46/EC and of Directive 2002/58/EC states the ultimate purpose of the rules contained therein is to protect the fundamental rights and freedoms of natural persons and in particular their right to privacy, with regard to the processing of personal data. This is a very important element to take into account in the interpretation and application of the rules of both instruments. It may play a substantive role in determining how to apply the provisions of the Directive to a number of situations where the rights of individuals are not at risk, and it may caution against any interpretation of the same rules that would leave individuals deprived of protection of their rights."

[862] Aharon Barak, *Purposive Interpretation in Law* (Princeton: Princeton University Press, 2005).

[863] While this may be easy to establish when the subjective and objective purposes do coincide, he suggests that the relative weight given to each purpose should depend on the nature of the text when the purposes don't coincide. For example, subjective purpose would given substantial weight in interpreting a document such as a will and objective purpose would given substantial weight in interpreting a document of a constitutional nature.

with that of textualists and neotextualists such as Antonin Scalia, pragmatists such as Posner, and legal philosophers such as Ronald Dworkin.

Gautrais and Trudel articulate the view that legal interpretation should place an emphasis on the global context of any given law, its purpose as well as the original intent of the lawmaker.[864] They refer to Gregory Mandel who suggests that we should verify what the rationale behind a legal construct actually is, when interpreting such construct:

> "a decision-maker must consider the rationale for the existing legal categories in the first instances, and then determine whether that rationale applies to the new technology. Legal categories (such as common carriers) are only that – legal constructs. Such constructs may need to be revised in the face of technological change."[865]

I elaborate in section 2.2.2.2 on the fact that the ultimate purpose behind DPLs was to protect individuals against a *risk of harm* that may be triggered by organizations collecting, using and disclosing their personal information. But this *risk of harm* triggered by the handling of personal information is a function of several variables, such as: situation-specific circumstances, the intentions of the parties involved, the kind of information being sought after and the way it is processed. Other variables include the historical context, the particular type of technology at stake, the political environment, the nature of the information within a given context, as well as the vulnerability of the individual. All of these variables (and many more) may be relevant in assessing this so-called *risk of harm*.[866] For a full contextual approach, all of these elements would need to be taken into consideration in an integrated manner.

---

[864] Elmer A. Driedger, *Construction of Statutes*, 2nd ed. (Toronto : Butterworths, 1983) at 87, quoted in *Stubart Investments Ltd. c. La Reine*, [1984] 1 R.C.S. 536 at 578 and discussed in Gautrais & Trudel, *supra* note 1 at 48: "Mais plus que la quête d'une seule méthode d'interprétation, c'est bien davantage selon une vision globale, 'moderne' selon le propos de Driedger, que les lois s'interprètent. À ce propos, la Cour suprême fait sienne la citation de l'auteur dans plusieurs de ses décisions selon laquelle : 'Aujourd'hui il n'y a qu'un seul principe ou solution : il faut lire les termes d'une loi dans leur contexte global en suivant le sens ordinaire et grammatical qui s'harmonise avec l'esprit de la loi, l'objet de la loi et l'intention du législateur'".

[865] Gregory Mandel, "History Lessons for a General Theory of Law and Technology" (2007) 8 Minn. J. L. Sci. & Tech. 551 at 553, 556 and following, discussed in Gautrais & Trudel, *supra* note 1 at 49.

[866] Other variables (which would be relevant for a contextual approach) may include: the long term as well as the short-term impact on the individual affected, on what terms the information is shared, the terms of further dissemination, the purpose of disclosure, the expectations of the individual, the identity of the recipient, whether the recipient has an interest in knowing the information disclosed, etc.

A contextual approach may pave the way for a more flexible framework necessary to adequately address the *kind* of harm resulting from the processing of personal information.[867] However, before elaborating on this full contextual approach, we first need to understand what kind of so-called "harms" DPLs were looking to address in the first place. My analysis should therefore be viewed as a first step towards a contextual model. Also, since a full contextual approach provides for a very subjective framework with the limits that I further discuss in section 2.2.1.3.2 (more subjectivity as to which data handling situations are covered under DPLs or which information qualifies as *personal* and therefore, more legal uncertainty), I propose a framework under which certain additional criteria which pertain only to the information (the object of protection of DPLs) will provide guidance as to which data should in fact be covered by DPLs. Section 2.2.2 elaborates on the ultimate purpose of DPLs, which is to protect individuals against a *risk of harm*, something that is really quite subjective in nature. However, it will be my contention that the scope of DPLs transcends this subjective sphere and can also be applied to other more *objective* types of harms.[868]

The definition of *personal information* is a legal construct. An interpretation taking into account the ultimate purpose behind DPLs will do just that: consider the rationale for this definition and determine how to best apply this rationale to any technology or piece of data in light of new technologies and the reality of the Information Age.

Before arguing for protection of information, it is necessary to consider what kind of information is to be protected and why, taking into account the goals of DPLs. Using an interpretation may be the proper way to translate the ultimate goal behind DPLs. Although it does present certain challenges, which are discussed below, I maintain that this approach has various benefits, which outnumber any potential drawbacks.

---

[867] See section 2.2.1.4.1 entitled "Providing More Flexibility ("Privacy" and "Harm" are Contextual)" which elaborates on this issue. See also section 2.2.1.3.2(d) entitled "Certain Jurisdictions Have Already Adopted a Flexible Interpretation " which discuses the fact that in Canada, the OPCC has been using a "total context approach" to interpret the notion of "personal information" in certain situations, claiming that doing so, it has been able to take into account the broader and more important context of the collection, use and disclosure of information.

[868] See section 2.2.2.1 entitled "Privacy and Data Protection are not One and the Same" which details the difference between "privacy" and "data protection".

2.2.1.3. Limits of a Purposive Approach

The two main limits regarding the implementation of a purposive approach are the following: first of all, the lack of a balance test to weigh privacy rights against countervailing values and secondly, the potential for more legal uncertainty.

2.2.1.3.1. Does not Provide a Balance Test : Privacy vs. Countervailing Values

As we have already seen, the all-encompassing notion of *personal information* entails not only the protection of data which may be harmful to individuals, but also a prohibition on the circulation of any data on individuals. This outcome is over-reaching and is especially problematic in light of the fact that data flows may be beneficial to society.[869] Also, placing the right to privacy ahead of other important rights and freedoms or competing values poses many unique challenges.[870]

Adopting a purposive approach to interpreting *personal information* will not provide for any type of "balance test" to weight the interest of the society against the right to individual privacy or the individual's right of control over his or her information.[871] It will also not provide for the framework allowing to balance the right to privacy with countervailing values such as the right to free speech and the right of the public to know.[872]

While the proposed approach will not provide these tools, a purposive interpretation of *personal information* will, at the very least, limit the scope and the extent of the information protected under DPLs. For instance, under the proposed approach, only data which were meant to be protected (instead of all personal information in a broader sense) will be covered by the definition. Since section 2.2.2 determines that the purpose of DPLs is to protect individuals against the *risk of harm* resulting from the collection, use or disclosure of their information, only the data, which creates such risk of harm, will in fact be covered by DPLs. This will therefore allow for the data, which were not meant to be covered by DPLs (which do not create a risk of harm to

---

[869] See section 2.1.1.1.1 entitled "Ignoring the Importance of Information Flow For the Society" which elaborates on this issue.

[870] See section 2.1.1.1.3 entitled "Ignoring Countervailing Values" which elaborates on this issue.

[871] See section 2.1.1.1 entitled "Privacy as an Absolute Right" which elaborates on this issue and more specifically, section 2.1.1.1.1 entitled "Ignoring the Importance of Information Flow For the Society".

[872] See section 2.1.1.1.3 entitled "Ignoring Countervailing Values" which elaborates on this issue.

individuals) to circulate freely. This also means that the "balancing" of countervailing rights will come as a second step, only if conflicting values are in fact at stake.

2.2.1.3.2. Outcome of Having a More Subjective Definition: More Legal Uncertainty

Canadian and French DPLs regulate *personal information* very broadly, to the point where a literal interpretation of this notion can create various uncertainties as to which data are in fact covered.[873] It could be argued that a purposive interpretation of *personal information* may lead to an even more subjective definition, potentially resulting in two unwanted outcomes.

First, and to begin with, a purposive approach (instead of a literal interpretation) used in determining what kind of data constitutes *personal information* under DPLs may potentially lead to more subjectivity. Subjectivity means uncertainty and additional subjectivity in interpreting *personal information* could translate into even more legal uncertainty. Organizations that handle information would be affected if they do not always know which kind of data is covered under a given DPL. They will therefore not know whether the obligations imposed on them by DPLs have to be respected. For instance, should the collection of data be disclosed to the relevant individuals or authorities? Moreover, should security measures be implemented in order to protect the data? This uncertainty will also impact individuals who will not always be aware of precisely when their information or profiles are covered under DPLs. Individuals will therefore have difficulty in assessing whether they can access their information (or profiles) or request that their information be updated, and so on.

Under the proposed approach, organizations handling personal information would have to determine if certain pieces of information are covered by DPLs, by following certain guidelines detailed in section 3 of this thesis. Interpreting the notion of *personal information* using a purposive approach may not always be easy to do in a consistent way and could lead to quite different results. The proposed guidelines will bring certain type of potentially subjective criteria further detailed in section 3 of this thesis. This means that the same piece of data could technically be "evaluated" by different organizations differently, one taking the position that a certain piece of data (for

[873] See section 2.1.2.2 for details on this issue.

example an IP address) qualifies as personal information and another, that it doesn't. Moreover, each piece of data would need to be evaluated in accordance with the proposed interpretation guidelines. This would mean that initially, whether a certain piece of data qualifies as *personal information* would always be dependent on other factors. The test proposed in section 3 of this thesis, which resembles a decision tree, would have to be applied to this data. The proposed approach will potentially have the outcome of greatly limiting the scope and range of the information protected and covered by DPLs, moving away from the model under which certain pieces of data will "always" qualify as *personal information*.[874] A certain piece of information such as a person's name which is usually considered as *personal information* under DPLs, may not be automatically covered by the notion of *personal information* using the proposed approach: if the collection, use or disclosure of this information creates no potential harm for the individual in question, this information will not qualify as *personal information* under the proposed model.[875]

Second, some could argue that the uncertainty triggered by the proposed approach would go against the "control" notion of privacy. As a matter of fact, the subjectivity resulting from the approach could create the situation in which organizations handling personal information may be the ones at the end of the day making the judgment call on which kind of data actually qualifies as "personal" (or not). The "control" notion of privacy would therefore be restricted and individuals would end up having less control over their information if organizations become in charge of deciding what kind of data is ultimately worthy of protection. Therefore, this uncertainty may be translated into less "control" for individuals over their personal information, and more control by organizations handling personal information. Since these organizations will be the ones partly responsible for taking a position on what constitutes *personal information*, some

[874] It will also, at the same time, ensure that only the data which should be covered by DPLs are in fact covered, also addressing over-reaching outcomes of DPLs discussed in section 2.1.2.1.1(d) entitled "Consequences of Over–Inclusiveness".

[875] See section 2.2.2 entitled "Determining Risk of Harm as Purpose Behind the Protection of Personal Information" which elaborates on the fact that the ultimate goal behind DPLs is the avoidance of a risk of harm to individuals.

may worry that they might use this uncertainty to their advantage as they have done in the past with new types of data or with profile data.[876]

Concerns have already been expressed over having some type of subjectivity in the evaluation of what kind of data qualifies as *personal information*. For instance, in the U.K., in the late 1970s, before they had adopted a DPL, it was reported that the Lindop Committee rejected having a certain subjectivity related to the "harm" that data may cause to an individual when evaluating such information, the main reason being that there was no objective standard whereby a data controller could assess harm prior to the processing of personal data.[877] Judging whether certain personal data would be sensitive or non-sensitive was a subjective assessment.[878]

The APEC Privacy Framework has adopted a "Prevention of Harm" principle under which organizations should prevent tangible harms to individuals and provide for appropriate recovery for those harms if they occur.[879] Many authors (such as Graham Greenleaf and Colin J. Bennet) criticised this *harm* principle when used in the context of information privacy, for the main reason that this is not a privacy principle.[880]

---

[876] See section 2.2.1.3.2(c) entitled "Organizations Already Doing as They Please with New Types of Data " which elaborates on this issue. In answer to this concern, I raise that DPLs already contain a lot of subjectivity and that if legislators are concerned with the fact that organizations handling data are not "motivated" to act in compliance with the provisions of DPLs, then they need to increase the penalties for non-compliance or ensure that organizations, at the end of the day, will be accountable for their data handling activities. I am not of the view that having an overly broad definition of *personal information* is the proper way to ensure proper data protection compliance.

[877] See Lindop, *supra* note 96 at paras. 18.24–18.27. Lindop concluded that there was no objective standard whereby a data controller could assess harm prior to the processing of personal data because there was no way an organization could judge whether its personal data or its processing would be sensitive or non-sensitive. This was because sensitivity was a subjective assessment that could only be accurately judged by each data subject concerned. Lindop also concluded that the impact of the principles would be modified by a number of factors – for instance, whether there was foreseeable harm to the data subject, the sensitivity of the personal data, or whether the personal data were in the public domain.

[878] See *ibid*.

[879] APEC, *Privacy framework*, *supra* note 363 at Principle 1: "Recognizing the interests of the individual to legitimate expectations of privacy, personal information protection should be designed to prevent the misuse of such information. Further, acknowledging the risk that harm may result from such misuse of personal information, specific obligations should take account of such risk, and remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information." See also section 2.2.2.2.2 entitled "Risk of Harm in Recent Documents" which elaborates on this issue.

[880] Graham Greenleaf, "APEC's Privacy Framework: A New Low Standard" (2005) 11 Privacy Law & Policy Reporter 121; Graham Greenleaf, "Criticisms of the APEC Privacy Principles (Version 9), and recommendations for improvements" (2004) [Prepared for publication and for consideration by the Australian Privacy Foundation (APF) and by the Asia-Pacific Privacy Charter Council (APPCC)]; Graham Greenleaf, "The APEC privacy initiative: 'OECD Lite' for the Asia-Pacific?" (2004) 71 Privacy Laws &

Pounder argues that this "harm" principle would not look at privacy protection from the point of view of the individual (since it is the individual who can accurately perceive any harm, and not the organization).[881] He states:

> "It states that "specific obligations should take account of such risk (…) threatened by the collection, use or disclosure of personal data". Thus, if no harm is perceived (e.g. by Government or by data controllers), then the impact of other principles can be negated (e.g. by allowing specific exemptions or not implementing certain procedures). There is a curious side effect which illuminates the central problem to this approach: access by the data subject to his or her own personal data can be refused if there is little risk of harm to the data subject, yet the reason why the data subject might want to seek access is to find out whether the processing is causing him harm" (…)[882]

While Pounder raises an interesting point, I argue that in the context of the Internet, the individual is not always fully able to perceive this *risk of harm*,[883] in part because of the increasingly sophistication in new technologies.[884]

The Australian Government recently did a 28-month inquiry into the extent to which its *Privacy Act 1988* and related laws continue to provide an effective framework for the protection of privacy in Australia. As part of this inquiry, a consultation was made as to whether a model Unified Privacy Principles ("UPPs") should include such a "prevention harm" principle. The Australian Law Reform Commission ("ALRC") Report 108 was

---

Business 16*;* Graham Greenleaf, "Five years of the APEC Privacy Framework: Failure or promise?" (2009) Computer Law & Security Report 25 at 28-43; Colin J. Bennet, "The APEC Privacy Framework: A Trading-up of Standards or the Opposite?" (Paper delivered at the Conference on privacy and security, Victoria, 9 and 10 February 2006).

[881] Chris Pounder, "Why the APEC Privacy Framework is unlikely to protect privacy" (15 October 2007), online: Out-law.com <http://www.out-law.com/page-8550>: "This approach (that assumes the data subjects assess the potential for harm) has been adopted by most countries that have data protection law. It is the exact opposite to the Framework's approach (that suggests the principles can be dispensed with, if no harm is apparent to the data controller of the government implementing the data protection law). Of course, risk assessment tools (e.g. Privacy Impact Assessments) could be used by the data controller to reveal or quantify risks and thereby reduce harm. However, the use of such tools does not avoid the fundamental misconception underpinning a principle based on harm; it is the data subject who can accurately perceive any harm and not the data controller."

[882] *Ibid*.

[883] See section 2.1.1.2 entitled "Notice and Choice Approach Challenged" which elaborates on this issue.

[884] See section 2.1.1.2.2(c) entitled "Technology Becoming Increasingly Sophisticated" which elaborates on this issue.

published in August 2008, which represents the culmination of the inquiry.[885] This Report mentions that some stakeholders or participants have supported the inclusion of a specific privacy principle in the model UPPs dealing with the prevention of harm.[886] For instance, Veda Advantage submitted that this aligns with the overall "purpose of regulating information flows, [which] is to protect individuals from harmful uses of information".[887] The majority of stakeholders that commented on this issue, however, opposed a "Prevention of Harm" principle.[888] One stakeholder argued that this is an unsuitable subject to be addressed in a privacy principle:

> "The sentiment that privacy remedies should concentrate on preventing harm (…) is unexceptional but it is strange to elevate it to a privacy principle because it neither creates rights in individuals nor imposes obligations on information controllers. To treat it on a par with other Principles makes it easier to justify exempting whole sectors (e.g. small business in Australia's law) as not sufficiently dangerous, or only providing piecemeal remedies in 'dangerous' sectors (as in the USA)."[889]

The Law Council of Australia was concerned that such a principle would be too imprecise because it is difficult to articulate a precise meaning of "harm".[890] Under the ALRC's view, they felt that a number of the principles in the model UPPs already incorporated a harm prevention approach (such as data "quality", data "security", etc.),[891] but more interestingly, they felt that the obligations imposed by a general

---

[885] Austl., Commonwealth, Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (Report No. 108) (Canberra: Australian Government Publishing Service, 2008) [Austl., Report No. 108].

[886] Government of South Australia, *Submission PR 187*, 12 February 2007; Veda Advantage, *Submission PR 163*, 31 January 2007; Centre for Law and Genetics, *Submission PR 127*, 16 January 2007.

[887] Veda Advantage, *Submission PR 163,* 31 January 2007.

[888] Austl., Office of the Privacy Commissioner, *Submission PR 499,* 20 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487,* 19 December 2007; Australian Federal Police, *Submission PR 186,* 9 February 2007; G Greenleaf, N Waters and L Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007; Law Council of Australia, *Submission PR 177,* 8 February 2007; AAMI, *Submission PR 147,* 29 January 2007; National Health and Medical Research Council, *Submission PR 114,* 15 January 2007.

[889] Graham Greenleaf, Nigel Waters and Lee Bygrave—Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007, citing Graham Greenleaf, 'APEC's Privacy Framework Sets a New Low Standard for the Asia-Pacific' in A Kenyon and M Richardson (eds), *New Dimensions in Privacy Law: International and Comparative Perspectives* (2006) 91, 100.

[890] The Law Council of Australia raised that while financial harm and damage to reputation or character are concepts which are well understood, other concepts of harm which are raised within the privacy debate such as "distress" and the knowledge that someone has their personal information are harder to place within a legislative context. See the Law Council of Australia, *Submission PR 177,* 8 February 2007.

[891] Austl., Report No. 108, *supra* note 885 at s. 32: "In particular, the 'Data Quality' principle and the 'Data Security' principle impose specific obligations to ensure the integrity of personal information that is handled

"Prevention of Harm" principle could be undesirably vague.[892] Accordingly, the ALRC decided not to support including such a principle in the model UPPs.[893] In answer to this concern ("harm" is too imprecise), I argue that the current definition of *personal information* is so broad that it already results in various uncertainties[894] and that various data protection principles already embodied in DPLs are extremely subjective.[895]

In recent years, when certain Canadian DPLs introduced notification obligations in the event of data security breaches, it was cautioned that notification obligations were falling short because they gave too much power or control to organizations and industry players whose data was compromised. Under Bill C-12 introduced in 2011, such breaches are to be reported to the privacy commissioner only if they are "material" and are to be disclosed to individuals only if they pose a "real risk of significant harm".[896] John Lawford, counsel with the PIAC, raised that these standards ("material" and "real risk of significant harm") are difficult to meet and even harder to measure (as they are relatively subjective).[897] Also, the fact that in both instances, it was the organizations themselves, which would determine whether the breaches had met those thresholds, was another concern. David Canton also shares the view that the language of these threshold tests is not as clear as they could be:

> "Since "material" remains a subjective test, it is somewhat at the discretion of the entity to determine whether the breach is "material." Individuals must be notified only "if it is reasonable in the circumstances

---

by agencies and organisations, and to guard against possible misuse and unauthorised disclosure. The 'Anonymity and Pseudonymity' principle also aims to lessen the threat of personal information being misused by reducing the amount of personal information that agencies and organisations collect."

[892] *Ibid*.

[893] *Ibid*. at s. 32: "In particular, the 'Data Quality' principle and the 'Data Security' principle impose specific obligations to ensure the integrity of personal information that is handled by agencies and organisations, and to guard against possible misuse and unauthorised disclosure. The 'Anonymity and Pseudonymity' principle also aims to lessen the threat of personal information being misused by reducing the amount of personal information that agencies and organisations collect."

[894] See section 2.1.2.2 which elaborates on this issue.

[895] See section 2.2.1.3.2(a) entitled "DPLs Already Subjective on Various Issues" which elaborates on this issue.

[896] *Safeguarding Canadians' Personal Information Act*s, *supra* note 506 aimed to amend PIPEDA, was re-introduced by the Government of Canada on September 29, 2011.

[897] Michael McKernan, "New federal privacy, anti-spam bills get mixed reviews" *Law Times* (31 May 2010), online: Law Times <http://www.lawtimesnews.com/201005316982/Headline-News/New-federal-privacy-anti-spam-bills-get-mixed-reviews>.

> to believe that the breach creates a real risk of significant harm to the individual." Again, this requirement is somewhat at the discretion of the entity that would have to notify the individual. Some will argue that the discretionary component of the notification requirements is valuable as it is not mandatory to disclose minor breaches. That may be a good thing, but it will take some time to figure out how to apply the tests in practice. The difficult part is knowing where the threshold actually is. The wording of the breach notification provisions leaves the possibility that entities may abuse the discretion provided to them and choose not to report breaches that many would argue are major."[898]

It is possible that the proposed interpretation may, in some cases, lead to a more flexible framework than the current one. But the concerns mentioned above (too much subjectivity and more legal uncertainty) can be challenged. I am of the view that the proposed approach can not be dismissed outright for this reason alone. Yes, the proposed approach will have the outcome of having organizations handling personal information more responsible for taking a position on what constitutes *personal information*, with the concerns that this can trigger.[899] However, with all the current uncertainty surrounding which information actually qualifies as *personal*,[900] organizations already have a lot of saying in what constitute *personal information*. Sections 1.1.2 and 2.1.2.1.1(a) elaborate on the fact that the FIPs (incorporated in DPLs) were meant to remain relevant even in the face of continuous technological improvements; the definition of *personal information* was drafted in broad terms in large part to ensure this. Koops articulates the view that a legislation that is too focused on sustainability and hence abstracts very much away from technology will result in vague laws that provide little legal certainty.[901] With *personal information* becoming little more than a nebulous notion and ongoing challenges to the concept of "identifiability", it could be said that DPLs that incorporate flexible principles (the FIPs) already provide little legal certainty.

---

[898] Canton, *supra* note 597.

[899] For example, they might use this subjectivity or uncertainty to their advantage as they have in the past with new types of data. See sections 2.1.2.2.1 entitled "Notion of Identifiable Individual", section 2.1.2.2.2 entitled "Identifying a Device or an Object" and section 2.1.1.2.1(b) entitled "Organizations Communicating their Practices in Conflict of Interests" which discuss this issue.

[900] See section 2.1.2.2 which elaborates on this issue.

[901] Koops, *supra* note 821 at 21.

Given that DPLs already contain a lot of subjectivity as illustrated below, it is even debatable if any such concern (potential increase in subjectivity and legal uncertainty) is a valid one.[902]

(a) DPLs Already Subjective on Various Issues

There is already a lot of subjectivity surrounding the application of DPLs. Because of this subjectivity, organizations and industry players handling personal information already enjoy a certain degree of control and discretion over the types of data that are to be included as *personal information* as well as how this data must be managed. Most DPLs are to a certain extent flexible, leaving organizations and industry players much room for interpretation in handling data.[903] There are various examples which can be used in order to illustrate the subjectivity found in the Canadian and French DPLs as well as in Directive 95/46/EC:

(i) Reasonableness or Legitimacy Tests

First, many DPLs have some type of "reasonableness" or "legitimacy" tests. For example, under subsection 5(3) of PIPEDA, an organization may collect, use or disclose personal information "only for purposes that a reasonable person would consider appropriate in the circumstances."[904] Since under PIPEDA any information can be considered sensitive, "depending on the context",[905] organizations and industry players handling data also have some measure of control regarding the sensitivity of the data. The Alberta DPL and the B.C. DPL also have various "reasonableness tests" which are similar to the ones found in PIPEDA and which leave some subjectivity to be assessed by organizations handling the data.[906] In meeting its responsibilities under the Alberta DPL or the B.C. DPL, an organization must act "in a reasonable manner",

---

[902] If legislators are concerned with the fact that organizations handling data are not "motivated" to act in compliance with the provisions of DPLs, then they need to increase the fines or penalties for non-compliance or ensure that organizations will be held more accountable for their data handling activities. An overly broad definition of *personal information* which can potentially cover all information in circulation is not the proper way to ensure data protection compliance.

[903] In the Directive 95/46/EC, some examples of subjective provisions are contained in article 7.f (balance of interest to justify processing), last paragraph of 10 (c) and 11.1 (c) (information to the data subject where necessary to guarantee fair processing), or 18 (exemptions from notification requirements).

[904] PIPEDA, *supra* note 63 at art. 5 (3).

[905] *Ibid*. at Schedule 1 (s. 5), principle 4.3.4.

[906] Alberta DPL, *supra* note 114 at Part 2, Division 3, s. 11 (1) and (2); See also Part 1, s. 3; B.C. DPL, *supra* note 115 at Part 4, s. 11.

and must develop and follow policies and practices "that are reasonable for the organization" to meet its obligations.[907] The golden standard is as follows: "what a reasonable person would consider appropriate in the circumstances"; quite a subjective criterion.[908] In Quebec, an organization can only establish a file on an individual for a "serious and legitimate reason."[909] In France, personal data can only be processed for "legitimate" purposes,[910] consistent with Directive 95/46/EC, which states that "any processing of personal data must be lawful and fair to the individuals concerned",[911] and personal data must be collected for "legitimate" purposes.[912] Under such "reasonableness", "legitimacy", or "fairness" tests, it is the organization handling the data that will make the judgment call of what is "reasonable", "legitimate" or "fair", which is a very subjective assessment.

(ii) Subjectivity in Type of Notices Provided and Method of Obtaining Consents

Certain DPLs provide for some measure of subjectivity when it comes to disclosing data protection practices to individuals. In Canada, PIPEDA states that organizations shall make a "reasonable effort" to ensure that the individual is advised of the purposes for which the information will be used or disclosed, which must be communicated in such a manner that the individual "can reasonably understand" such purpose.[913] The Alberta DPL has a similar reasonableness provision since an organization may collect, use or disclose personal information about an individual if it provides notice, "in a form that the individual can reasonably be expected to understand".[914] The B.C. DPL also has a similar requirement.[915]

There is a lot of subjectivity surrounding the notion of "consent" depending on the given DPL. PIPEDA specifies that the form of consent sought by the organizations may vary,

---

[907] Alberta DPL, *supra* note 114 at Part 2, Division 1, s. 5 (5); B.C. DPL, *supra* note 115 at Part 2, s. 4 (1).

[908] Alberta DPL, *supra* note 114 at s. 2; B.C. DPL, *supra* note 115 at Part 2, s. 4 (1).

[909] Quebec DPL, *supra* note 110 at s. 4.

[910] *Loi informatique et liberté*, *supra* note 131 at c. II, s. 1, art. 6 (1) and (2).

[911] EC, *Directive 95/46/EC*, *supra* note 99 at Whereas (28).

[912] *Ibid*. at art. 6 (1) (b).

[913] PIPEDA, *supra* note 63 at Schedule 1 (s. 5), principle 4.3.2.

[914] Alberta DPL, *supra* note 114 at Part 2, Division 2, s. 8 (3).

[915] B.C. DPL, *supra* note 115 at Part 3, s. 8 (3) (a), (b), (c), (d), (e).

"depending upon the circumstances and the type of information" and "the sensitivity of the information."[916] Furthermore, in obtaining consent, "the reasonable expectations of the individual are also relevant".[917] In Alberta, an individual is deemed to consent to the collection, use or disclosure of personal information if "it is reasonable" that a person would voluntarily provide that information.[918] Under the B.C. DPL, an individual is deemed to consent to the collection, use or disclosure of personal information if at the time of consent, the purpose would be considered to be "obvious to a reasonable person".[919]

(iii) Subjectivity Pertaining to Collection, Use and Disclosure Activities

There is also subjectivity surrounding the right for an organization to collect personal information from third parties (instead of directly from the individual) or without the individual's consent. In Quebec, an organization may collect personal information from a third person without the consent of the person concerned "if he has a serious and legitimate reason" for doing so.[920] In Alberta and B.C., the relevant criterion (collecting information without consent) is if the collection is "in the interests of the individual".[921] What exactly these "legitimate reasons" are, or in which cases a given collection is "in the interest of the individual" are subjective assessments. At the point of collection, the organization collecting the information is the one making this judgment call.

There is also a certain degree of subjectivity in some DPLs with regards to the disclosure of personal information without the consent of the individual. In both Alberta and B.C., an organization may disclose personal information "for purposes that are reasonable" (Alberta)[922] or "for purposes that a reasonable person would consider are appropriate in the circumstances" (B.C.).[923] In B.C., this disclosure can take place

---

[916] PIPEDA, *supra* note 63 at Schedule 1 (s. 5), principle 4.3.4.

[917] *Ibid*. at Schedule 1 (s. 5), principle 4.3.5.

[918] Alberta DPL, *supra* note 114 at Part 2, Division 2, s. 8 (2).

[919] B.C. DPL, *supra* note 115 at Part 3, s. 8 (1) (a) and (b).

[920] Quebec DPL, *supra* note 110 at s. 6.

[921] Alberta DPL, *supra* note 114 at Part 2, Division 3, s. 11 (a); B.C. DPL, *supra* note 115 at Part 4, s. 12 (1) (a).

[922] Alberta DPL, *supra* note 114 at Part 2, Division 5, s. 19 (1) and (2).

[923] B.C. DPL, *supra* note 115 at Part 6, s. 17 (a).

without the consent of the individual if it is "in the interests of the individual".[924] In France, there is a similar provision provided that the processing of personal data without consent is legal if it is done for a "legitimate purpose", taking into account the individual's fundamental rights.[925]

In Quebec, there is an exemption for obtaining the individual's consent prior to disclosing personal information to a third party which may want to then use it for purposes of commercial or philanthropic prospection. According to the Quebec DPL, an organization may, without obtaining prior consent, communicate a nominative list, if this communication "does not infringe upon the privacy of the persons concerned."[926] How this works in practice and identifying the situations in which the transfer of a marketing list infringes on the privacy of individuals is anything but objective.

DPLs are quite subjective on what kinds of uses of the personal information are acceptable. In Quebec, an organization may only use personal information for purposes which are "relevant" to the object of the file, in the absence of consent.[927] Under the B.C. DPL, an organization may use personal information only for purposes that "a reasonable person would consider appropriate in the circumstances",[928] and it may use the information without the consent of the individual, "if the use is clearly in the interests of the individual".[929] In France, the processing of personal data can only take place if the data is collected and processed in an honest and legitimate manner.[930] Organizations therefore can make a subjective assessment as to whether a given use is relevant, appropriate or reasonable in the circumstances.

(iv) Subjectivity in Security Measures to Adopt and Retention Obligations

DPLs usually provide for subjectivity in the assessment of the security measures that have to be implemented by an organization to protect the personal information that it is

---

[924] *Ibid*. at Part 6, s. 18 (1) (a).

[925] *Loi informatique et liberté*, *supra* note 131 at c. II, s. 1, art. 7 (5).

[926] Quebec DPL, *supra* note 110 at s. 22.

[927] *Ibid*. at s. 13.

[928] B.C. DPL, *supra* note 115 at Part 5, s. 14 (a).

[929] *Ibid*. at Part 5, s. 15 (1) (a).

[930] *Loi informatique et liberté*, *supra* note 131 at c. II, s. 1, art. 6 (1) and (2).

handling. PIPEDA provides that personal information shall be protected by security safeguards "appropriate to the sensitivity of the information",[931] and that the nature of the safeguards will vary depending on "the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage".[932] The Quebec DPL,[933] the Alberta DPL,[934] and the B.C. DPL[935] all have similar very subjective security requirements.

In France, there is also a provision under which the "necessary measures" need to be taken by the organization processing personal data in light of the "risks" that the processing entails.[936] This provision is in line with article 17 of Directive 95/46/EC which states that "appropriate" technical and organizational measures be taken in order to maintain the security of the data, and that such measures shall ensure a level of security "appropriate to the risks represented by the processing and the nature of the data to be protected."[937] These security tests are context-based and quite subjective. It is therefore up to the organizations to determine what these "reasonable", "necessary" or "appropriate" measures are.

As already mentioned, certain DPLs provide for a very subjective notification obligation in the event of a security breach. In Canada, the Alberta DPL states that an organization must provide notice to the Alberta Privacy Commissioner of any incident involving the unauthorized access to or disclosure of personal information if, "a reasonable person would consider that there exists a real risk of significant harm to an

---

[931] PIPEDA, *supra* note 63 at Schedule 1 (s. 5), principle 4.7.

[932] *Ibid*. at Schedule 1 (s. 5), principle 4.7.2.

[933] Quebec DPL, *supra* note 110 at s. 10. It is interesting to note that prior to the adoption of Bill 86, the Quebec DPL did not, *per se*, allow an entreprise to adapt its safeguard measures based on the sensitivity of the information. But the CAI has considered the "sensitivity" of personal information in some decisions. This debate became academic with the new wording of section 10 of the Quebec Private Sector Act, which includes sensitivity as one of the factors to be considered. See *X. and Y. v. Hôpital du Sacré-coeur de Montréal*, (16 July 2002), CAI 98 13 00, v. C. Constant, J. Stoddart and M. Laporte; *X. v. Ville de Saint-Laurent*, (14 June 2000), CAI 97 04 78, v. P.-A. Comeau; *X. v. Centre de protection et de réadaptation de la Côte-Nord*, (24 July 2003), CAI 02 06 08, v. D. Boissinot; *X. v. Ministère de la Sécurité Publique*, (4 August 2003), CAI 02 06 20, v. D. Boissinot.

[934] Alberta DPL, *supra* note 114 at Part 3, Division 2, s. 34.

[935] B.C. DPL, *supra* note 115 at Part 9, s. 34.

[936] *Loi informatique et liberté*, *supra* note 131 at c. V, s. 1, art. 35.

[937] EC, *Directive 95/46/EC*, *supra* note 99 at art. 17 (1).

individual".[938] This assessment is again rather subjective. In Europe, organizations have to provide notification to third parties, to whom personal data have been disclosed, of any rectification, erasure or blocking carried out in compliance with Directive 95/46/EC, "unless this proves impossible or involves a disproportionate effort."[939] Whether a certain effort is disproportionate or not will be determined by the organization.

There is also a great deal of subjectivity with regards to the retention delay requirement. In Canada, personal information under PIPEDA shall be retained only as long "as necessary" for the fulfilment of those purposes.[940] France has a similar requirement and the data must be kept for only as long "as necessary" for their purpose of collection,[941] consistent with article 6 of Directive 95/46/EC.[942] Personal information that has been used to make a decision about an individual shall be retained "long enough" to allow the individual access to the information after the decision has been made.[943] In Alberta, an organization may retain personal information only for as long as the organization "reasonably requires" the information for legal or business purposes. Within a "reasonable period" of time after an organization no longer "reasonably requires personal information", the organization must destroy or render the information non-identifying. [944] In B.C., there is a similar requirement.[945] As illustrated above, according to most DPLs, organizations handling personal data may decide for how long it is reasonable for them to retain the data, and at what point the information becomes non-identifying.[946]

---

[938] Alberta DPL, *supra* note 114 at Part 3, Division 2, s. 34.1 (1).

[939] EC, *Directive 95/46/EC*, *supra* note 99 at art. 12 (c).

[940] PIPEDA, *supra* note 63 at Schedule 1 (s. 5), principle 4.5.

[941] *Loi informatique et liberté*, *supra* note 131 at c. II, s. 1, art. 6 (5).

[942] EC, *Directive 95/46/EC*, *supra* note 99 at art. 6 (1) (e).

[943] PIPEDA, *supra* note 63 at Schedule 1 (s. 5), principle 4.5.2.

[944] Alberta DPL, *supra* note 114 at Part 3, Division 2, s. 34.1.

[945] An organization must destroy personal information or render the information non-identifying, "as soon as it is reasonable" once the purpose of collection is no longer being served by retention. B.C. DPL, *supra* note 115 at Part 9, s. 35 (2) (a), (b).

[946] It is interesting to note that this concern (of having individuals decide for how long an organization could retain their data instead of the organization) is not a new one. Documents from the seventies illustrate that already back then, this concern was on the table. Lindop, *supra* note 96 at 51, para. 5.59.

(v) Subjectivity in Access Rights and Data Quality

DPLs usually allow for a right of access and rectification to personal information in the hands of organizations. There is substantive subjectivity surrounding this access right. For example, in Canada, PIPEDA states that in certain situations which should be "limited and specific", an organization may not have to provide access to personal information it holds, which leaves room for interpretation by organizations.[947] Under the Alberta DPL, an organization must provide the applicant with access to the applicant's personal information "taking into consideration what is reasonable",[948] and may refuse to provide access to personal information in certain circumstances if it is "not unreasonable to withhold that information".[949] In France, the organization can refuse to comply with the access requests if they are "abusive".[950] In Europe, Directive 95/46/EC stipulates that organizations shall provide "as appropriate", the rectification, erasure or blocking of data the processing of which does not comply with its provisions.[951] Furthermore an organization does not need to comply with this obligation if the provision of information "proves impossible or would involve disproportionate efforts".[952] Again, subjectivity allows for organizations to actually decide when to grant access to personal information that is in their possession.

The data quality principle found in all DPLs also gives rise to subjectivity. In Canada, PIPEDA specifies that the extent to which personal information shall be accurate, complete, and up-to-date "will depend upon the use of the information, taking into account the interests of the individual".[953] In Alberta, an organization must make a "reasonable effort" to ensure that any personal information handled is accurate and complete "to the extent that is reasonable for the organization's purposes".[954] There is a similar requirement in the B.C. DPL,[955] which further states that if an organization is

---

[947] PIPEDA, *supra* note 63 at Schedule 1 (s. 5), principle 4.9.

[948] Alberta DPL, *supra* note 114 at Part 3, Division 1, s. 24 (1.2).

[949] *Ibid*. at Part 3, Division 1, s. 24 (2) (a), (b) and (d).

[950] *Loi informatique et liberté*, *supra* note 131 at c. V, s. 1, (II), art. 39.

[951] EC, *Directive 95/46/EC*, *supra* note 99 at art. 12 (b).

[952] *Ibid*. at Whereas (40).

[953] PIPEDA, *supra* note 63 at Schedule 1 (s. 5), principle 4.6.1.

[954] Alberta DPL, *supra* note 114 at Part 3, Division 2, s. 33.

[955] B.C. DPL, *supra* note 115 at Part 9, s. 33 (a).

satisfied "on reasonable grounds" that a request made should be implemented, then it must correct the information.[956] Also, an organization must make a "reasonable effort" to ensure that personal information collected by or on its behalf is accurate and complete, if it is likely to be disclosed to another organization (B.C.).[957] Similar requirements are found in Directive 95/46/EC which states that "every reasonable step" must be taken to ensure that data which are inaccurate or incomplete are erased or rectified.[958]

In light of the examples discussed above, it is clear that DPLs are already very subjective. Organizations are already having a lot of control on what kind of data handling activities are in fact covered by DPLs, on whether the information that they handle is sensitive and the risks that this handling may entail. Therefore, arguing that a purposive interpretation to the definition of personal information will further reduce the control that individuals have on their data is not realistic, since they already do not have total control over their information. It is already some type of "joint control" between individuals and organizations handling their personal information.

(b) Individuals Already Not in Total Control of their Information

With this degree of subjectivity surrounding the application of DPLs (detailed in section (a) above), organizations and industry players are invested with a certain measure of control over various types of information. Although the notion of privacy as "individuals in control of their personal information" is great in theory, it is also utopic. We would not be honest with ourselves if we believed that individuals have absolute control over their personal information under DPLs.

In the early 1970s, when FIPs were discussed and being established, the right of an individual to control personal information was not to be "untouchable", as the inclusion of various loopholes was being considered.[959] It was already quite clear that the said "control over the information" was not uniquely in the hands of the individual. Rather, there was some type of dual control between the individual and the organization

---

[956] *Ibid*. at Part 7, s. 24 (2) (a), (b).

[957] *Ibid*. at Part 9, s. 33 (b).

[958] EC, *Directive 95/46/EC*, *supra* note 99 at art. 6 (1) (d).

[959] U.S. Department of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *supra* note 57 at s. III.

handling the personal information of the individual.[960] In 1973, a Scottish report mentioned that: "Personal privacy, as it relates to personal-data record keeping must be understood in terms of a concept of mutuality."[961]

Many believe that it is impossible or unrealistic for an individual to keep complete control over their personal information in the Internet Age.[962] Another argument which provides "food for thought" on this issue is the fact that given that DPLs are based on a "notice and consent" model, the control exercised by individuals over their personal information through consent procedures is not always effective for reasons further detailed in section 2.1.1.2. As a matter of fact, disclosures made by organizations handling personal information often do not indicate how the information will be used. Otherwise, something of little or no value will be offered in exchange for the information. And while the organization may insist that it will not share personal information with third parties, it will not explain who the third parties in question really are. Personal information therefore ends up more than often in the control of organizations, with no limitations on use. According to Nigel Waters, the prospect of individuals managing their own privacy is seductive, but to rely on this as the only means of privacy protection is unrealistic based on experience:

> "As Dyson acknowledges '[customers] are too busy consuming, or working, or just living regular lives' to be good at protecting their own interests. It is quite unrealistic to expect individuals to negotiate each and every transaction, to overcome the inevitable power imbalances and to resist the economic incentives that would be offered."[963]

It may thus be challenging to argue that the proposed purposive interpretation will reduce the "control" that individuals actually have over their personal information. Certain industry players (such as Microsoft) are even proposing a system which would

---

[960] *Ibid*. : "Each of the above formulations, however, speaks of the data subject as having a unilateral role in deciding the nature and extent of his self-disclosure. None accommodates the observation that records of personal data usually reflect and mediate relationships in which both individuals and institutions have an interest, and are usually made for purposes that are shared by institutions and individuals. In fact, it would be inconsistent with this essential characteristic of mutuality to assign the individual record subject a unilateral role in making decisions about the nature and use of his record. To the extent that people want or need to have dealings with record-keeping organizations, they must expect to share rather than monopolize control over the content and use of the records made about them."

[961] *Ibid*.

[962] See section 2.1.1 entitled "Deconstructing the Concept of Privacy as Control" which elaborates on this issue.

[963] Waters, *supra* note 508.

focus on "accountability" and interestingly, this approach would put a lot more control in the hands of the organizations handling personal information:

> "While the Data Protection Directive imposes a number of obligations on data controllers to manage personal data appropriately, in practice all too often much of the burden for controlling the use of personal data has been shifted to data subjects through notice and consent. Under an accountability-based approach, a company processing data would assume the responsibilities envisaged by the drafters of the Directive. A data controller would be responsible for understanding the risks to a data subject that comes from such processing, and for mitigating those risks. Such an approach might rely less on specific rules, instead requiring that organizations adopt policies that align with external criteria found in law -- generally accepted principles or best practices -- and foster a level of data protection commensurate with the risk to individuals. This would give organizations greater flexibility to adapt their data practices to serve emerging business models and to meet consumer demand. At the same time, organizations would be held accountable for any misuse of data in their care."[964]

The proposed approach shares some similarities with Microsoft's preferred approach as the burden for controlling the collection, use and disclosure of *personal information* will not be automatically transferred to individuals through notice and consent. An organization will have to determine if a certain piece of information creates a *risk of harm* to the individual, in which case the notice shall be provided to the individual, consent shall be obtained, and proper security measures adopted. It would be the organization collecting, using or disclosing the personal information that will initially be responsible for understanding the risks involved in its data handling activity and for mitigating those risks. Under this framework, organizations would have every incentive to make a reasonable and appropriate assessment as they would be held accountable for any harm resulting from their handling of the information.

(c) Organizations Already Doing as They Please with New Types of Data

The prospect of additional subjectivity and therefore legal uncertainty, emerging from the purposive approach proposed, could potentially have more serious implications if the current definition of *personal information* did not already present so many uncertainties.[965]

---

[964] Microsoft Corporation, *supra* note 358 at 8-9.

[965] See section 2.1.2.2 which elaborates on this issue.

There is already so much uncertainty with new types of data, that industry players usually decide for themselves which data qualifies as *personal information* (as discussed in section 2.2.1.3.2(c)). Many provide their own definition of *personal information* in their privacy policy, often different from those included in DPLs. For example, certain industry players define "sensitive personal information" as "personal information relating to confidential medical facts, racial or ethnic origins, political or religious beliefs or sexuality".[966] This version is different from the definition which can be found in certain Canadian and French DPLs.[967]

To make matters worse, industry players are thus encouraged to use this uncertainty to their advantage and decide what kind of data qualifies as personal information. More specifically, privacy policies often make a distinction between "Identifiable Information" or "personally identifiable information" ("PII") and "non-PII" (also referred to as "Aggregate Information") and this Aggregate Information is not considered as personal information by the industry. It may be constituted of one or more of the following elements: IP addresses, traffic patterns, usage patterns, survey information, previous website visited, the type of computer, Internet browser used or *clickstream* data.[968] The Internet Advertising Bureau of Canada ("IAB") illustrates the industry's position on the notion of PII vs. non-PII as they hold the view that web publishers and ad networks only collect non-PII and therefore should not be governed by DPLs.[969] In the context of behavioural targeting, most of the aggregated data collection and processing would therefore require no prior consent, given the definition of PII (vs. personal information) adopted by most industry players such as the ones detailed above. Moreover, some behavioural marketers believe that behavioral targeting data may be collected, used and disclosed provided the data is in some way "anonymized" or "de-identified" by

---

[966] See for example Google.ca Privacy Policy, online: <https://www.google.ca/intl/en/policies/privacy/key-terms/#toc-terms-sensitive-info>.

[967] See section 2.1.2.3.2 entitled "Pre-determined Categories of Sensitivite Data Challenged" which discusses the provisions of the Canadian and the French DPLs regulating the sensitivity of information.

[968] For example, Google states the following in its privacy policy: "Non-personally identifiable information (…) is information that is recorded about users so that it no longer reflects or references an individually identifiable user." See Google.ca Privacy Policy, *supra* note 966.

[969] IAB, *supra* note 284 at 8.

removing key data elements such as name or birth date.[970] There are various concerns with this practice, as outlined below.

First, behavioral marketers may collect and use web pages viewed by users, web search terms, the amount of time spent at websites, response to advertisements, and postal codes. Some may consider this information to qualify as *personal*.[971] As a matter of fact, this type of "aggregate Information" or non-PII is considered by the Privacy Commissioner of Canada and by various French courts as *personal information* in certain situations. More specifically, Canadian findings would suggest that IP addresses (computer net bios)[972] and information collected by online cookies[973] qualify as *personal information* under PIPEDA, as long as there is the *potential* of identifying an individual. In France, although conflicting rulings exist on this issue, various courts and even the CNIL has taken the position that IP addresses are *personal information*.[974]

Second, if one considers that this kind of aggregated personal information (or non-PII) does not qualify as *personal information*, then it is therefore not governed by DPLs (individuals may then not be required to consent to the collection, use and disclosure of this type of data even), although individuals may feel like it involves a breach of their privacy or may be harmful to them.[975] It is therefore interesting to note that the PIAC has articulated the view that the result of the confusion of PII with the entire sphere of personal information is cataclysmic from a personal privacy perspective.[976] For this

---

[970] PIAC, *supra* note 448 at 3.

[971] Lo, *supra* note 188 at 36.

[972] OPCC, *PIPEDA Case Summary #2001-25, A Broadcaster accused of collecting personal information via Web site* (20 November 2001), online: <http://www.privcom.gc.ca/cf-dc/2001/cf-dc_011120_e.asp>.

[973] OPCC, *PIPEDA Case Summary #2003-162*, *supra* note 748.

[974] See section 2.1.2.2.1(b) entitled "At what costs and using what kind of efforts?" which elaborates on the various positions of the French courts.and authorities on the issue of whether IP addresses are *personal information*.

[975] On this issue, the PIAC has raised that industry players often use a "black-is-white" statement of which data qualifies as *personal information* although that analysis cannot be made without examining each piece of information to see if it is indeed *personal information*. It further suggests that Google's definitions of "aggregated non-personal information" and "sensitive information" both support the theory that personal information is limited to PII and both definitions attempt to limit recourse to the rules in PIPEDA that apply to personal information by ignoring or assuming consent. See PIAC, *supra* note 448 at 4.

[976] *Ibid*.

reason, it has called upon the Canadian OPCC to impose a level of intellectual rigour in its consultations, with industry and other stakeholders, on behavioural targeting.

Third, with new technologies and the volume of data available,[977] many industry players may wish to merge or aggregate certain sets of data. Although each set of data taken separately may not qualify as *personal information*, the data, once merged, may qualify as such.[978] Also, more often than not, the data collected is mined and analyzed in order to create some type of more detailed or accurate profile of an individual. Some industry players may feel that they "own" this new profile data and can therefore do what they want with it.[979]

Hence there is currently a substantial gap between what the behavioral marketing industry considers as being a legal practice under DPLs and concerns of individuals resulting form this practice. As we now stand, behavioral marketers can easily make an argument that the data that they are collecting, using and disclosing are not *personal information* under the DPLs. And since it is in their interest to do so, they have no incentive to use an interpretation of the notion of *personal information* other than a literal one, which may actually work in their favor.

When applying the purposive interpretation to the notion of *personal information*, behavioral marketers will not be able to hide behind a literal interpretation of *personal information*. They will have to evaluate if their activities create a *risk of harm* to individuals and if so, they will have to adapt their practices accordingly and comply with DPL requirements. This issue is further discussed in section 3.1.2.3.1 and in section 3.2.3.2.2.

---

[977] See section 1.2.1 "Increase in Volume of Information" which elaborates on this issue.

[978] See section 1.2.3 "New Identifying Methods" which elaborates on this issue.

[979] On this issue, the IAB and the AAAA released the final version of the updated "Terms and Conditions Version 3.0" at the end of February 2010. One of the big questions the Terms and Conditions task force tackled with was the notion of data ownership. See IAB & AAAA, *4A's/IAB Education Guide to the Standard Terms and Conditions for Interactive Advertising for Media Buys One Year or Less, Version 3.0* (February 2010); See also Reed, *supra* note 520. This paper analyses the likely expectations of those involved in a cloud computing relationship about information ownership, and attempts to identify how closely the current legal framework matches those expectations. It also identifies the categories of information which are likely to be generated in a cloud computing relationship, and analyses how is that information is likely to be owned.

(d) Certain Jurisdictions Have Already Adopted a Flexible Interpretation

Certain jurisdictions, such as Canada, have already adopted a very subjective approach to interpreting *personal information* in certain cases. For example, the OPCC, instead of using a literal approach to interpreting the notion of *personal information,* has been using a "total context approach" to determine whether certain types of data created by an employee should be excluded from the application of DPLs. The first OPCC finding that limited the scope of the definition of *personal information* concluded that a medical prescription did not constitute a piece of personal information emanating from a physician; the argument being that the prescription was a tangible result of the physician's work activity and therefore not personal information.[980] However, in subsequent findings, the OPCC's approach has evolved and is no longer limited by the rigid distinction between personal information "produced in a work or business context" and other types of personal information.[981]

Consequently, the OPCC has been able to consider not only the narrow context of information production but also the broader and more important context of its collection, use and disclosure. In two cases, the fact that information about an identifiable individual was generated in a work or business context did not alone determine the outcome.[982] Rather, the rationality of the collection, use and disclosure of personal information was assessed in light of relevant contextual elements, including the needs of the organization and applicable industry standards. This approach is referred to as a "total context approach" to reviewing the privacy implications of specific

---

[980] OPCC, *PIPEDA Case Summary #2001-15, Privacy Commissioner releases his finding on the prescribing patterns of doctors* (2 October 2001), online: <http://www.priv.gc.ca/media/an/wn_011002_e.cfm>.

[981] For example, in *PIPEDA Case Summary #2003-220*, the Commissioner concluded that a telemarketer's sales results could be disclosed to other members of the telemarketing team, but mentioned that sales records were still considered as *personal information* and that PIPEDA would not tolerate the use of this information for purposes that are "indiscriminate, ill-defined, unnecessary, inconsistent, or otherwise unreasonable". See OPCC, *PIPEDA Case Summary #2003-220, Telemarketer objects to employer sharing her sales results with other employees* (15 September 2003) [OPCC, *PIPEDA Case Summary #2003-220*]. In *PIPEDA Case Summary #2005-303*, the OPCC was asked to determine whether the sales records of real estate agents constitute *personal information*. The OPCC ruled in the affirmative while concluding that sales records could be used only for purposes reasonably contemplated by participants in the system in which the information was entered, but also specified that this did not include the disclosure of these records to third parties for comparative and advertising purposes. See OPCC, *PIPEDA Case Summary #2005-303 Real estate broker publishes names of top five sales representatives in a city* (31 May 2005) [OPCC, *PIPEDA Case Summary #2005-303*].

[982] See OPCC, *PIPEDA Case Summary #2003-220*, *supra* note 981; OPCC, *PIPEDA Case Summary #2005-303*, *supra* note 981.

information practices.[983] It has been argued that the chief virtue of the current approach is that it enables the OPCC to investigate the privacy implications of specific information practices on a case by case basis, and to provide guidance accordingly. In developing a "total context approach", the OPCC believes that it has been mindful both of privacy rights and the needs of organizations to remain competitive, which sometimes requires collecting and using personal information from employees.[984]

While the proposed approach is different than a contextual approach,[985] this illustrates that great subjectivity is already being applied in certain jurisdictions in order to ensure that the outcome of the application of the FIPs are appropriate and context-based. A more flexible approach such as the proposed purposive approach will provide the core guidelines that may be useful when using this "total context approach" or any other flexible context-based approach.

***

Under the approach proposed in this thesis, the goal is not to remove all data protection risk, but instead to moderate the most serious risks. This strategy is consistent with certain European privacy commissioners' views such as the U.K. Information Commissioner's Office.[986]

2.2.1.4. Benefits of a Purposive Approach

Many believe that conceptualizing privacy as "control over personal information" can be too vague, too broad, or too narrow.[987] DPLs can have an over-reaching effect, an

---

[983] The significant feature of this approach is that it is based on *how information is used* ("total context"), and not *where it is produced* (a "work product" approach). Although not identical, this approach is more in line with the totality of circumstances test developed by the Supreme Court of Canada in connection with the criminal law and, in particular, to delineate the circumstances in which an individual can claim a reasonable expectation of privacy. See, for example, *Tessling*, supra note 107.

[984] OPCC, *supra* note 135.

[985] See section 2.2.1.1 which elaborates on this issue.

[986] Information Commissioner's Office, *Data Protection Strategy, Consultation Draft*, U.K., June 2007, at 5 [ICO, *Data Protection Strategy*].

[987] See section 2.1.1 entitled "Deconstructing the Concept of Privacy as Control" which elaborates on this issue.

under-reaching effect and create various uncertainties as to which kind of data qualifies as *personal*.[988]

At the time that the FIPs were initially elaborated in the early 1970s, their main purpose was to address specific concerns pertaining to computerized databases. The best way to deal with these data protection issues was deemed to be individuals in control of their information.[989] Forty years later, that selfsame concept is still one of the most predominant theories of privacy and the basis for DPLs around the world.[990] While many issues with this theory still remain,[991] a new approach in interpreting the notion of *personal information* may go a long way in dispelling them. This new approach is necessary in order for DPLs to be and remain effective in the future.

The ultimate purpose of DPLs is to protect individuals against the *risk of harm* that may result from the collection, use or disclosure of their information.[992] Likewise, with the proposed approach only data that may present a *risk of harm* to individuals would be protected. The Committee on Privacy in the Information Age of the National Research Council states:

> "While we can reasonably (be) sure that privacy is a matter of individual's control over information about themselves, it is less clear whether the emphasis should be on control over the gathering of that information, the access to that information after it has been gathered, the use of information that has been gathered, or on all equally".[993]

---

[988] See section 2.1.2.2 which elaborates on this issue.

[989] See section 1.1.2 entitled "Control over Personal Information and Fair Information Practices" which elaborates on this issue. See also Council of Europe, *Report on data processing*, *supra* note 66 at 5, s. II, s. 3: "Although the idea of privacy is very difficult to define, it is possible to tell when and how it may be infringed by the computerised use of personal data. The present technical trend is towards the spread of small computers storing small quantities of data, but which may be connected with each other and with a central computer, thus forming a network in which all sorts of information circulate. From this point of view, control is necessary not only over the information stored, but also over its use and the means by which it is obtained, i.e. data processing control."

[990] See section 1.1.2.2 which elaborates on this issue. See also Solove, "Conceptualizing", *supra* note 23 at 1109.

[991] See section 2.1 entitled "Deconstructing the Definition of Personal Information" which elaborates on this issue.

[992] See section 2.2.2 "Determining Risk of Harm as Purpose Behind the Protection of Personal Information" which elaborates on this issue.

[993] Waldo, Lin & Millet, *supra* note 6 at 69.

I argue in section 3 that in certain cases, the *harm* will take place at the point of *collection* while in other cases, at the point where the data will be *used* or even *disclosed*. The *risk of harm* approach applied to the definition will take this into account, and protect data only at the time that it presents such risk or in light of the importance or extent of such risk or harm.

This section will discuss how a purposive approach will provide for a more optimal protection, in the sense that data presenting no such risk of harm will flow freely. Therefore, for those entities that handle data presenting no palpable risk, many needless undertakings will be averted and no undue financial burden will be imposed.[994] Another benefit with the purposive approach will be the elaboration of a badly needed flexible framework in the context of modern data protection issues; which is the best way to address both over-reaching and under-reaching outcomes of DPLs. It may also provide for a guide when there is uncertainty surrounding the qualification of certain information,[995] or when there are provisions in DPLs providing for some type of subjectivity.[996] Lastly, this approach may limit some of the disclosure and consents, in the sense that only data which may be harmful to individuals will be in fact covered by DPLs. This may translate in less "consents" to be obtained, or at least in a framework under which consents which are obtained are necessary in the sense that they are required for the collection, use or disclosure of information which may trigger a *risk of harm* for individuals (data which were meant to be protected by DPLs).

2.2.1.4.1. Providing More Flexibility ("Privacy" and "Harm" are Contextual)

The conception of privacy as "control over personal information" which is the hard core of the current DPLs, would not be flexible enough to handle the challenges of today according to many.[997] By applying a purposive interpretation to the notion of *personal*

---

[994] For example, the approach proposed may enable the various commercial entities (websites, search engines, ISPs, etc.), which collect, use and disclose these data to have to obtain consent prior to collecting, or using the data only if such data can trigger a *risk of harm* to the individual. They will have to dedicate the resources to protect the information against a security breach in light of the risk of harm that such disclosure of data may trigger.

[995] See section 2.1.2.2 which elaborates on this issue.

[996] See section 2.2.1.3.2(a) entitled "DPLs Already Subjective on Various Issues" and section 2.2.1.4.4(a) "Guide In Cases of Uncertainty with Certain Data" which elaborate on this issue.

[997] See section 2.1.1 entitled "Deconstructing the Concept of Privacy as Control" which elaborates on this issue. See also the OECD has mentioned in 2008 that it is undertaking an assessment of its 1980 Privacy Guidelines in light of these changing technologies, markets and user behaviour such as the ones detailed in section 1.2 entitled "Technological Background Affecting Personal Information". See, OECD, *The Seoul*

information, this concept of privacy as "control over personal information", and the principles of FIPs*, which* are incorporated in DPLs, may be shown to provide for a much more flexible and effective framework to address modern data protection issues than we in fact realize.

Section 1.2 details the recent changes which have emerged at the technological level, which include an increase in the volume of data available, the emergence of new types of data and collection tools, new methods for identifying individuals and new uses for this data. In this context, Reidenberg and Schwartz state that: "The ability of information technology to combine and share data makes impossible any abstract, noncontextual evaluation of the impact of disclosing a given piece of personal information."[998] Industry players such as Microsoft believe that a greater focus on substantive outcomes, rather than prescriptive requirements, may be desirable to address challenges arising from these changes:

> "A more nuanced, or context-based approach to application of some of the Directive's provisions might also strengthen data protection. Both data subjects and data controllers might benefit from the application of greater or lesser protections to personal data depending on the context in which such data are used."[999]

Personal information can be more or less sensitive (in terms of being potentially harmful to individuals), depending on the context and the current definition of *personal information* may in a way ignore this. For example, an individual's name appearing on a company Intranet page has less privacy implications than the same name appearing on a "black list" related to credit ratings.[1000] In the context of consumer privacy, the sale

---

Declaration for the Future of the Internet Economy (OECD, 2008), online: <http://www.oecd.org/dataoecd/49/28/40839436.pdf>; Rand corporation believes that in the online world, it is difficult to establish exactly how information collected is being used or to set up any comprehensive means for individuals to exercise management or control of the uses of such data. See: Robinson et al., *supra* note 151 at 4 and see also at 7: "However, it is also important to realise that the Directive was written at a time when data processing involved filing systems and computer mainframes. The risks related to such a model could easily be managed by defining obligations and procedures linked to each role. Its main objective was to harmonise existing regulations to safeguard the data subject's right to informational privacy and to create a common European market for the free movement of personal data, not to create a legal framework that could cope with future data processing and privacy challenges"; Daniel Solove takes the position privacy law has fixed itself too firmly to certain conceptions of privacy, and as a result, has lost flexibility in dealing with emerging privacy problems. See: Solove, "Conceptualizing", *supra* note 23 at 1093.

[998] Reidenberg & Schwartz, *supra* note 203 at 9.

[999] Microsoft Corporation, *supra* note 358 at 2.

[1000] *Ibid*. at 5-6.

of one's entire consumer history (including information of "intimate" nature) would be fundamentally more harmful then a telemarketing call based on records of a newspaper subscription. DPLs may not necessarily make a distinction in light of the sensitivity of data handling activities and put all of the personal information at the same level, or simply list categories of "sensitive" information without taking into account the context of their availability.[1001]

In order to provide for better outcomes, certain European Member States have introduced DPLs providing for context-based protections for personal data. Austria, for instance, has adopted an approach where coded data is subject to less protections when processed by an entity that does not have the key to the code.[1002] Microsoft argues that this type of context-based approach could strengthen user protections, while also ensuring that data controllers allocate resources to the situations where protections are most needed.[1003] Google is welcoming the principle of "harm" in the context of enforcing data protection rules in the Information Age as it would provide for the much needed flexibility in the context of the Internet and related technologies.[1004] Google states:

> "Sure, identity theft and spam are bad. But is targeted advertising harmful or beneficial for consumers? What about the use of cookies to remember consumers' preferences or computer settings? Do they make life easier or are they a harmful consequence of our online activities?"[1005]

[1001] This is the case for Canadian DPLs, since Directive 95/46/EC and the French DPL have a list of "sensitive" information. See section 2.1.2.3.2 entitled "Pre-determined Categories of Sensitivite Data Challenged" which elaborates on this issue.

[1002] Microsoft Corporation, *supra* note 358 at 6.

[1003] *Ibid*. at 5-6.

[1004] See: Fleischer, "IP addresses", *supra* note 610; see also Peter Fleischer, "Global privacy standards should focus on preventing harm to consumers" (14 November 2007), online: The Official Google Blog <http://googlepublicpolicy.blogspot.com/2007/11/global-privacy-standards-should-focus.html>: "Others see the APEC framework as the weakest international framework in this area and support the original OECD Privacy Guidelines because they are based on a simple approach to privacy protection. But is this approach a valid one to address the challenges of the Internet age? In today's world, virtually every organization – public or private, large or small, offline or online – relies on the collection and use of personal information for core operational purposes (…) What is wrong then with looking at this very practical challenge in a practical manner and trying to prioritise what really matters to people in an objective, yet flexible, way?"

[1005] *Ibid*.

Solove has stated: "In a world constantly being transformed by technology, how can we erect a robust and effective law of privacy when the ground is constantly shifting?"[1006] In my view, if we are to work with DPLs, the best means of enhancing their legal flexibility, in a context of ongoing technological change, is to adopt a purposive approach to interpretation. This view is shared by many authors, including Bennett Moses:

> "Both common law and statutory rules can be interpreted either rigidly or flexibly, with varying degrees of weight given to their underlying purposes. A judge applying a rule rigidly will enforce the rule without considering whether such application is in line with the rule's purposes, whereas a flexible judge will seek to preserve the rule's intended effect in spite of its wording. A judge adopting a purposive approach in dealing with cases involving new technologies is more likely to reach the result that would have been reached at the time of the rule's creation had the future been foreseen".[1007]

A purposive interpretation of *personal information* will enable the protection of certain data that should be protected while avoiding needless protection of other data. But it may also provide for some type of flexibility, which may be welcome in the Informative Age, especially when attempting to determine whether a certain activity or a certain piece of data should be governed by a DPL.

2.2.1.4.2. Ensuring that the Law is Technology Neutral

DPLs were initially elaborated in order to address the management and handling of personal information which was in electronic form. The Article 29 Working Party states:

> "It is useful to recall that the reasons for enacting the first DPL in the seventies stemmed from the fact that new technology in the form of electronic data processing allows easier and more widespread access to personal data than the traditional forms of data handling."[1008]

[1006] Solove, "Conceptualizing", *supra* note 23 at 1089-90.

[1007] Bennett Moses, *supra* note 552 at 72 [footnotes omitted] Lyria Moses suggests that Judges, as interpreters of common law rules, statutory rules and administrative regulations, have an important role to play in ensuring that the legal system adapts well to technological change. This avoids some of the targeting problems encountered with a more textual approach and provides guidance where laws are uncertain. See *ibid*. at 71. See also *generally* Arthur Cockfield, "Towards a Theory of Law and Technology" (2004) 30 Manitoba L.J. 383.

[1008] Article 29 Data Protection Working Party, *Opinion 4/2007*, *supra* note 100 at 5.

The initial concern was that individuals were going to lose control over their personal information since their data, once in electronic form, would become more easily shared among organizations from the private and public sectors, without the individual's knowledge.[1009] In fact, DPLs were initially only meant to apply to electronic data and this distinction (electronic data vs. non electronic data) is still present in certain DPLs.[1010] For instance, Directive 95/46/EC makes a distinction between the processing of personal data by automatic means and the processing of personal data by non-automatic means.[1011]

In light of this original distinction (information in paper vs. electronic format) one can reasonably argue that the FIPs (and DPLs incorporating theses FIPs) may not be technology neutral. This distinction (paper vs. electronic) may have made sense forty years ago when data was passing from the "paper" form to an "electronic" one and was therefore to be shared more easily. But we are now facing a new reality with all of the changes that have recently taken place at the technological level.[1012]

In various DPLs, this distinction is no longer present and we can even note that certain DPLs have provisions for technology neutral application. For example, in Canada, PIPEDA states that "organizations shall protect personal information regardless of the format in which it is held",[1013] and the Quebec DPL, that "The Act applies to such information whatever the nature of its medium and whatever the form in which it is accessible, whether written, graphic, taped, filmed, computerized, or other."[1014] In Canada, PIPEDA is based on flexible principles rather than prescriptive rules. According to some (including Canadian privacy expert David Fraser), this translates

[1009] See section 1.1.2.1 entitled "Initial Concern: Computers and Electronic Data Banks" which elaborates on this issue.

[1010] See section 1.1.2.1.2 entitled "Electronic Databanks becomes All Databanks" which elaborates on this issue.

[1011] EC, *Directive 95/46/EC*, *supra* note 99 at Whereas (27); See also Article 29 Data Protection Working Party, *Opinion 4/2007*, *supra* note 100 at 5.

[1012] See section 1.2 entitled "Technological Background Affecting Personal Information" which elaborates on this issue.

[1013] PIPEDA, *supra* note 63 at Schedule 1 (s. 5), principle 4.7.1.

[1014] Quebec DPL, *supra* note 110 at s. 1.

into a piece of legislation being able to accommodate various industries and new technologies, and it would therefore be a technology neutral legislation.[1015]

A first goal and benefit to using such a purposive interpretation in the evaluation of *personal information* would be to ensure that DPLs are technology neutral as much as possible.[1016] Koops suggests that regulation should be technology neutral in its effects.[1017] I believe that if we use a literal approach of interpretation of the notion of *personal information*, DPLs may not be technology-neutral since this can trigger a situation in which it is not always clear whether certain types of data are in fact covered by DPLs.[1018] Certain types of data (such as names, addresses, telephone numbers, medical information) may more easily qualify as *personal information* (and therefore will be automatically governed by DPLs) while other new types of data (IP addresses, *clickstream* data, profiles, search engine searches, etc.) may not. We may end up having certain types covered by DPLs as they automatically qualify as *personal information*, while other types that may create a similar *risk of harm* to individuals will not be covered, simply because they don't fall within the strict literal interpretation of the notion of *personal information*.

For example, a man may search online about being depressed and about cures to depression. Using a literal interpretation of the notion of *personal information*, these online searches may not qualify as *personal information* if they are not directly linked with the name of an individual or some other clear identifier. Marketers may therefore take the position that they can use this data for marketing purposes on the Internet. But this search data may create a *risk of harm* to this man if the next time that he logs on to the Internet, he receives advertisements about therapists, which are experts in dealing

---

[1015] See David Fraser, "Privacy Commissioner consultations on new technologies: a few thoughts" (12 February 2010), online: Canadian Privacy Law Blog <http://blog.privacylawyer.ca/2010/02/privacy-commissioner-consultations-on.html>: "PIPEDA, for all its weirdness as a statute, is in my view surprisingly resilient. It is because it is based on flexible principles rather than prescriptive rules that it can accommodate various industries and new technologies. The defects that were there on day one are generally still there, but its technological neutrality was well drafted and has withstood the test of time."

[1016] According to Vincent Gautrais, it would be in many cases impossible to have perfect technology neutrality. See Gautrais, *Neutralité technologique*, *supra* note 826.

[1017] Koops, *supra* note 821 at 6.

[1018] See section 2.1.2.2.2(a) entitled "Dealing With New Types of Data" which elaborates on this issue.

with depression symptoms or worse, that such advertisements are made to his colleague with who he shares a computer at work.[1019]

Koops also argues that "the more detailed the legislation, the less transparent it may be and, particularly with technology, it will be the case that the more technology is put into the law or into its formulation, the less understandable it will be to ordinary citizens."[1020] If we can find a way to work with the current definition of *personal information*, which I believe we can with the proposed purposive approach, then we should move forward with this approach. This is a better option than proposing to redraft the definition into more complicated terms. The traditional understanding of DPLs is that they exist to protect individuals by making sure that their personal information will not be collected, used or disclosed to harm them in some way or without their knowledge.

Bennett Moses suggests that the only way to guarantee technology-neutrality, in the sense that new technologies will be treated fairly, is to enact a law with a level of generality consistent with the highest level goal that the lawmakers wish to achieve.[1021] For example, high level goals such as *preserving human life* or *improving economic efficiency* would be relatively immune to successive waves of technological change.[1022] The idea is to address the challenges brought on by the application of DPLs in the context of new technologies and the Information Age with a new interpretation, one that is in line with the DPLs' ultimate goal.

DPLs regulate the actions of collecting, using and disclosing personal information. Koops suggests that instead of regulating the means (the action itself), we should be regulating functions and effects. Furthermore, regulation should be focused on the effects of actions.[1023] He articulates the view that "of particular importance is exactly

---

[1019] If this man's colleague only shares the computer with him, has no interest for the topic of depression and suddenly receives this kind of advertisment about depression on many websites that he visits, he could easily make the assumption that his colleague probably is depressed and has made online searches regarding this topic with the computer that they share at work. See section 3.1.2.1.2(a) entitled "Fear of a Disclosure or that Information Disclosed will be Used" which elaborates on this kind of harm.

[1020] Koops, *supra* note 821 at 12.

[1021] Bennett Moses, *supra* note 552 at 62.

[1022] *Ibid*. at 66.

[1023] Koops, *supra* note 821 at 6.

what effects must be regulated." [1024] DPLs were meant to protect individuals against the *risk of harm* to individuals that data handling activities could trigger.[1025] By increasing the flexibility and hence the effectiveness of DPLs, a purposive interpretation of *personal information* would allow DPLs to stay true to their initial *raison d'être*.

2.2.1.4.3. Ensuring that the Law has Appropriate Effects

Another benefit of the purposive interpretation in the evaluation of *personal information* would be to ensure that DPLs have appropriate effects and outcomes. A broad definition of *personal information* coupled with a literal interpretation may lead to situations where DPLs are applied in an over-reaching or under-reaching way. Using a purposive approach to interpreting *personal information*, we may be reducing this additional unwanted outcome (over or under-reaching) in the application of DPLs.

(a) Avoid Over-Inclusive Outcome of DPLs

As discussed in section 2.1.2.1.1, privacy as "control over personal information" is a concept that can be over-reaching, and the very broad definition of *personal information* may be a primary contributing factor. Canadian and French DPLs (including Directive 95/46/EC) define *personal information* in a potentially broad manner. The undesirable aspects of the over-reaching interpretation of this notion are further discussed in section 2.1.2.1.1(d).

Section 1.2.3 has already discussed the fact that with the greater volume of available personal information and new technologies (which may converge) and new data-mining and matching techniques available, every piece of information can conceivably be linked to an identifiable individual. Bercic and George agree that DPLs are over-reaching, probably due to the very broad notion of *personal information*:

[1024] *Ibid*. For instance, as suggested by Koops, in the case of regulating unsolicited commercial communications (also known as spam), an obvious aim may be to protect people from being bothered by messages they did not request nor wished to receive. But the extent of bother can vary for different technologies: telephone "spamming" is physically distracting because it makes a noise, and facsimile "spamming" is intrusive because it requires paper and machine time and thus costs money, whereas email spamming does not distract physically nor does it cost as much as a fax. For that reason, legislatures have enacted different laws for commercial communications through different communications media, apparently considering that the effects of the technologies differ.

[1025] See section 2.2.2.2 entitled "Evidence that Ultimate Purpose of DPLs: Avoid the Risk of Harm" which elaborates on this issue.

> "Because it is possible to interpret almost any data as personal data (any data can in one way or another be related to some individual) the question arises as to how such data should be treated. The answer to this question is important both because of the above mentioned rights of individuals with respect to the processing of personal data relating to them under the Directive and because of the processors' duty to ensure the confidentiality and security of processing of all personal (but not other kinds of) data."[1026]

Ohm proposes that we abandon the problematic notion of *personal information* and that regulators should seek "to prevent privacy harm by squeezing and reducing the flow of information in society, even though in doing so they may need to sacrifice, at least a little, important counter values like innovation, free speech, and security."[1027] Schwartz and Solove rightfully disagree with this approach and maintain that: "Yet, an approach where the first step is to restrict the flow of information is a move in the wrong direction".[1028]

Mindful of the over-reaching nature of DPLs, certain industry experts have proposed to refocus the definition on data which is of a private nature. RAND Corporation suggested that one of the crucial characteristics of Directive 95/46/EC is that it is tied to the concept of "personal data", and not to a notion of privacy.[1029] This translates into the provisions of Directive 95/46/EC applying to acts of data processing that are not considered to be privacy sensitive in their own right. Trudel and Benyekhlef suggest that in the context of the Internet, only information which is truly of a private nature should be protected by law.[1030] Solove takes issue with conceptualizing privacy as "control of information" as he believes the conception to be too broad.[1031] He suggests

---

[1026] Bercic & George, *supra* note 574 at 248.

[1027] Ohm, *supra* note 562 at 1704.

[1028] Schwartz & Solove, *supra* note 529 at 1868. See also section 1.2.4.1 entitled "New Business Models (Customization and Sponsored Services)" details how personal and/or new types of data – which may qualify as personal information – are useful to new business models. See section 2.1.1.1.1 entitled "Ignoring the Importance of Information Flow For the Society" which details how, in some cases, the free flow of information may be beneficial to the society at large.

[1029] Robinson et al., *supra* note 151 at 7.

[1030] Trudel & Benyekhlef, *supra* note 367 at 1.

[1031] Solove, "Conceptualizing", *supra* note 23 at 1114.

that one possibility is that the "control" conception of privacy be limited in scope by including only intimate information.[1032]

The ultimate objective of DPLs is in fact broader than only protecting the privacy of individuals.[1033] In fact, the ultimate goal is to protect the individual against the *risk of harm*, part of which harm may include privacy-related harm which is more subjective in nature.[1034] Certain jurisdictions have proposed only enforcing DPLs when a data handling activity creates a *risk of harm*. This has been recently the case in the U.K. where the Information Commissioner's Office has articulated the view that it needed to focus particular attention on situations "where there is a real likelihood of serious harm."[1035] Implementing a purposive approach would go a long way in ensuring that only data that present a tangible *risk of harm* are governed by DPLs.

(b) Avoid Under-Inclusive Outcome of DPLs

In this section, I will first address the importance of the right to privacy. Then, I will discuss how the proposed framework will address the fact that the notion of "identifiable" is obsolete in certain situations.

(i) Protecting Privacy is Important

Privacy is no doubt essential for individuals as well as for society in general.[1036] Protecting privacy has always been seen as an important, sometimes even as a fundamental right.[1037] Personal information would be a key factor in interpersonal

---

[1032] Although he is still concerned that it would still be too broad of a conception. See *ibid*.

[1033] See section 2.2.2.1.2 entitled "Data Protection is Broader than Privacy" which elaborates on this issue.

[1034] See section 2.2.2.2 entitled "Evidence that Ultimate Purpose of DPLs: Avoid the Risk of Harm" which elaborates on this issue.

[1035] ICO, *Data Protection Strategy*, *supra* note 986 at 5: "Being a strategic regulator means that, in so far as we have a choice, we have to be selective with our interventions. We will therefore apply our limited resources in ways that deliver the maximum return in terms of a sustained reduction in data protection risk. That is the risk of harm through improper use of personal information. There are priorities we have to set. We need to focus most attention on situations where there is a real likelihood of serious harm."

[1036] Jeroen Van Den Hoven & Pieter E. Vermaas, "Nano-Technology and Privacy: On Continuous Surveillance Outside the Panopticon" (2007) 32:3 Journal of Medicine and Philosophy 283 at 284-85, online: <http://dx.doi.org/10.1080/03605310701397040>: "Laws, policies, and regulations to protect the personal sphere and the privacy of persons have been formulated and implemented in the last 100 years around the world, but not without debate and controversy. (…) Different authors have presented different accounts of privacy, but the majority of them agree that privacy is important in human lives."

[1037] Waldo, Lin & Millet, *supra* note 6 at 12: "privacy would be an important value to be maintained and protected, because the loss of privacy would often result in significant tangible and intangible harm to individuals and groups". See also Westin, *Privacy and Freedom*, *supra* note 45 at 7.

relationships and, as Charles Fried argues, controlling access to personal information is a necessary precondition for friendship, intimacy, and trust.[1038]

Privacy is also indispensable for the protection of other rights, including freedom of speech and freedom of association.[1039] These rights would be considerably curtailed or limited if individuals felt they were under surveillance at all times.[1040] The freedom to practice religion, for instance, requires that individuals have a suitable personal sphere in which they can develop their convictions.[1041] These rights may also include the freedom and the right to have access to information that individuals may be interested in (even if this information may be personal to other individuals).

The continuous or excessive collection of personal information can be seen as the modification of the individual's behavior (self-censorship, free choice).[1042] Calo suggests that it is harmful for individuals to be under constant observation: "Episodic solitude—in essence, the periodic absence of the perception of observation—is a

---

[1038] Fried, "Privacy", *supra* note 79 at 484; See also Charles Fried, *An Anatomy of Values: Problems of Personal and Social Choice* (Cambridge: Harvard University Press, 1970).

[1039] Joel Feinberg, *Freedom and Fulfilment: Philosophical Essays* (Princeton: Princeton University Press, 1994) at 248.

[1040] U.S. Department of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *supra* note 57 at s. III: "As a social value, furthermore, privacy can easily collide with others, most notably free speech"; See also Conseil de l'Europe, *L'autodétermination informationnelle*, *supra* note 20 at 26: "Ainsi, pour parler de la liberté d'expression et d'association, comment imaginer que celles-ci puissent survivre si la personne se sait surveiller dans ces communications et ne puisse à certains moments s'exprimer anonymement si la technologie garde systématiquement trace de mes messages."

[1041] Feinberg, *supra* note 1039 at 248.

[1042] The monitoring of individuals or the knowledge that data is excessively being collected about them can cause people to modify their behavior since they know that they are (or may be) watched. Charles Fried notes that, were our every action public, we might limit what we think and say. See Fried, "Privacy", *supra* note 79 at 483-84. David Flaherty states: "The existence of dossiers containing personal information collected over a long period of time can have a limiting effect on behavior; knowing that participation in an ordinary political activity may lead to surveillance can have a chilling effect on the conduct of a particular individual." See David H. Flaherty, Protecting privacy in surveillance societies: the Federal Republic of Germany, Sweden, France, Canada, and the United States (Chapel Hill: University of North Carolina Press, 1989). Solove suggests, for instance, that public surveillance can have a "chilling effects" kind of harm that make people less likely to associate with certain groups, attend rallies, or speak at meetings or criticize popular views. Solove, "A taxonomy", *supra* note 339 at 498-99. See also *ibid*. at 493-94: "direct awareness of surveillance make a person feel extremely uncomfortable, but it can also cause that person to alter her behavior". Kang, *supra* note 734 at 1260: "Simply put, surveillance leads to selfcensorship."; Peter P. Swire, "Financial Privacy and the Theory of High-Tech Government Surveillance" (1999) 77 Wash. U. L.Q. 461 at 473 : "If I know I am under surveillance, I might (…) restrict my activities, so that nothing embarrassing or otherwise harmful could be detected."; See also Pomerance, *supra* note 233 at 293: "The ability to move about freely without constant supervision by the government is an important source of individual liberty that must be addressed. A fear of systematic observation, even in public places, destroys this sense of freedom."

crucial aspect of daily life. People need solitude for comfort, curiosity, self-development, even mental health."[1043]

The right to privacy is especially relevant on the web, a virtual space in which anonymity allows individuals to exercise the aforementioned rights more freely; be it by creating an online *alter ego* or by anonymously publishing information.[1044] According to the U.K. Information Commissioner's Office, improper use of personal information could equate to excessive intrusion into the private lives of citizens, threatening personal autonomy and dignity.[1045] Without adequate privacy safeguards, a climate of fear and suspicion could take hold on the masses.

George Radwanski, a former Canadian privacy commissioner, has articulated the view that *privacy* means *freedom*:

> "Without privacy, there is no real freedom. In fact, many have suggested that privacy is the right from which all others flow – freedom of speech, freedom of association, freedom of choice, any freedom you can name. That's why privacy is recognized as a fundamental human right in the United Nations Declaration of Human Rights. And it's why lack of real privacy is a distinguishing characteristic of so many totalitarian societies."[1046]

Privacy protection is therefore not only essential as a safeguard for personal wellbeing, but also to ensure the needed freedom and creativity that may benefit society as a whole.[1047] The proponents of strong privacy protections point out the importance not only of individual but also of collective privacy as well. Robert Post contends that the

---

[1043] Calo, "The Boundaries", *supra* note 443 at 18. See also Lior Strahilevitz, "Reputation Nation: Law in an Era of Ubiquitous Personal Information" (2008) 102 N.W. U. L. Rev. 1667 at 1736: "Privacy theorists have long argued that protecting privacy is essential so that individuals can relax, experiment with different personalities to figure out who they truly are, or develop the insights that will make them better citizens."; Julie Cohen, "Cyberspace as/and Space" (2007) 107 Colum. L. Rev. 210; Paul Schwartz, "Internet Privacy and the State" (2000) 32 Conn. L. Rev. 815; Cohen, "Examined Lives", *supra* note 459; Schwartz, *Cyberspace*, *supra* note 355 at 1640-41; Barrington Moore, *Privacy: Studies in social and cultural history* (Armonk, N.Y.: M.E. Sharpe, 1984) at 73. As Alan Westin argues: privacy allows for "respite from the emotional stimulus of daily life. (…) To be 'always on' would destroy the human organism". Westin, *Privacy and Freedom*, *supra* note 45 at 35.

[1044] Sonia Katyal, "The New Surveillance" (2004) 54:2 Case Western Law Review 297 at 316: "Yet today, the perception of informational privacy extends, at least in cyberspace, to something quite different: It covers the very act of creating fictive personalities, in addition to the possibility of anonymously publishing information online."

[1045] ICO, *Data Protection Strategy*, *supra* note 986 at 8.

[1046] Radwanski, *supra* note 28 at 5.

[1047] Robinson et al., *supra* note 151 at 16.

tort of invasion of privacy "safeguards rules of civility (…) both [for] individuals and [the] community."[1048] Cohen and Schwartz both argue that privacy is a constitutive element of civil society.[1049] With regards to medical information, interesting insights have been proposed by Janlori Goldman. With a more robust protection of medical information, Goldman posits, people would be more willing to seek medical care and agree to participate in medical research; this would have a positive impact on public health as well as social welfare. Furthermore, Renée M. Pomerance articulates the view that privacy is a cherished right in our modern society:

> "(…) Privacy is the oxygen that allows the self to breathe and develop. It is the medium in which individual personality flourishes. Any society that values individualism and diversity must, by necessity, treasure the right to privacy. It could be argued that virtually every rule that has developed about privacy is fundamentally concerned with the inviolability of the self – this is what constitutional instruments seek to shield from the prying eyes of the state."[1050]

On top of these concerns, the monitoring of individuals (or an excessive collection of their information) may also enable the organizations collecting the data to better control individuals.[1051] For instance, pervasive individual monitoring would be a key component in abusive control.[1052] While every society must exercise a sizeable degree of social

---

[1048] Robert C. Post, "The Social Foundations of Privacy: Community and Self in the Common Law Tort" (1989) 77 Cal. L. Rev. 957 at 959.

[1049] Cohen, "Examined Lives", *supra* note 459 at 1427-28: "Informational privacy, in short, is a constitutive element of a civil society in the broadest sense of the term."; Schwartz, *Cyberspace*, *supra* note 355 at 1613 : "[I]nformation privacy is best conceived of as a constitutive element of civil society."; See also Ruth Gavison, "Privacy and the Limits of Law" (1980) 89 Yale L.J. 421 at 455: "Privacy is also essential to democratic government because it fosters and encourages the moral autonomy of the citizen, a central requirement of a democracy."

[1050] Pomerance, *supra* note 233 at 281.

[1051] Paul M. Schwartz, "Privacy and Participation: Personal Information and Public Sector Regulation in the United States" (1995) 80:3 Iowa L. Rev. 553 at 560: "data processing creates a potential for suppressing a capacity for free choice. The more that is known about an individual, the easier it is to force his obedience"; John Gilliom, *Overseers of the poor: surveillance, resistance, and the limits of privacy* (Chicago: University of Chicago Press, 2001) at 3: "Surveillance of human behavior is in place to control human behavior, whether by limiting access to programs or institutions, monitoring and affecting behaviour within those arenas, or otherwise enforcing rules and norms by observing and recording acts of compliance and deviance."; Greene, *supra* note 328: "As Schneier sees it, the problem is one of balancing control over data to maximize individuals' liberty. If individuals control data about themselves, that gives them liberty. If their information is controlled by the government, they lose liberty and power, he says. 'If you give an individual privacy, he gets more power,' Schneier says. Similarly, if government is forced to work in the open and its information is public, that gives the people power over the government. Government secrecy shifts the power balance to government."

[1052] Calo suggests that repeated "checking in" throughout the day is thought to be an early sign of domestic abuse and there is evidence that the "learned helpless" experienced by some abuse victims

control (for example, surveillance can serve as a deterrent to crime) imbalances in power can also be risk enhancing and help spawn abuses in power.[1053]

(ii) Protecting Harmful but Non Identifying Data is Important

As already discussed in section 2.1.2.1.2, privacy as "control over personal information" is a concept that can be under-reaching. This is often the case with new types of data or profiles, which may end up not being covered by the definition of *personal information* of DPLs if using a strict literal interpretation, while there may be certain privacy concerns and potentially a *risk of harm* surrounding the collection, use and disclosure of this information.

The purposive interpretation proposed in this thesis may be useful in order to ensure that DPLs are governing the data that they should, including new types of data or profiles, if the collection, use or disclosure of this data creates a *risk of harm to* the individuals (even if the individual is not identifiable by name).

Section 1.2.3 discusses the creation of profiles which can also create concerns. This is because in the case of a profile, while every piece of information creating the profile taken in isolation may not qualify as *personal information*, once aggregated, they may end up identifying an individual. While a strict literal interpretation could mean evaluating data piece by piece without looking at the whole picture, a purposive approach would instead focus on the intent of the law (DPLs). Using this approach, a given profile would in fact be governed by the relevant DPL, if the use or disclosure of this profile data creates a *risk of harm* to individuals.

The notion of "identity" may be obsolete in certain cases, at least when a certain profile, which cannot identify a specific individual, may nonetheless be used to qualify or categorise an individual triggering some type of objective harm for this individuals.[1054] The proposed purposive interpretation will therefore also be useful in

---

stems in part from having internalized the feeling of being monitored. See Calo, "The Boundaries", *supra* note 443 at 16-17.

[1053] Solove, "Privacy", *supra* note 1, at 1415: "by constantly living under the reality that one could be observed at any time, people assimilate the effects of surveillance into themselves. They obey not because they are monitored but because of their fear that they could be watched. This fear alone is sufficient to achieve control."

[1054] See section 3.2 and more specifically, section 2.1.2.3.1 entitled "Notion of Identity Obsolete in Certain Situations" which elaborate on this issue.

order to ensure that a certain profile is governed by the relevant DPL, for instance, if it is used to take a decision about an individual possibly leading to some type of negative impact (regardless of the fact that the organization doesn't not know the identity behind the said profile). Section 3.2.2.1 further discusses this issue.

2.2.1.4.4. Provides a Guide

The purposive interpretation proposed may provide for a guide to determine whether certain information is covered under the notion of *personal information*, addressing the potential uncertainty as to which data qualifies as *personal information*. The present section will also demonstrate how this approach will be useful when DPLs provide for subjective assessments to be made by organizations handling personal information.

(a) Guide In Cases of Uncertainty with Certain Data or Obsolete Situations

The issue as to what constitutes *personal information* is not trivial as it is at the very heart of DPLs. When certain data qualifies as *personal information*, all kinds of obligations are triggered on the part of the organizations handling the data (i.e. consent, protection of information, etc.). Personal information also entails certain rights on the part of individuals (i.e. right to access this information and to request that it be updated or amended, etc.). In Europe, a very important legal question (that of what constitutes a personal data filing system) also depends on the question of what constitutes *personal data*. [1055]

I discuss in section 2.1.2.1.1(a) entitled "Definition Meant to be Broad" how the purpose of adopting a very broad yet flexible definition of *personal information* was initially to ensure that the law would keep up with technological developments. But section 2.1.2.2 details how the current broad definition of *personal information* creates various uncertainties as to which data is in fact covered by DPLs, especially with new types of data. More specifically, it is not always clear if a certain piece of data relating to a device which may be used by one or more individuals qualifies as *personal*

[1055] Bercic & George, *supra* note 574 at 236.

information.[1056] The resources of work required to determine whether a certain piece of data can "identify" and individual are also not clear.[1057]

As discussed in section 2.1.2.2.2, although documents, findings, rulings or press releases from the authorities in charge of data protection or courts have been issued which may provide for some type of general guidance as to how to interpret this notion, the approaches used from different jurisdictions or even by different courts within the same jurisdiction are often different or even contradictory. Therefore, a guide providing for a more uniform approach of interpreting *personal information* will be useful.

A purposive approach will provide guidance when evaluating a certain piece of data and determining which kinds of data should be governed by DPLs. Using this purposive interpretation, if the data collected, used or disclosed creates a *risk of harm* following the test proposed in section 3 of this thesis, then it will be covered by the DPL in question. More specifically, the issues that have been raised in sections 2.1.2.2 and 2.1.2.3 can be addressed using the *risk of harm* approach. For instance, this approach would be useful in making sure that new types of data and unique identifiers linked to people or objects, and not just basic biographical data, are covered if they present a *risk of harm* to individuals.[1058] The following hypothetical situations illustrate this application of the purposive approach: in making sure that two pieces data which, once correlated, present a *risk of harm* once used or disclosed will be covered,[1059] in providing guidance in order to set guidelines assessing the sensitivity of certain data[1060] and in order to make sure that certain data, although they may not "identify" an individual, may still be considered as *personal information* in the presence of an objective *harm* to the individual.[1061]

[1056] See section 2.1.2.2.2(b) entitled "Device Used by a Group: At What Point is it Identifiable?" which elaborates on this issue.

[1057] See section 2.1.2.2.1 entitled "Notion of Identifiable Individual" and more specifically section 2.1.2.2.1(b) entitled "At what costs and using what kind of efforts?" which elaborate on this issue.

[1058] See section 2.1.2.2.2 entitled "Identifying a Device or an Object" which elaborates on this issue.

[1059] See section 1.2.3.1 entitled "Aggregation and Correlation of Data" and section 2.1.2.1.1(b) entitled "Correlation Required to Identify an Individual" which elaborate on this issue.

[1060] See section 2.1.2.3.2 entitled "Pre-determined Categories of Sensitivite Data Challenged" which elaborates on this issue.

[1061] See section 2.1.2.3.1 entitled "Notion of Identity Obsolete in Certain Situations", section 2.2.1.4.3(b)(ii) entitled "Protecting Harmful but Non Identifying " and section 3.2.2.1 entitled "Identifiability Replaced by Negative Impact (Objective Harm)" which elaborate on this issue.

For example, behavioural advertising may often involve the collection of IP addresses and the processing of unique identifiers (through the use of cookies). Since the use of unique identifier allows the tracking of users of a specific computer, individuals could be targeted or "singled out", even if their real names or contact information are not necessarily known.[1062] Taking decisions based on a given profile without actually knowing the name of the individual associated with it could create some type of harm. We will recall that Amazon was accused of practising *adaptative pricing* using cookies that would identify the profile of a specific client in order to readjust and raise the price of certain items in accordance with the profile of the potential purchaser.[1063] A purposive approach of the notion of *personal information* following the proposed test in section 3.2.2 of this thesis may determine that since this kind of use of the profile data by Amazon creates a risk of objective harm (discrimination) to the individual behind the given profile, then this profile qualifies as *personal information* under the relevant DPL, with all of the implications and obligations that this entails for the organization handling this profile information.

PIPEDA has been using a very flexible "total context approach" in certain situations when having to determine whether a piece of information is governed by PIPEDA.[1064] The purposive approach proposed in this thesis may assist in determining facets of this approach. Using the proposed approach, the OPCC could take into account the fact that if the information collected, used or disclosed creates no *risk of harm*, then it is automatically not covered by PIPEDA.[1065]

The "sensitivity" of certain information is also a subjective assessment, which will depend on different criteria. In Europe, most DPLs have categories of data which are

---

[1062] Article 29 Data Protection Working Party, *Opinion 2/*2010, *supra* note 191 at 9.

[1063] See section 2.1.2.1.2(a) which discusses this Amazon issue. See also Conseil de l'Europe, *L'autodétermination informationnelle*, *supra* note 20 at 29.

[1064] Such as when evaluating whether information created in the context of an employment is considered as *personal information*. More specifically, the OPCC has rendered findings which address whether or not the handling of a certain piece of data is governed by PIPEDA. The OPCC does not analyse whether certain information qualifies as personal, but instead whether it is covered under the definition. See section 2.2.1.3.2(d) entitled "Certain Jurisdictions Have Already Adopted a Flexible Interpretation " which discusses this "total context" approach.

[1065] The OPCC suggests that in using this contextual approach, it has been able to take into account not only the narrow context of information production, but also the broader and more important context of its collection, use and disclosure. See OPCC, *supra* note 135: "the OPC has been able to take into account not only the narrow context of information production but also the broader and more important context of its collection, use and disclosure."

"sensitive" by nature or according to article 8 of Directive 95/46/EC, "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life".[1066] In Canada however, PIPEDA is much more flexible on this issue of sensitivity and suggests that any data can be sensitive "depending on the context".[1067] A purposive approach may be useful in determining whether the context of a given piece of information creates a *risk of harm*, which in turn will determine its sensitivity under DPLs. Given that DPLs usually stipulate that the sensitivity of the information impacts certain obligations that an organization handling personal information may have, for example with regards to security measures or the level of consent that should be obtained, a purposive interpretation of *personal information* would provide certain guidance on this issue. The benefits of using a purposive approach to interpreting *personal information* when DPLs provide for some type of subjective assessment to be made by an organizations handling personal information is further discussed below.

(b) Guide When there is Subjectivity in DPLs

Organizations handling personal information are bound by a number of data protection rules. Section 2.2.1.3.2(a) details the various areas in DPLs under which there is some subjectivity or where organizations handling personal information need to make a judgment call. Organizations using a purposive interpretation of the notion of *personal information* will be able to more easily determine if their collection, use or disclosure of certain information is creating a *risk of harm* for the relevant individuals. Whether or not there is in fact a *risk of harm* will guide them in making these "judgment calls" as illustrated below.

Section 2.2.1.3.2(a)(iii) elaborates on the fact that there are various subjective provisions pertaining to the collection, use or disclosure of personal information, which also include some reasonableness, relevancy or legitimacy tests. Organizations using the purposive approach in interpreting the notion of *personal information* may more easily be able to determine if a collection or disclosure of personal information is in fact legitimate or reasonable under the provisions of these Canadian and French DPLs. To

---

[1066] EC, *Directive 95/46/EC*, *supra* note 99, art. 8, para. 1; See French DPL: *Loi informatique et liberté*, *supra* note 131 at c. II, s. 2, art. 8 (II) (1).

[1067] PIPEDA, *supra* note 63 at Schedule 1 (s. 5), principle 4.3.4.

do so, they will take into account whether the collection or disclosure at stake does in fact create a *risk of harm* for the relevant individuals. More specifically, when organizations need to make a subjective assessment as to whether a given collection, use or disclosure is relevant, appropriate, reasonable or licit in the circumstances, they may first wish to determine if the data handling activity is in fact creating a *risk of harm* to the individual. For instance, if a certain data handling activity creates no or very low *risk of harm* for the individuals, then the organization could reasonably take the position that their activities are in fact reasonable, legitimate and fair.

Section 2.2.1.3.2(a)(iv) elaborates on the fact that Canadian and French DPLs usually provide for subjectivity in the assessment of security measures that have to be implemented by an organization to protect the personal information that it is handling. In determining what kind of security measures to adopt and whether these measures are "reasonable", "necessary" or "appropriate", the first step for the organization must be to determine the extent of the *risk of harm* to individuals upon the occurrence of a security breach (or a disclosure of personal information). Using the purposive approach proposed, organizations will be positioned to establish what kind of resources to dedicate to the implementation of these proper security measures in light of the risk of harm that such disclosure may trigger to the relevant individuals.

The *European Communities (Data Protection) Regulations, 2001* introduced new rules (effective as of 1 April 2002) to clarify and build upon the existing obligation to keep personal data secure. In particular, the new rules clarified what was meant by "appropriate security measures".[1068] Among other things, the new security rules stated that in deciding what level of security was appropriate, organizations handling data must consider the nature of the personal data in question, and the *harm* that might result from its unauthorised use, disclosure or loss. Interestingly, under these rules, the *risk of harm* has to be taken into account by an organization when determining the proper security measures to adopt.[1069] For instance, it would be reasonable for

---

[1068] EC, Data Protection Commissioner, *Security Measures for Personal Data: A Guide to the New Data Protection Rules* (2001), online: <http://www.dataprotection.ie/documents/legal/6si626-01.htm> [EC, *Security Measures*].

[1069] *Ibid*.: "Comment: Organizations dealing with personal data of a private or sensitive nature – such as people's medical files, personnel files, or private telecommunications – naturally need to have very robust standards of security in place. Organizations that hold personal data with a lower privacy value – such as name, address, or membership of a local drama group – do not need to go to such great lengths, but must still have reasonable security measures in place."

organizations to weigh the costs of security measures against other factors. So, if upon the occurrence of a security breach (disclosure of personal information) the likely *harm* that would arise is trivial or minor, then an organization might justifiably decide not to invest a great deal of money in state-of-the-art security measures.[1070] Conversely, if the likely *harm* to an individual would be high in the event of a security breach, then an organization should invest in robust security measures, and indeed should regard such an investment as a budget priority.

In deciding what kind of retention delay is acceptable, necessary or reasonable, an organization may wish to first assess the kind of harm that would result in keeping this data rather than discarding it. For instance, if individuals may suffer a substantial risk of harm upon the disclosure of their data to unauthorized parties (for example, following a security breach), the organization may wish to delete the data sooner rather than later. If the disclosure of the data would create no such harm to the individual, then the organization may interpret this "necessary" or "reasonable" test more softly if it has a legitimate purpose for doing so. The purposive approach proposed may therefore be a crucial element in helping organizations decide how long it is acceptable, necessary or reasonable for them to retain the personal information that they are handling.[1071]

Section 2.2.1.3.2(a)(iv) also elaborates on the fact that ccertain DPLs provide for a very subjective breach notification obligation. The proposed purposive approach may assist in providing for a framework assisting in the assessment of whether certain types of data create a *materia*l or real risk of *significant* harm and whether certain breach notifications should be made.

Section 2.2.1.3.2(a)(v) elaborates on the fact that DPLs usually provide for a right to the individual to access and rectify his or her personal information, but there is substantive subjectivity surrounding this access right. In assessing whether the refusal by an organization to grant access is reasonable, or whether it is important for the organization to maintain accurate information, an organization may wish to assess whether this refusal of access or the potential lack of quality of the data will create a

---

[1070] *Ibid*.

[1071] It is interesting to note that this concern (individual should be the ones to determine for how long organizations can retain their data) is not a new one and documents from the seventies illustrate that already back then, this concern was on the table. Lindop, *supra* note 96 at 51, para. 5.59: "Many users urged that it should be for them to decide how long they needed to retain data."

risk of harm to individuals. Section 3.2.2 will detail how in such situations, there will be a *risk of harm* mostly in the event that the information is being "used" in such a way as to cause a negative impact on the individual. Therefore, organizations may not have to dedicate resources in order to ensure that they can grant access rights or that they periodically update information that they maintain about an individual, as long as they do not use this information in a way which is harmful to individuals.

Certain DPLs provide for some type of a subjectivity test when it comes to organizations disclosing their data protection practices to individuals and obtaining consent. This issue is discussed next.

2.2.1.5. Limit the Volume of Privacy Policies to Disclose and Consents to Obtain

Section 2.2.1.3.2(a)(ii) elaborates on the fact that in certain Canadian DPLs, there is subjectivity surrounding the notion of "consent". For example, under PIPEDA, the form of the consent may vary, "depending upon the circumstances", "the sensitivity of the information",[1072] and "the reasonable expectations of the individual".[1073] The B.C. DPL[1074] and the Alberta DPL[1075] each has similar requirements. In assessing these "circumstances" and these "reasonable expectations" of the individual, an organization may wish to first determine if a given collection, use or disclosure of personal information creates a *risk of harm* using the test proposed in section 3 of this thesis. If there is no such risk, then logically, the individual should have no expectation as to the protection of this information.

Section 2.1.1.2.1 illustrates how ineffective privacy disclosures really are, especially in the online environment, and how this translates into the situation in which is it a challenge to confirm that consumers can in fact be said to have provided informed and meaningful consent to certain data handling practices. More specifically, this section details the fact that the problem with a consent or a choice-based approach is the fact that, with the volume of data exchanges and collections taking place in the modern society (as further discussed in section 1.2.1 entitled "Increase in Volume of

---

[1072] PIPEDA, *supra* note 63 at Schedule 1 (s. 5), principle 4.3.4.

[1073] *Ibid*. at Schedule 1 (s. 5), principle 4.3.5.

[1074] B.C. DPL, *supra* note 115 at Part 3, s. 7 (3) (a), (b).

[1075] Alberta DPL, *supra* note 114 at Part 2, Division 2, s. 8 (2).

Information"), the time required to read privacy policies is too great. Gautrais and Trudel agree that there are too many consent requests, sometimes for random uses of data, ultimately distracting the user when more sensitive collections, uses or disclosures are in fact taking place.[1076]

The FTC shares the views of Gautrais and Trudel. More specifically, the FTC's staff has recently proposed that organizations provide choices to consumers about their data practices in a simpler, more streamlined way than has been used in the past.[1077] Under this approach, consumer choice would not be necessary for a limited set of "commonly accepted" data practices, thus allowing clearer, more meaningful choice with respect to practices of greater concern. This component of the proposed framework reflects the concept that it is reasonable for organizations to limit their disclosure obligations to their data handling practices that may create a *risk of harm* to individuals. These "commonly accepted" data practices (which create no risk harm for the individuals) would include product and service fulfillment, internal operations such as improving services offered, fraud prevention, legal compliance, and first-party marketing.[1078] As a matter of fact, when an online retailer collects a consumer's address solely to deliver a product the consumer ordered, this use is obvious from the context of the transaction, and therefore since there is no harm in the intended use, consent is inferred and there would be no need to disclose this practice to the consumer.

In the proposed framework under which the notion of *personal information* would take into account the *risk of harm* to individuals, principles such as notice, disclosure and consent may become more efficient. DPLs generally provide that individuals be told who is collecting their data and the purpose of such collection to enable them to decide whether to release control of all or part of such data. Given that individuals may be overloaded with information in quantities that they cannot realistically be expected to process or comprehend, obtaining proper consent from individuals may be impossible in many cases. An interpretation of *personal information,* which focuses on the *risk of harm*, would have the result of reducing the burden of the notification obligation (and

---

[1076] Gautrais & Trudel, *supra* note 1 at 179-80.

[1077] FTC, *Recommendations* 2012, *supra* note 381 at vi.

[1078] *Ibid*. at 36 and following.

concurrently, the consent obligation). While transparency of data processing would remain a fundamental principle, notification would be required only in cases of the presence of *risk or harm*.

For example, instead of detailing all of the information that has been collected as well as the uses which will be made of the data in a lengthy policy statement,[1079] a very short notice relating exclusively to the collection, use or disclosure of data that may present a *risk of harm* to the individual would be just as effective. We may one day see one paragraph user-friendly statements outlining, for example, the possible sale of profile information to third parties for marketing purposes (instead of detailing what is blatantly obvious, what the individual already knows or which constitutes no risk of harm for the individual).

This proposed purposive approach may allow organizations to streamline their communications with individuals, reducing the burden and confusion on individual consumers. Also, it may assist in providing for a framework allowing for organizations handling personal information to focus on disclosing the collection, the use and the disclosure of personal information in line with the original purpose of DPLs. This may translate into shorter and more efficient privacy policies.

The proposed approach may also assist in providing guidance on various notices and consent issues. Certain DPLs provide for some type of subjectivity test when it comes to organizations disclosing their data protection practices to individuals. PIPEDA provides that organizations shall make "a reasonable effort" to ensure that the individual is advised of the purposes for which the information will be used.[1080] The Alberta DPL[1081] and the B.C. DPL[1082] have similar requirements. If a given use or disclosure of personal information creates a high *risk of harm* using the tests proposed in section 3 of this thesis, organizations may wish to ensure that they dedicate more

---

[1079] For example, this could be a transactional website stating the following: "we collect your name, email and physical addresses and financial information in order to process the transaction, send you a confirmation and deliver the goods that you have purchased on our website". Since these activities would not create a risk of harm, they would not be governed under DPLs since this information would not be considered *personal information*.

[1080] PIPEDA, *supra* note 63 at Schedule 1 (s. 5), principle 4.3.2.

[1081] Alberta DPL, *supra* note 114 at Part 2, Division 2, s. 8 (3).

[1082] B.C. DPL, *supra* note 115 at Part 3, s. 8 (3) (a), (b), (c), (d), (e).

efforts and resources in hopes of ensuring that individuals are properly and clearly advised of the purposes for which the information collected will be used or disclosed. This may be done, for example, by having individuals click to confirm that they have read the organization's privacy policy or by drawing their attention to the data handling practices which are potentially more harmful to them. On the other hand, if this *risk of harm* is nonexistent or minimal, organizations may logically dedicate fewer resources in complying with these notice requirements and may simply post a simple privacy policy on their website.

***

The present section simply summarizes the type of benefits that may result from using the purposive approach but there are various other benefits that have not been mentioned. For example, if an organization commits a breach of the provisions of DPLs, individuals may decide to claim from this organization the damages that this breach has caused them. In Europe, Directive 95/46/EC states that individuals that "*have suffered damage*" as a result of a processing operation unlawful according to a DPL are entitled to receive compensation from the organization.[1083] According to the case law rendered in Canada, the recourse available pursuant to PIPEDA cannot be used as a vehicle to claim damages that are not a direct result of the illegal breach of the organization.[1084] This means that an organization's lack of compliance with this DPL does not automatically imply any *type of harm* for an individual. The purposive approach proposed in this thesis may therefore be useful to assist in providing for a framework in order to assess whether individuals may have a certain right to damages resulting from a confirmed breach under PIPEDA or another DPL. Also, in the U.K., a jurisdiction considering enforcing their DPL only in cases that the organization's activity has created a *risk of harm* to individuals,[1085] the purposive test proposed in this thesis may provide a good framework on which to build on.

The approach proposed in this thesis may assist in providing for a framework assisting lawmakers, policymakers, privacy commissioners, courts, organizations handling

---

[1083] EC, *Directive 95/46/EC*, *supra* note 99 at art. 23 (1).

[1084] See *Randall*, *supra* note 599; *Stevens*, *supra* note 599; *Nammo v. Transunion of Canada*, 2010 FC 1284 (CanLII) [*Nammo*].

[1085] See section 2.2.2.2.2 entitled "Risk of Harm in Recent Documents" that discusses this issue.

personal information and individuals assessing whether certain information should be governed by the relevant DPL, depending on whether the data handling activity creates a *risk of harm* for an individual. This will be useful when ensuring that DPLs are efficient and that these DPLs have an appropriate outcome in light of modern technologies. In the context of proposing a new purposive interpretation to the definition of *personal information*, the idea is to aim for a level of generality which corresponds with the highest level goal that the lawmakers wished to achieve. In the following section, I will elaborate on what is the ultimate purpose of DPLs.

2.2.2. Determining Risk of Harm as Purpose Behind the Protection of Personal Information

In proposing a new interpretation of *personal information*, which will address the challenges brought on by the application of DPLs in the context of new technologies and the Information Age, the idea is to aim for a level of generality which corresponds with the highest-level goal that the lawmakers initially had in mind.[1086] I maintain that this will provide for an optimal protection (protecting the information that should be protected) while ensuring that new technologies will be treated fairly. DPLs should therefore focus on protecting data that can create some type of *risk of harm* to individuals. Moreover, the interpretation of *personal information* should reflect this goal.

Although DPLs or transnational policy instruments pertaining to the protection of personal information that have been adopted since the early 1980s (OECD Guidelines, Convention 108, Directive 95/46/EC and the APEC privacy framework) all claim to protect the privacy of individuals,[1087] they underline a much broader purpose: the one of protecting individuals from the risk of harm resulting from the collection, use and disclosure of their personal information. First, this ultimate purpose is the most logical one in the context of data protection rights, since although these rights include a privacy aspect, the type of harm that may result from the use of data is much broader than *privacy harm* in the strict sense. Second, this much broader goal is evidenced

---

[1086] According to Moses, having a law whose level of generality corresponds with the highest level goal that the lawmakers wish to achieve will ensure that new technologies will be treated fairly. Bennett Moses, *supra* note 552 at 62. See also at 66: "For example, high level goals such as *preserving human life* or *improving economic efficiency* would be relatively immune to waves of technological change."

[1087] See OECD, *Guidelines*, *supra* note 11 at Preface; Convention 108, *supra* note 10 Preamble; EC, *Directive 95/46/EC*, *supra* note 99 at Whereas (1), (2) and (10); APEC, *Privacy framework*, *supra* note 363 at part. I, Preamble, s. 1.

from old texts dating back to the pre-enactment of DPLs or leading to the adoption of national laws or transnational policy documents incorporating the FIPs, as well as from more recent documents.

This section will first elaborate on the difference between the following two notions: "privacy" and "data protection". Then, I will discuss how the ultimate purpose behind DPLs was the protection of individuals against a *risk of harm*.

2.2.2.1. Privacy and Data Protection are not One and the Same

One of the main purposes behind the adoption of DPLs was to protect the privacy of individuals.[1088] Privacy debates have quite naturally focused on information and on constraining its use and dissemination. As a matter of fact, when referring to DPLs, contemporary privacy scholarship links data collection with "privacy invasion" so frequently that this assumption has become second nature to many scholars.[1089] We usually refer to "privacy laws", when we are in fact referring to DPLs. It has been raised that "The connection between the collection of personal information and personal privacy is straightforward: the more personal data the websites collect, store, use, the less privacy that data subjects have."[1090] Van den Hoven and Pieter E. Vermaas ("Vermaas") state that "No data, no need for data protection; no personal information, no need for informational privacy."[1091]

Privacy and data protection are two fields that definitely overlap.[1092] DPLs address personal privacy, as it relates to personal-data record keeping.[1093] But privacy and data protection are not one and the same. In Europe, the Article 29 Working Party has

---

[1088] See section 2.2.2 entitled "Determining Risk of Harm as Purpose Behind the Protection of Personal Information" which elaborates on this issue.

[1089] Karas, *supra* note 362 at 9.

[1090] Steven Hetcher, "Changing the Social Meaning of Privacy in Cyberspace" (2001) 15 Harv. J.L. & Tech. 149 at footnote 29.

[1091] Van Den Hoven & Vermaas, *supra* note 1036 at 292-93.

[1092] Lindop, *supra* note 96 at 9-10, para. 2.04: "The Younger Committee has to deal with the whole field of privacy. Our tasks has been to deal with that of data protection. In fact, the two fields overlap, and the area of overlap can be called 'information privacy' or, better, 'data privacy'. It is an important area (…) But it is not by itself the whole field of data protection, and we have had to consider some matters which do not directly raise questions of privacy. However, we found it useful to examine the concept of data privacy, and its implications and consequences. For this purpose we have used the term data privacy to mean the individual's claim to control the circulation of data about himself."

[1093] U.S. Department of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *supra* note 57 at s. III.

reiterated the fact that the right to the protection of personal data is separate and different from the right to private life:

> "(…) It should be noted that the Charter of Fundamental Rights of the European Union enshrines the protection of personal data in Article 8 as an autonomous right, separate and different from the right to private life referred to in Article 7 thereof and the same is the case at national level in some Member States."[1094]

Many separate the privacy or human dignity aspect and the data protection rights aspect when these are under analysis, given that these are two different things that may bring different concerns. For example, in Europe, the Article 29 Working Party makes a distinction between the "violation of human dignity" and "data protection rights" which may take place with some applications of RFID technology.[1095] This implies that they may therefore potentially be two separate types of rights.

The concept of "informational privacy" (or privacy as "control over personal information") was brought into the academic mainstream by Alan Westin, who famously characterized this notion as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others".[1096] Ian R. Kerr and Jenna McGill, suggest that while data protection is indeed an important aspect of privacy, it remains unclear how effective it is in protecting privacy writ large.[1097] According to these authors, it is also unclear whether informational privacy, so defined, is foundational or instrumental, whether it is a human right or merely an economic right.[1098]

[1094] Article 29 Data Protection Working Party, *Opinion 4/2007*, *supra* note 100 at 7. The Article 29 Working party also states at the same page 7: "(…) and the same is the case at national level in some Member States. This is consistent with the terms of Article 1.1, aimed at protecting 'the fundamental rights and freedoms of natural persons, and *in particular* [but not exclusively] their right to privacy'. Accordingly, the Directive makes particular reference to the processing of personal data in contexts outside of the home and family, like that provided for by labour law (Article 8.2 (b)), criminal convictions, administrative sanctions or judgements in civil cases (Article 8.5) or direct marketing (Article 14 (b))."

[1095] Article 29 Data Protection Working Party, *RFID technology*, *supra* note 196 at 2: "On the data protection front, Working Party 29 ('Working Party 29') is concerned about the possibility for some applications of RFID technology to violate human dignity as well as data protection rights."

[1096] Westin, *Privacy and Freedom*, *supra* note 45 at 7.

[1097] Kerr & McGill, *supra* note 625 at 412-13.

[1098] *Ibid*. Ian R. Kerr and Jenna McGill refer to the following other authors: Ann Cavoukian, *Privacy as a Fundamental Human Right vs. an Economic Right: An Attempt at Conciliation* (Toronto: Information and Privacy Commissioner, 1999), online: Office of the Information and Privacy Commission for Ontario <http://www.ipc.on.ca/images/Resources/up-1pr_right.pdf>. The human rights approach, construing

While "privacy" includes various aspects of "data protection", I argue that these are not one and the same since privacy is broader than data protection, and that data protection is broader than privacy. I maintain that DPLs' ultimate purpose was to protect individuals against data handling activities which were potentially harmful to them. This notion of "risk of harm" behind DPLs (or data protection) is actually broader than the notion of "privacy", and "privacy" is also broader than data protection, although these two notions clearly overlap.

2.2.2.1.1. Privacy is Broader than Data Protection

Throughout time, privacy risks have been described in various different ways. In many cases these risks having nothing to do with the handling of personal information. Privacy is therefore broader than data protection since it involves all sorts of things that are not necessarily or directly linked to the handling of personal information. Professor Alan Westin first described privacy as "the state of solitude or small group intimacy".[1099] In the late 1960s, the jurists attending the Nordic Conference, expanding on what they meant by the right of privacy (which they equated with the right to be let alone), spoke of a person's "private, family or home life" as the first area to be protected, but they also singled out as activities against which a person should be protected: "(b) interference with his physical (…) integrity (…)(g) spying, prying, watching and besetting; [and] (h) interference with his correspondence (…)".[1100] In Europe, the "Justice" Bill spoke of a person's state of being "protected from intrusion upon himself, his home, his family, his relationships and communications with others, his property and his business affairs, including intrusion by spying, prying, watching and besetting [and] the unauthorised overhearing (…) of spoken words (…)".[1101] The Scottish Office in 1972 referred to the fact that the right of privacy was broader than data protection

---

privacy as a moral and social "good", has been the primary approach to privacy advocacy and is bolstered by a number of international human rights covenants including the *Universal Declaration of Human Rights*, *supra* note 7, the *European Convention for the Protection of Human Rights and Fundamental Freedoms*, *supra* note 7, and the *International Covenant on Civil and Political Rights,* 19 December 1966, 999 U.N.T.S. 171, arts. 9-14, Can. T.S. 1976 No. 47, 6 I.L.M. 368 (entered into force 23 March 1976, accession by Canada 19 May 1976).

[1099] Westin, *Privacy and Freedom*, *supra* note 45 at 7.

[1100] Conclusions of the Nordic Conference of International Jurists on the Right of Privacy, Stockholm, 1967; at Appendix K hereto; discussed in *Report of the Committee on Privacy*, *supra* note 3 at 18, para. 60.

[1101] See "Privacy and the Law" Appendix J, at clause 9 discussed in *Report of the Committee on Privacy*, *supra* note 3 at 18, para. 60.

since it has two main aspects, only one of them relating to data protection (the other one being freedom from intrusion upon oneself, one's home, family and relationships).[1102] In the U.K., the Lindop Report stated that with DPLs, we did not have to define privacy since the law would be limited to data handling activities, and would therefore not have to address other privacy problems which are unrelated to data, such as problems of rights of entry, intrusion into the home, surveillance by electronic or optical devices, or embarrassing press publicity.[1103]

While some of these "privacy" problems may in some way be related to the collection or disclosure of personal information, to a certain extent (for example the surveillance may involve the collection of images of individuals and the embarrassing press publicity, the disclosure of information of "intimate" nature) other rights such as the rights against intrusion are not directly linked to data handling activities.

In the U.S., courts which had to take a position on what constitutes the right to privacy, also took the position that this right was two-fold in *Whalen v. Roe.*[1104] According to them, it would first include the right to make private decisions, and second, the right to withhold information about them. Only the second one precisely relates to data protection, implying that privacy is broader than data protection.

Solove also makes a distinction between "Information privacy" and "decisional privacy" which involves the extent to which the state can interfere with personal decisions, on matters such as contraception, procreation, abortion, and child bearing.[1105] He has designed different categories of privacy harm, some of which are not "data related" such as the category of "Invasion". He has divided this "Invasion" category into two sub-sections. Intrusion and Decisional Interference: "*Intrusion* concerns invasive acts that disturb one's tranquility or solitude. *Decisional interference* involves the government's incursion into the data subject's decisions regarding her private

---

[1102] *Report of the Committee on Privacy*, *supra* note 3 at 10, para. 38.

[1103] Lindop, *supra* note 96 at 204, para. 21.27.

[1104] 429 U.S. 589 (1977).

[1105] See Solove, "Privacy", *supra* note 1 at 1413: "'Information privacy' is the term theorists use to discuss the privacy implications of the collection, use, and disclosure of personal information. Information privacy is often contrasted with 'decisional privacy' which involves the extent to which the state can interfere with the decisions one makes with regard to one's body and family. Decisional privacy involves matters such as contraception, procreation, abortion, and child bearing."

affairs."[1106] Unlike the other groupings, the Invasion group does not necessarily involve personal information.

David O'Brien articulates the view that privacy is invaded not just by intrusions into information but also by nuisances such as noises, smells, and other noxious disruptions of one's peace of mind.[1107] Judith Wagner DeCew points out that privacy can be invaded even if nobody else knows something new about a person, such as by being forced to hear propaganda, by being manipulated by subliminal advertisements, or by being disrupted by a nuisance that thwarts one's ability to think or read.[1108] Nissenbaum suggests that the scope of privacy is wide-ranging, potentially extending over information but also to activities, decisions, thoughts, bodies, and communication.[1109]

While the collection, use and disclosure of personal information may create a privacy breach for individuals involved, there may still be a privacy breach without any actual collection of personal information. Privacy is therefore broader than data protection.

This may happen if a person is filmed while trying on a lipstick through an RFID chip.[1110] There may be no collection of personal information since the data collected (picture of the lips) is not enough to be able to identify an individual but the individual in question may still feel that his or her privacy has been invaded. Another example may be an employee with a surveillance camera directly above their desk. The camera may not be functioning (or it may be a dummy camera) and therefore, there may not be any collection of information or images of that employee collected. But this employee may still feel unease with this camera potentially filming her desk 24-7.[1111] The harm in this

---

[1106] Solove, "A taxonomy", *supra* note 339 at 490-91.

[1107] David M. O'Brien, *Privacy, Law, and Public Policy* (Westport: Praeger Publishers, 1979) at 13-14.

[1108] Judith Wagner DeCew, *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology* (Ithaca: Cornell University Press, 1997) at 2.

[1109] Therefore, she believes that a full theory of privacy would need to take account of all these dimensions. Nissenbaum, *supra* note 230 at 123-24.

[1110] Conseil de l'Europe, *L'autodétermination informationnelle*, *supra* note 20 at 25.

[1111] Customers purchasing certain "awkward" products experienced measurably higher levels of discomfort when a dummy camera was trained on the register. See Thomas J.L. van Rompay et al., "The Eye of the Camera: Effects of Security Cameras on Prosocial Behavior" (2009) 41:1 Env't & Behav. 60.

case may result from the mere "feeling" or impression of being observed or evaluated[1112] and does not automatically involve data collection.

2.2.2.1.2. Data Protection is Broader than Privacy

The two notions "data protection" and "privacy" overlap. As a matter of fact, while privacy is broader than data protection, it is interesting to note that data protection is also broader than privacy. As early as the 1970s, at the time that DPLs were being discussed and adopted, certain committees which were in charge of analysing these issues were clear on the fact that the notion of data protection is broader than privacy. For example, the U.K. Lindop Report dating back to 1978 states:

> "(…) we believe that data protection goes further than the protection of privacy in its narrowest sense: it serves to protect many interests of the data subject, of which his privacy is only one."[1113]

The Article 29 Working Party also raises the fact that the data protection concept is much broader that the right to privacy:

> "On the one hand, it has to be considered that the concept of private and family life is a wide one, as the European Court on Human Rights has made clear. On the other hand, the rules on protection of personal data go beyond the protection of the broad concept of the right to respect for private and family life. (…) This is consistent with the terms of Article 1.1, aimed at protecting "the fundamental rights and freedoms of natural persons, and *in particular* [but not exclusively] their right to privacy". Accordingly, the Directive makes particular reference to the processing of personal data in contexts outside of the home and family, like that provided for by labour law (Article 8.2 (b)), criminal convictions, administrative sanctions or judgments in civil cases (Article 8.5) or direct marketing (Article 14 (b)). The European Court of Justice has endorsed this broad approach."[1114]

There are definite aspects of data protection which have no immediate connection with privacy. For example, the use of inaccurate or incomplete information for taking decisions about people is a legitimate subject for data protection, but it may not always raise questions of privacy.[1115] Various lawmakers and experts mandated to analyze

---

[1112] See section 3.1.1.1.1 entitled "Knowledge of Collection: Psychological Harm" which elaborates on this issue.

[1113] Lindop, *supra* note 96 at 204, para. 21.26.

[1114] Article 29 Data Protection Working Party, *Opinion 4/2007*, *supra* note 100 at 7 [footnotes omitted]

[1115] Lindop, *supra* note 96 at 9, para. 2.03. See section 3.2 which elaborates on this kind if harm.

data protection issues in the 1970s were in fact initially struggling with the distinction (privacy vs. data protection) since it was difficult to deal with the concept of privacy, as applied to records and databases.[1116]

Legal philosopher van den Hoven, in his essay on *Privacy and the Varieties of Moral Wrong-doing in an Information Age* discusses four forms of wrongdoing which typically involve personal information. He specifies that although they are all forms of informational wrongdoing, which call for data-protection, they do not all involve privacy in a strict sense.[1117] For instance, the fact that information about persons is used to inflict harm on an individual doesn't necessarily make it a privacy issue and he proposes the following examples to better illustrate his views:

> "Post modern criminals are known to have used computerized data-bases and the Internet to stage their crimes. We have to realize that in an information society there is a new vulnerability to what might be called 'information based harms'. Because of the ubiquitousness of information and information processing equipment inflicting harm and thwarting of individual preferences and life-plans will often involve as a matter of course the use of information and personal data on the part of others. As you can grab someone's arm and twist it to hurt him, you can get someone's personal information and use it to his harm. Rigorous security policies have to be put in place to protect citizens against information-based harms. (…) The reason for insisting on security and reasonable care in the context of storing sensitive data on persons is of course fear of harm. Just like we ban weapons out of fear of harm. It not strange that we fear information-based harm now information is becoming more and more like a gun."[1118]

This difference between privacy and data protection is crucial and should be taken into account when interpreting the notion of *personal information*. I argue that the ultimate purpose of the FIPs (in the context of the adoption of DPLs) while it included the

---

[1116] U.S. Department of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *supra* note 57 at s. III: "Dictionary definitions of privacy uniformly speak in terms of seclusion, secrecy, and withdrawal from public view. They all denote a quality that is not inherent in most record-keeping systems. Many records made about people are public, available to anyone to see and use. Other records, though not public in the sense that anyone may see or use them, are made for purposes that would be defeated if the data they contain were treated as absolutely secluded, secret, or private. Records about people are made to fulfill purposes that are shared by the institution maintaining them and the people to whom they pertain. Notable exceptions are intelligence records maintained for criminal investigation, national security, or other purposes. Use of a record about someone requires that its contents be accessible to at least one other person-and usually many other persons. Once we recognize these characteristics of records, we must formulate a concept of privacy that is consistent with records."

[1117] Van den Hoven, "Moral Wrong-doing", *supra* note 272 at 34.

[1118] *Ibid*. at 34-35.

protection of privacy, was actually much broader and included the protection of individuals against the *risk of harm* resulting from the collection, use and disclosure of their personal information.

2.2.2.2. Evidence that Ultimate Purpose of DPLs: Avoid the Risk of Harm

Section 2.2.2.1 has elaborated on the fact that "privacy" is not exactly the same thing as "data protection", although these two notions greatly overlap. Ohm suggests that:

> "Regulators need to shift away from thinking about regulation, privacy, and risk only from the point of view of the data, asking whether a particular field of data viewed in a vacuum is identifiable. Instead, regulators must ask a broader set of questions that help reveal the risk of reidentification and threat of harm."[1119]

I maintain that the highest level goal that the lawmakers wished to achieve with DPLs was to avoid the *risk of harm* to individuals resulting from the handling of their personal information by organizations.

2.2.2.2.1. Risk of Harm in Older Documents

While documents from the 1970s leading to the elaboration of the FIPs and the adoption of DPLs mention the fact that protection of the privacy of individuals was a central element, they also make reference and discuss the broader notion of *risk of harm* in great length.[1120]

For instance, in the U.S., the Secretary's Advisory Committee on Automated Personal Data Systems[1121] was asked to analyze and make recommendations about the "harmful consequences" that may result from using automated personal data systems, safeguards that might protect against these potentially "harmful consequences", and measures that might afford redress for any "harmful consequences".[1122] The Preface of

---

[1119] Ohm, *supra* note 562 at 1761.

[1120] See also for example, *Report of the Committee on Privacy*, *supra* note 3 at 19, para. 63: We have concluded therefore that the type of conduct against which legal protection might be afforded on the ground of intrusion on privacy should be confined to injurious or annoying conduct deliberately aimed at a particular persons or persons where the invasions of privacy is the principal wrong complained of."

[1121] This committee was established by former Secretary of Health, Education, and Welfare Elliot L. Richardson in response to growing concern about the *harmful consequences* that may result from uncontrolled application of computer and telecommunications technology to the collection, storage, and use of data about individual citizens. U.S. Department of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *supra* note 57 at Preface.

[1122] *Ibid*.

the Report of this Secretary's Advisory Committee entitled: "Preface, *Records, Computers and the Rights of Citizens*" of July 1973 unmistakably referred to this notion of *harm*.[1123]

In Europe, working documents from the 1970s leading to the elaboration of Convention 108 also include this notion of *risk of harm*. The Resolutions (73) 22 and (74) 29 refer to electronic data processing which can be "harmful" to individuals,[1124] to information that "may cause serious damage",[1125] that "may lead to unfair discrimination",[1126] to "unreasonably long retention of data that could be harmful",[1127] to retention of information that, even if not intended for use, "presents a certain risk (for example, in case of accidental leaks)".[1128] These Resolutions (73) 22 and (74) 29 also mention that in the context of making exceptions in the interests of science and of historiography, these exceptions had to be reconciled with the interests that citizens have "against the preservation of data harmful to them".[1129] They suggested that processing of sensitive information should be governed by special rules "in view of the damage which individuals might suffer in case of misuse".[1130] These concerns which FIPs were meant to address refer to a *risk of harm* to an individual that may take place if certain information is inappropriately used or disclosed.

I already discuss in section 2.2.1.3.2 that in the U.K., in 1978, before they introduced their first DPL, a notion closely related to the "harm principle" was firmly rejected by the Lindop Committee, the main reason being that there was no objective standard

---

[1123] *Ibid*.: "there is a growing concern that automated personal data systems present a serious potential for harmful consequences, including infringement of basic liberties. This has led to the belief that special safeguards should be developed to protect against potentially harmful consequences for privacy and due process."

[1124] See Council of Europe, *Explanatory Report: Resolution (73) 22*, *supra* note 56 at para. 12.

[1125] *Ibid*. para. 18.

[1126] *Ibid*. para. 19; Council of Europe, *Resolution (74) 29*, *supra* note 13 at Principle 3 of Annex.

[1127] See Council of Europe, *Explanatory Report: Resolution (73) 22*, *supra* note 56 at para. 24. See also: Council of Europe, *Explanatory Report: Resolution (74) 29*, *supra* note 65 at para. 21: "21. The first paragraph of this principle deals with the time-limits for keeping and using the information. In the public sector, just as in the private sector, individuals have a legitimate interest in seeing certain kinds of information concerning them, particularly that which is harmful to them, wiped off or rendered inoperative after a certain time has passed."

[1128] See Council of Europe, *Explanatory Report: Resolution (73) 22*, *supra* note 56 at para. 25.

[1129] Council of Europe, *Explanatory Report: Resolution (74) 29*, *supra* note 65 at para. 22.

[1130] *Ibid*. para. 18, principle 3 and para. 21.

whereby a data controller could assess *harm* prior to the processing of personal data.[1131] There was no way an organization could judge whether the personal data that it is handling or processing would be sensitive or non-sensitive, as sensitivity is a subjective assessment. And the idea behind DPLs was that individuals were the ones that were to be in control of their personal information (not organizations).[1132]

I also discuss in section 2.2.1.3.2 how more recently, this "harm principle" was also rejected by the ACRL. Under the ALRC's view, they felt that a number of the principles in the model UPPs already incorporate a *harm prevention* approach (such as data "quality", data "security", etc.),[1133] but more interestingly, they felt that the obligations imposed by a general "Prevention of Harm" principle could be undesirably vague. I also elaborate in section 2.2.1.3.2(a) how current DPLs are already very subjective on various issues (and therefore, they are already very vague) and how, in section 2.1.1.2, individuals are already not in "total control" of their information.

Interestingly, this notion of *harm*, or *risk of harm* is now back on the agenda. It has been raised recently, in the context of the application and enforcement of recent data protection transnational policy instruments or DPLs.

2.2.2.2.2. Risk of Harm in Recent Documents

The main objective of DPLs is to protect individuals.[1134] In Europe, the Article 29 Working Party has also mentioned that the Directive 95/46/EC is meant to apply to situations where the rights of individuals are *at risk*.[1135]

While many claim that the purpose of DPLs is to protect the privacy of individuals (and most DPLs mention the protection of the privacy of individuals as their main

---

[1131] Lindop, *supra* note 96 at paras. 18.24–18.27.

[1132] See section 1.1.2 entitled "Control over Personal Information and Fair Information Practices" which elaborates on this issue.

[1133] Austl., Report No. 108, *supra* note 885 at s. 32: "In particular, the 'Data Quality' principle and the 'Data Security' principle impose specific obligations to ensure the integrity of personal information that is handled by agencies and organisations, and to guard against possible misuse and unauthorised disclosure."

[1134] See for example, Article 29 Data Protection Working Party, *Opinion 4/2007*, *supra* note 100 at 4: "The objective of the rules contained in the Directive is to protect individuals."

[1135] *Ibid*.

purpose),[1136] the underlying purpose is to protect against the *risk of harm* caused by such privacy breach. For example, certain authors suggest that: "privacy would be an important value to be maintained and protected, because the loss of privacy would often result in *significant tangible and intangible harm* to individuals".[1137] Certain authors such as Trudel are confirming that the protection of individuals against the *risk of harm* is probably the main purpose behind DPL:

> "In sum, the system of regulation is designed to re-establish balance between risks and precautions. It has to encourage all stakeholders to minimize the risks flowing from situations over which they have some control and to maximize the risk incurred by stakeholders who choose to behave in ways that are harmful or unduly increase risks to legitimate users. Privacy protection on the Internet belongs to this approach."[1138]

Although section 3 will discuss the harm purpose underlined in DPLs for each data handling activity in great length,[1139] the present section will simply underline the fact that Canadian and French DPLs (including Directive 95/46/EC) mention this principle of *harm* or *risk of harm*, or at least imply it.

For example, according to these DPLs, files containing *personal information* are to be kept up to date and accurate when used to make a decision in relation to a given individual, which produces legal effects concerning or "significantly affects" the individual in question.[1140] The idea is that there be suitable measures to safeguard the individual's legitimate interests, including the opportunity for these individuals to divulge their point of view.

Organizations are prohibited to disclose personal information to third parties under DPLs. Certain Canadian and French DPLs even mention the potential harm that may

---

[1136] See OECD, *Guidelines*, *supra* note 11 at Preface; Convention 108, *supra* note 10 Preamble; EC, *Directive 95/46/EC*, *supra* note 99 at Whereas (1), (2) and (10); APEC, *Privacy framework*, *supra* note 363 at part. I, Preamble, s. 1.

[1137] Waldo, Lin & Millet, *supra* note 6 at 12.

[1138] Trudel, "Privacy Protection", *supra* note 164 at 330.

[1139] I argue that the activities of collection and disclosure were meant to address a subjective type of harm, while the activity of using information, a more objective type of harm. See section 3.1 and section 3.2 which elaborate on these two types of harm.

[1140] See section 3.2.2.1.1 entitled "Purpose behind Regulating the Use of Data: Negative Impact" and section 3.2.2.2 entitled "Accuracy of Information Used" which elaborate on this issue. See also for example: Quebec DPL, *supra* note 110 at s. 11; B.C. DPL, *supra* note 115 at Part 9, s. 33 (a); EC, *Directive 95/46/EC*, *supra* note 99 at art. 15 (1).

take place in such an event, for instance if the disclosure "may *seriously harm* that third person".[1141] An organization may disclose, without the consent of the individual, personal information for research purposes, including statistical research, only if linkage of the personal information to other data "is not *harmful* to the individuals identified by the personal information".[1142] Personal information may be processed for purposes of scientific research or statistics where there is "*clearly no risk of breaching the privacy"* of the data subject.[1143]

Organizations that possess computerized personal information are bound by a number of data protection rules. One of these rules is that they must take *appropriate security measures* to protect the personal information in their possession against the "*risks*" of unauthorised access, loss, or disclosure.[1144] They must also take into account the sensitivity of the information when determining the proper security measures to adopt, therefore implying that the disclosure of sensitive data will be more harmful to individuals. In Europe, certain new security rules notably state that in deciding what level of security is appropriate, organizations handling data must assess the nature of the personal data in question, and, interestingly, the *harm* that might result from the unauthorised use, disclosure or loss of the data.[1145]

In recent years, the few Canadian security breach notification laws that have been introduced stipulate that organizations notify affected individuals when security breaches occur. In Alberta, there is a new requirement for organizations to notify the provincial Information and Privacy Commissioner of incidents where personal information has been compromised and where a reasonable person would consider

---

[1141] Quebec DPL, *supra* note 110 at s. 40.

[1142] B.C. DPL, *supra* note 115 at Part 6, s. 21 (1) (c).

[1143] EC, *Directive 95/46/EC*, *supra* note 99 at art. 13 (2).

[1144] See section 2.2.1.3.2(a)(iv) entitled "Subjectivity in Security Measures to Adopt and Retention Obligations" which elaborates on this issue.

[1145] According to this document it is reasonable for organizations to weigh up the costs of security measures against the other factors so that if the *risks* of security breaches are low, and the *likely harm* that would arise is trivial or minor, then a data controller might justifiably decide not to invest a great deal of money in state-of-the-art security measures. Conversely, if the risks of security breaches (or attempted breaches) are high, and/or the *likely harm* to an individual would be high, then the organization should invest in robust security measures. EC, *Security Measures*, *supra* note 1068.

that there exists "*a real risk of significant harm to an individual*."[1146] At the federal level, Bill C-12 was introduced in 2011 and proposed many new sections to PIPEDA.[1147] Among the many proposals was the requirement to notify the relevant individuals when there has been a breach of security surrounding their personal information. However, this notification should only take place if it is reasonable in the circumstances to believe that the breach creates "a real risk of significant harm to the individual".[1148] It is interesting to note that when legislators are attempting to limit the scope of DPLs, they are inclined to focus of the notion of "risk of harm", probably because this is in fact the main goal at the heart of DPLs and its ultimate purpose.

Some regulators are also looking at the "*preventing harm*" principle as a valid way forward. In 2007, the U.K. Information Commissioner published its data protection strategy, which emphasised the need to make judgments about the seriousness of the risks of individual and societal harm.[1149] The strategy document goes on to say that the U.K. regulator's actions will give priority to tackling situations where there is a real likelihood of serious harm. By acknowledging that DPLs are over-reaching, the U.K. has been proposing to enforce them based on their original goal and purpose:

> "Being a strategic regulator means that, in so far as we have a choice, we have to be selective with our interventions. We will therefore apply our limited resources in ways that deliver the maximum return in terms of a sustained reduction in data protection risk. That is the risk of harm through improper use of personal information. There are priorities we have to set. We need to focus most attention on situations where there is a real likelihood of serious harm."[1150]

In 2009, RAND Corporation was mandated to evaluate Directive 95/46/EC in light of recent technological advancements. One of the main weaknesses that was identified

---

[1146] Alberta DPL, *supra* note 114 at Part 3, Division 2, s. 37.1(3). This section requires an organization to notify individuals in circumstances where the "*real risk of significant harm*" to an individual as a result of the loss or unauthorized access or disclosure is obvious and immediate.

[1147] *Safeguarding Canadians' Personal Information Act*s, *supra* note 506 aimed to amend PIPEDA, was re-introduced by the Government of Canada on September 29, 2011.

[1148] New section 10.1 of Bill C-12 which requires organizations to notify the Commissioner when there has been a "material breach" of the security surrounding their holdings of personal information. New section 10.2 requires the organization to notify the individuals involved as well if it is reasonable in the circumstances to believe that the breach creates "a real risk of significant harm to the individual". Definitions are provided for how the elements of this test are met.

[1149] ICO, *Data Protection Strategy*, *supra* note 986.

[1150] *Ibid*. at 5.

by RAND Corporation was the truly obscure link between the concept of personal data and real privacy risks.[1151] One of its main recommendations was to enforce the regulatory framework only in cases where significant *risk of harm* or *actual harm* exists:

> "Overall, we found that as we move toward an increasingly global, networked environment, the Directive as it stands will not suffice in the long term. The widely applauded principles of the Directive will remain as a useful front-end, yet will need to be supported with a harms-based back-end in due course, in order to be able to cope with the challenges of globalisation and flows of personal data".[1152]

Sweden, following a review, has recently adopted a set of regulations using a risk-based approach toward the misuse of personal data.[1153]

The objectivity and rigidity in Directive 95/46/EC has been criticized recently. As a response, the Article 29 Working Party published an opinion on the notion of *personal data* in 2007, in which it reminds all interested parties that these rules were designed to apply to situations where the rights of individuals could be *at risk* and hence in need of protection.[1154]

Recently, this notion of *harm* has been included in several national and transnational policy instruments. The Treasury Board of Canada Secretariat recently released a guidance document in which it proposes an Invasion-of-privacy Test.[1155] When organizations need to determine whether a contract that would involve personal information would result in *harm* or *injury* to an individual, this "test" can be of assistance. According to this Guide, there are three main factors that should be taken into account in any Invasion-of-privacy Test: sensitivity of the information, expectations

---

[1151] Robinson et al., *supra* note 151 at ix.

[1152] *Ibid*. at 41.

[1153] See Rebecca Wong, "The Shape of Things to Come: Swedish Developments on the Protection of Privacy" (2005) 2:2 Script-Ed 98 at 107; Robinson et al., *supra* note 151 at 41.

[1154] Article 29 Data Protection Working Party, *Opinion 4/2007*, *supra* note 100 at 25, 34.

[1155] Treasury Board of Canada Secretariat, in its 2006 *Guidance Document: Taking Privacy into Account Before Making Contracting Decisions*, Issued to federal government institutions by the Treasury Board of Canada Secretariat, 2006, online: <http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/gd-do/gd-do-eng.asp>.

of the individuals, and probability and gravity of injury.[1156] The *risk of harm* resulting from this test is then categorized as being "no risk, low risk, medium risk or high risk".

In 2005, APEC confirmed having developed a Framework on information privacy protection in recognition of the importance of developing appropriate privacy protections for personal information; particularly from the harmful consequences of unwanted intrusions and the misuse of personal information.[1157] More specifically, Principle I, "Preventing Harm" states:

> "Recognizing the interests of the individual to legitimate expectations of privacy, personal information protection should be designed to prevent the misuse of such information. Further, acknowledging the risk that harm may result from such misuse of personal information, specific obligations should take account of such risk, and remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information".[1158]

Prompted by concern over offline data privacy threats and the increasing convergence of online and offline data systems, the FTC has, since 2000, decided on a privacy approach evolved to include a focus on specific consumer harms as the primary means of addressing consumer privacy issues.[1159] The FTC admits that this harm-based approach does have its limitations.[1160] However, rather than emphasizing on potentially costly notice-and-choice requirements for all uses of information similar to what we may find in the DPLs or the FIPs, the FTC's harm-based model was meant to target practices that caused or were likely to cause physical or economic harm, or unwarranted intrusions into consumers' daily lives.[1161]

[1156] *Ibid*.

[1157] APEC, *Privacy framework*, *supra* note 363 at Preamble, s. 8.

[1158] *Ibid*. at Principle I, s. 14.

[1159] See FTC, *Recommendations* 2012, *supra* note 381 at 2.

[1160] *Ibid*. See also Fordham University School of Law Professor Joel Reidenberg has characterized the "misuse of personal information" as a "significant privacy wrong. When data is collected for one purpose and then treated differently, the failure to respect the original expectation constitutes a cognizable harm." Joel R. Reidenberg, "Privacy Wrongs in Search of Remedies" (2003) 54 Hastings L.J. 877 at 881.

[1161] FTC, Preliminary Staff Report, *supra* note 372 at 9. In announcing the Commission's expanded privacy agenda, then FTC Chairman Muris noted that "[m]any consumers are troubled by the extent to which their information is collected and used . . . [but that] what probably worries consumers most are the significant consequences that can result when their personal information is misused." *See* Remarks of FTC Chairman Tim Muris at the Privacy 2001 Conference (4 October 2001), online: <http://www.ftc.gov/speeches/muris/privisp1002.shtm>. Chairman Muris then identified various harms

Legal philosopher van den Hoven notes that privacy laws and regulations define constraints on the processing of *personal information* and that in Europe (and in Canada) the main moral principle in the area of personal data (…) is the principle of informed consent: before personal data can be processed, informed consent from the individual is required. Van den Hoven suggests a certain taxonomy which illustrates the moral reasons for the justification of protection of personal information – which are mostly harm related – and which captures most of the relevant accounts of privacy and has the advantage of turning the privacy discussion into a tractable problem.[1162] More specifically, van den Hoven posits that we would not want to be "left alone" or to be "private", but instead we want to prevent others from harming us, treating us unfairly, discriminating against us, or making assumptions about who we are.[1163]

In this thesis, I discuss the notion of "risk" of harm, instead of simply referring to the notion of "harm". This is because in evaluating whether certain pieces of information qualify as *personal information*, I maintain that we first need to assess if a certain data handling activity may be harmful to an individual.[1164] Since this harm is only potential, I find it proper to refer to a "risk" of harm. This is also because in certain situations, the harm will be subjective in nature, in which case whether the harm does in fact takes place (for instance whether an individual feels embarrassed following a disclosure of his or her medical information) will depend on each individual and their personal sensitivities.[1165] I am proposing to evaluate the "risk" that certain harm may take place. In section 3, I am proposing criteria in order to assist in determining whether this "risk" of harm is present, and if so, the extent of it.

I realize that the test proposed may not ensure that all the harmful data handling activities which may take place are in fact covered by DPLs. For instance, in a given

---

caused by the misuse of consumer data – for example, risks to physical security from stalking; economic injury resulting from identity theft; and commercial intrusions into daily life by unwanted solicitations.

[1162] Van Den Hoven & Vermaas, *supra* note 1036 at 284-85: These 4 categories are: "1. prevention of information-based harm, 2. prevention of informational inequality, 3. prevention of informational injustice, and 4. respect for moral autonomy."

[1163] *Ibid*.

[1164] See section 2.2.2.2 entitled "Evidence that Ultimate Purpose of DPLs: Avoid the Risk of Harm" which elaborates on this issue.

[1165] Whether financial information available will be used against an individual in order to inflict an objective harm (such as discriminating this individual for certain employment for instance) is only "a risk" as it may or may not take place in the future.

situation, an individual may feel some discomfort by having their name and address disclosed through a search engine service online. This information may not be covered by the test which I propose under the disclosure section 3.1.2.2 (and therefore not governed by DPLs), because this information, while being "identifiable", is not of "intimate" nature and is already widely "available" on the web.[1166] Still, I argue that at least we can build on a certain set of criteria which may be useful in establishing this *risk of harm*, since in many situations, most individuals may not suffer the subjective harm from the disclosure of their information which is not of "intimate" nature and already "available", or which is not "identifiable" to them.

***

A more targeted approach to data protection is becoming increasingly important in the era of online computing. The interpretation of *personal information* should focus on the ultimate purpose of the adoption of DPLs, which is to avoid the *risk of harm* to individuals resulting from the collection, use or disclosure of information. The following section 3 will detail how this focus is not strictly privacy based, and may differ depending on the data handling activity at stake. More specifically, it will elaborate on the fact that the type of harm to be addressed can be subjective and privacy-related (if the personal information is either "collected" or "disclosed") or more objective in nature (if the personal information is "used"). I will propose a framework assisting lawmakers, policymakers, courts, organizations handling personal information and individuals assessing whether certain types of data are "sensitive" or not (in the sense that their collection, use or disclosure may be harmful to individuals). This approach will prove to be useful when determining whether certain data are or should be covered by DPLs. The purpose being to ensure that DPLs remain efficient in light of data flows which constantly increase in volume and complexity.

[1166] See the test proposed under section 3.1.2.2 entitled "Risk of Subjective Harm: Revisiting the Sensitivity Criteria".

3. IMPLEMENTING THE RISK OF HARM APPROACH TO THE DEFINITION OF PERSONAL INFORMATION

Calo articulates the view that the vast majority of privacy harms fall into just two categories—one subjective and the other objective.[1167] Although he includes the "objective" type of harm resulting from the use of personal information under the notion of "privacy", we are both undoubtedly in agreement that there are clearly two distinct types of harms that result from the collection, use and disclosure of personal information. Esther Dyson also points out that it is possible to distinguish between objective harms resulting from the use of personal information (ex. the denial of a service, fraud) from subjective privacy harms (ex. the knowledge of certain intimate details pertaining to an individual by a second or third person which is experienced as an injury).[1168]

Evidence that two types of harms (subjective vs. objective) were targeted by DPLs can be found in documents prepared in the context of the elaboration of the FIPs in the 1970s. The following excerpt illustrates that the subjective/objective distinction was at the very heart of the original goals of the FIPs. Resolution (74) 29 mentions that:

> "Especially when electronic data banks process information relating to the intimate private life of individuals or when the processing of information might lead to unfair discrimination, their existence must have been provided for by law (…)".[1169]

In this resolution, when referring to the "intimate private life of individuals", the authors are in fact alluding to a more subjective kind of harm. Conversely, the reference to an "unfair discrimination" relates to a more objective harm. Around the same period, the Lindop Report (U.K., 1978) addressed the issue of privacy in relation to data subjects, mentioning that:

[1167] Calo, "The Boundaries", *supra* note 443 at 3: "By 'subjective,' I mean internal to the mind of the victim. By 'objective,' I mean external. My use of the terms generally comports with usage in traditional psychology, *see* Jay Moore, "Radical Behavioralism and the Subjective-Objective Distinction" (1995) 18 The Behavior Analyst 33 at 33, with an important exception: "I am counting events that are subjective to person A as objective to person B."

[1168] Robinson et al., *supra* note 151 at 3.

[1169] Council of Europe, *Resolution (74) 29*, *supra* note 13 at Principle 3 of Annex.

> "(…) Privacy means, in relation to any data subject, his interest to determine for himself what data relating to him should be *known to what other persons*, and upon what terms as to the *use which those persons may make of those data*."[1170]

This assertion also refers to a subjective kind of harm when it states: "what data relating to him should be known to what other persons", and it refers to a more objective kind of harm when it states: "and upon what terms as to the use which those persons may make of those data." [1171]

The U.K. Information Commissioner published a report on its data protection strategy in 2007, in which it is emphasizing on the need to judge the seriousness of the risks of individual harm which can present itself in different ways, also making a distinction between objective vs. subjective harms: "Sometimes it will be tangible and quantifiable, for example the loss of a job" (which implies an objective kind of harm), while: "At other times it will be less defined, for example damage to personal relationships and social standing arising from disclosure of financial circumstances" which implicitly refers to a more subjective kind of harm.[1172]

In the face of uncertainty presented by new types of data,[1173] the Article 29 Working Party recently commented on information generated by RFID tags and, more specifically, when this data should be considered as relating to an individual:

> "data relates to an individual if it refers to the identity, characteristics or behaviour of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated."[1174]

When the Article 29 Working Party suggests that the data "refers to the identity, characteristics or behaviour of an individual", it implicitly refers to a risk of harm that is of a more subjective nature.[1175] On the other hand, when referring to the information

---

[1170] Lindop, *supra* note 96 at 204, para. 21.27.

[1171] *Ibid*.

[1172] ICO, *Data Protection Strategy*, *supra* note 986 at 7-8.

[1173] See section 2.1.2.2 and section 2.1.2.2.2 entitled "Identifying a Device or an Object" which elaborates on this issue.

[1174] Article 29 Data Protection Working Party, *RFID technology*, *supra* note 196.

[1175] See section 3.1 which elaborates on this kind of harm.

"used to determine or influence the way in which that person is treated or evaluated", the Article 29 Working Party refers to a more objective kind of harm.[1176]

DPLs usually regulate three data handling activities: the "collection", the "use" and the "disclosure" of personal information.[1177] The *risk of harm* (which may be either subjective or objective) is directly linked with the type of data handling activity at stake. More specifically, a risk of subjective harm may result from the activities of "collecting" and "disclosing" personal information,[1178] while the risk of objective harm may result from the "use" of this information.[1179]

Solove has put together a "privacy taxonomy" in order to assist the legal system in grappling with the concept of privacy. He believes that since the goal of the law is to have protections that adequately prevent and redress particular problems or risks, we need to first understand the problems in order to evaluate the effectiveness of the protections.[1180] In devising a taxonomy, although there are many different ways to go about carving up the landscape, he has decided to focus on the activities that invade privacy and create problems.[1181] This taxonomy is comprised of four basic groups of harmful activities: information collection, information processing, information dissemination, and invasion.[1182] It is interesting to note that three out of the four groups relate to data handling activities, which illustrates that this is a good starting point when attempting to determine the type of harm that may take place. What may also be implied is that each data handling activity has its own set of problems that DPLs were looking to address.

[1176] See section 3.2 which elaborates on this kind of harm.

[1177] The French DPL refers to the activity of "processing" (instead of "collection", "use" and "disclosure") which includes all of these activities. See chapter I, article 2 of the French DPL which defines "Processing of personal data" as "any operation or set of operations in relation to such data, whatever the mechanism used, especially the obtaining, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, deletion or destruction."

[1178] See section 3.1 entitled "Subjective Harm Associated with Definition of Personal Information" which elaborates on this kind of harm.

[1179] See section 3.2 which elaborates on this issue.

[1180] Solove, "A taxonomy", *supra* note 339.

[1181] *Ibid*. at 485.

[1182] *Ibid*. at 488-89.

Canadian courts, perhaps even without realizing it, have (logically) separated subjective and objective harms depending on the data handling activity at stake. More specifically, there were two recent decisions rendered by the Federal Court of Canada, in which it had to evaluate the damages suffered by employees who had been dismissed following the "disclosure" of their personal information, performed without their consent, by a third party to their respective employers.[1183] The employees in question claimed damages from these third parties after they were dismissed. The court felt that in each case, sufficient evidence of a subjective type of harm (resulting from the "disclosure" of their information) was not put forward by the plaintiffs. Since the damages claimed by these employees were financial, therefore objective in nature and linked to the use of the data by the employers who dismissed them (instead of being linked to the illegal disclosure by the third parties) damages were not granted.[1184] This simply illustrates how courts are making this distinction ("use" of information = objective harm vs. "disclosure" of information = subjective harm) on an instinctive basis.

The OPCC has also made a distinction between different data handling activities in some of its findings in which it had to assess whether certain information was covered by PIPEDA (and whether certain activities are "reasonable" in accordance with PIPEDA).[1185] For example, in *PIPEDA Case Summary #220*,[1186] the OPCC concluded that a telemarketer's sales results could be disclosed to other members of the telemarketing team,[1187] but mentioned that sales records were still considered as *personal information* and that PIPEDA would not tolerate the use of this information for purposes that are "indiscriminate, ill-defined, unnecessary, inconsistent, or otherwise unreasonable". In *PIPEDA Case Summary #303*,[1188] the OPCC was asked to determine whether the sales records of real estate agents constitute *personal*

[1183] See *Randall*, *supra* note 599; *Stevens*, *supra* note 599. These are further discussed in section 3.1.2.1.2(b) entitled "Harm Caused by the Use of Information Disclosed".

[1184] These decisions are further discussed in section 3.1.2.1.2(b) entitled "Harm Caused by the Use of Information Disclosed".

[1185] Under subsection 5(3) of PIPEDA, an organization may collect, use or disclose personal information "only for purposes that a reasonable person would consider appropriate in the circumstances".

[1186] OPCC, *PIPEDA Case Summary #2003-220*, *supra* note 981.

[1187] The argument being that in an incentive-based sales environment, a telemarketer's consent to this industry practice is implied by his or her participation in the sales environment.

[1188] See OPCC, *PIPEDA Case Summary #2005-303*, *supra* note 981.

information. The OPCC ruled in the affirmative while concluding that sales records could be used only for purposes reasonably contemplated by participants in the system in which the information was entered, but also specified that this did not include the disclosure of these records to third parties for comparative and advertising purposes. It is interesting to note, when reviewing these cases, the OPCC judged "what was reasonable" based on the data handling activity in question.[1189] In the first case, it was found acceptable to "disclose" the information but not to "use" it and in the second, it was found acceptable to "use" the information but not to "disclose" it. This illustrates the fact that different harms (objective or subjective) may take place depending on the data handling activity at stake. What is "reasonable" when using personal information can be quite different from what is "reasonable" when disclosing personal information.

I maintain that in order to ensure that DPLs are effective in light of modern technologies and the Information Age, it will be essential to implement an interpretation of *personal information* which takes into account the purpose behind DPLs. By embracing this approach, we ensure that information meant to be protected by DPLs will in fact be protected. More specifically, the approach may avoid the over-inclusive or under-inclusive regulation of information by DPLs currently being witnessed.[1190] One of the main thrusts of this analysis will also be to provide guidance in situations of uncertainty regarding the classification of data and *personal information*.[1191]

If we are looking to identify the ultimate purpose of DPLs (in order to guide us in determining which kind of data should qualify as *personal information*), we need to be sensitive towards the particular type of data handling activity in question and whether the underlying *risk of harm* is subjective or objective.

[1189] In both these cases (OPCC, *PIPEDA Case Summary #2003-220*, *supra* note 981 and OPCC, *PIPEDA Case Summary #2005-303*, *supra* note 981), the fact that information about an identifiable individual was generated in a work or business context did not alone determine the outcome. Rather, the *reasonableness* of the collection, use and disclosure of personal information was assessed and this, in light of relevant contextual elements, including the needs of the organization and applicable industry standards. This approach could be called a "total context approach" to reviewing the privacy implications of specific information practices. The significant feature of this approach is that it is based on *how information is used* ("total context"), and not *where it is produced* (a "work product" approach).

[1190] See section 2.1.2.1 entitled "Over-inclusiveness and Under-inclusiveness of the Definition" which elaborates on this issue.

[1191] See section 2.1.2.2 which elaborates on this issue.

In section 3.1, I will examine the kind of harm (subjective) that may result from the collection or disclosure of personal information (and what kind of problems or concerns DPLs were attempting to address by regulating these activities). In section 3.2, I will examine the kind of harm (objective) that may result from the "use" of personal information and what kind of problems or concerns DPLs were attempting to address by regulating this data handling activity. In each section, I will present particular sets of criteria in order to streamline the evaluation of subjective and objective harms.[1192]

[1192] While this will not provide guidance on all of the elements which may be relevant in evaluating a situation in a full "total context" approach, it provides initial guidance on what kind of elements should be relevant when evaluating the information. I don't discuss all of these contextual elements in this document because they are extrinsic to the information. The proposed approach is different than a contextual approach. See section 2.2.1.2 entitled "Proposed Interpretation: Purposive Approach (vs. Contextual Approach)" which elaborates on the difference between the two approaches.

SUMMARY GRAPHIC
PROPOSED INTERPRETATION OF THE NOTION OF *PERSONAL INFORMATION*

- Interpretation depends on the ultimate purpose behind DPLs;
- Main purpose of DPLs: protecting individuals against the *risk of harm* which may take place upon an organization collecting, using or disclosing their personal information. This harm may be objective or subjective, depending on the data handling activity at stake;
- Whether a piece of information qualifies as *personal information* should therefore be determined in light of the following decision tree:

DATA HANDLING ACTIVITY	TYPE OF HARM	TEST TO DETERMINE IF DATA IS "PERSONAL"
1. Data is **COLLECTED**	Harm: **Subjective** (feeling of being under surveillance)	Since DPLs are not the proper tool to address this kind of harm, information collected should be considered *personal information* only if it may trigger a risk of harm upon being "disclosed" or "used". **Please refer to the tests under 2 (Data is Disclosed) and 3 (Data is Used).**
2. Data is **DISCLOSED**	Harm: **Subjective** (psychological: feeling of humiliation, embarrassment)	To determine if data is *personal* the following three criteria should be taken into account: 1) The data is **"identifiable"** to the individual (the more identifiable, the higher is the risk of subjective harm) 2) The data is of **"intimate" nature** (the more intimate, the higher is the risk of subjective harm) 3) The data is **"available"** (the less available it was pre-disclosure or the more available it will become post-disclosure, the higher is the risk of subjective harm)
3. Data is **USED**	Harm: **Objective** (discrimination, financial, physical harm)	**If the use of the data triggers an objective harm for the individual, the data should qualify as *personal information*. In such case, it will have to be (only) two things:** 1) **Accurate** (complete, up-to-date, etc.) 2) **Relevant** for the use If the use of data will not create such objective harm (negative impact for the individual), then the data does not qualify as *personal information.*

3.1. Subjective Harm Associated with Definition of Personal Information

DPLs and transnational policy instruments pertaining to the protection of personal information that have been adopted since the early 1980s (OECD Guidelines, Convention 108, Directive 95/46/EC and the APEC privacy framework) all generally claim to have been adopted for the main purpose of protecting the privacy of individuals.[1193] Protecting individuals against *privacy harm* would therefore be one of the main purposes of DPLs, but this kind of harm is usually very subjective in nature. It is subjective in the sense that "privacy" represents different things to different people;[1194] in other words it depends heavily on individual sensibilities.[1195] As a matter of fact, the value of privacy can even vary with age according to a 1973 U.S. report.[1196] Privacy is difficult to define for the simple reason that it is an evolving concept. Privacy, as a value, is not an absolute or a constant and its significance may vary with time and place.[1197] Already in 1972, it was raised that "the scope of privacy is governed to a considerable extent by the standards, fashions and mores of the society of which we form part, and these are subject to constant change, especially at the present time."[1198] Each society would have its own forms of privacy, which may vary widely.[1199] Privacy

---

[1193] See OECD, *Guidelines*, *supra* note 11 at Preface; Convention 108, *supra* note 10 at Preamble; EC, *Directive 95/46/EC*, *supra* note 99 at Whereas (1), (2) and (10); APEC, *Privacy framework*, *supra* note 363 at part. I, Preamble, s. 1.

[1194] J. Thomas McCarthy, *The Rights of Publicity and Privacy*, § *5.59* (*2d ed. 2005*): "Like the emotive word 'freedom,' 'privacy' means so many different things to so many different people that it has lost any precise legal connotation that it might once have had."

[1195] Pomerance, *supra* note 233 at 278: "Each person has a distinct barometer for determining when his or her privacy threshold is breached. What is jealously guarded as secret by one individual may be proudly publicized by another. Some feel violated when captured on public surveillance cameras, while others pass by without a second thought. Section 8 of the Charter only protects privacy interests that are reasonable, but reasonableness will mean different things to different people. This nebulous feature of privacy makes it difficult to measure or meaningfully quantify. It also makes it more difficult to determine when it has been lost or taken away."

[1196] U.S. Department of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *supra* note 57 at s. III.

[1197] Jean-Louis Halperin, "L'essor de la 'privacy' et l'usage des concepts juridiques" (2005) 61 Droit et Société 765 at 781 discussed in Trudel, "Privacy Protection", *supra* note 164 at 321-22. See also Karas, *supra* note 362 at 19: "(…) it lacks necessary appreciation for the significant differences in the social and cultural contexts of various kinds of data collection."

[1198] Justice Committee on privacy, "Privacy and the Law", at 5, para. 18, discussed in *Report of the Committee on Privacy*, *supra* note 3 at 17, para. 47.

[1199] *Report of the Committee on Privacy*, *supra* note 3 at 34, para. 110: "In many societies doors are non-existent, communal living is normal and an accident, a birth, a death or a quarrel is accepted as a public event."

also varies depending on the context.[1200] Since privacy is an evolving concept, at the time that the FIPs were established, it was generally agreed that there was no use in attempting to define privacy.[1201] In the U.K., the Lindop report (1978) also shared this view:

> "When the debate about privacy and computers began in the USA (and soon afterwards here) in the late 1960s, its starting point was the concept of privacy. But that concept has proved difficult to define, and elusive to pin down. Many attempts have been made (…). The Younger Committee concluded (Cmnd 5012, paragraph 58) that no useful purpose would be served by further attempts to formulate a precise and comprehensive definition, and we share their view."[1202]

Nowadays, various authors still agree that there is no point in detailing what is meant by the term "privacy".[1203] As already discussed in section 1.1.2, working documents leading to Convention 108 suggest that it was this difficulty that led to the conception of privacy as "control of information" in the first place. The idea was probably that this

---

[1200] See section 2.2.1.4.1 entitled "Providing More Flexibility ("Privacy" and "Harm" are Contextual)" which elaborates on this issue. See also Fred Cate, *Privacy in the Information Age* (Washington: Brookings Institution Press, 1997) at 31. He suggests that privacy is always contextual, that a breach of a privacy principle may be unacceptable in many circumstances, but is usually accepted as justified in at least *some* circumstance.

[1201] Justice Committee on privacy, "Privacy and the Law" at 5, para. 18, discussed in *Report of the Committee on Privacy*, *supra* note 3 at 17, para. 47: "(…) the scope of privacy is governed to a considerable extent by the standards, fashions and mores of the society of which we form part, and these are subject to constant change, especially at the present time. We have therefore concluded that no purpose would be served by our making yet another attempt at developing an intellectual rigorous analysis. We prefer instead to leave the concept much as we have found it, that it as a notion about whose precise boundaries there will always be a variety of opinions, but about whose central area there will always be a large measure of agreement." See also *ibid*. at 18, para. 59: "If one abandons the attempt to find a single and comprehensive definition of privacy, as we have done, the next task is to try to decide what are the values in which privacy is a major element, and then to decide which deserve protection. (…) We agree further that opinions as to what are aspects of privacy will vary from time to time. Man, as the 'Justice' Committee point out, is a social animal; his society evolves; and this evolution will alter from time to time the public's view on what needs to be dealt with by the law. This brings us to the various concepts of privacy that have been advanced in other studies of the problem."

[1202] Lindop, *supra* note 96 at 9, para. 2.01.

[1203] For instance, see Van den Hoven, "Information Technology", *supra* note 642 at 303: "I will not deal with the possible answers to the question as to what the best conceptual analysis of the term 'privacy' is because we can do without such an analysis and still articulate what bothers us about others having access to information about us that we did not volunteer." See also Solove, "A taxonomy", *supra* note 339 at 486: "Using the general term 'privacy' can result in the conflation of different kinds of problems and can lead to understandings of the meaning of 'privacy' that distract courts and policymakers from addressing the issues before them."

approach provided for a more objective evaluation.[1204] In the early 1970s, during the emergence of DPLs, it was already acknowledged in the U.S. that it was difficult to define personal privacy in terms that provide a conceptually sound framework for public policy consistent with record keeping practices.[1205]

According to Calo, the subjective category of privacy harm would be the unwanted perception of observation and the unwelcome mental states—anxiety or embarrassment—that accompany the belief that one is or will be watched or monitored.[1206] He states:

> "The first category is "subjective" in the sense of being internal to the person harmed. Subjective privacy harms are those that flow from the unwanted perception of observation. Subjective privacy harms can be acute or ongoing, can accrue to one individual or to many. They can range in severity from mild discomfort at the presence of a security camera to mental pain and distress far greater than could be inflicted by mere bodily injury."[1207]

The first type of harm that may be triggered by DPLs is of a subjective nature and usually is linked with two types of data handling activities: the collection of personal information and the disclosure of this information, as detailed below.

3.1.1. Subjective Harm Resulting from the Collection of Information

The first data handling activity typically regulated by DPLs involves the collection of personal information. Although the term "collection" is not specifically defined in the Canadian and French DPLs discussed in this thesis, it usually relates to the activity or the means by which personal information is gathered or obtained.[1208]

[1204] It was an easier method than defining privacy since: "although the idea of privacy is very difficult to define, it is possible to tell when and how it may be infringed upon by the computerized use of personal data". See Council of Europe, *Report on data processing*, *supra* note 66 at 5, s. II, s. 3.

[1205] U.S. Department of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *supra* note 57 at s. III.

[1206] Calo, "The Boundaries", *supra* note 443 at 3.

[1207] *Ibid*. at 14 [footnotes omitted].

[1208] Gautrais and Trudel examine to the notion of "collection" in the Quebec public sector DPL and under PIPEDA. See Gautrais & Trudel, *supra* note 1 at 112-25. More specifically, at 120: "La collecte de renseignements personnels s'entend donc comme une opération par laquelle des renseignements sont placés sous le contrôle d'une entité qui du fait de cette operation acquiert, à l'égard des documents ou

The *risk of harm* resulting from the collection of personal information is usually of a subjective nature: it can be assimilated with a psychological type of harm, similar to a feeling of being observed (or under surveillance), as discussed below. I will explain, in this section, why DPLs were not specifically aiming at addressing this kind of harm. I also maintain that, in light of the Information Age, the kind of harm resulting from the "collection" of information is extremely difficult to regulate through DPLs. Given the volume of personal information readily available today,[1209] we should be focusing on the type of harm which can take place through other data handling activities, namely the types of harm triggered by the use or the disclosure of *personal information*. As a matter of fact, if an organization collects personal information without ever actually "using" it (for instance to take a decision which will impact the individual)[1210] and adequately protects the information against any potential disclosure,[1211] then the risk of harm at the "collection" level is either minimal, or it should be regulated by tools other than DPLs.

I will first discuss the type of harm that may result from the collection of personal information, and then I will elaborate on the original concerns that DPLs were meant to address. Finally, I will outline the type of challenges that result from regulating this activity through DPLs, in light of advancements in modern technologies.

3.1.1.1. Harm Resulting from the Collection (1960s – 1970s Concerns)

We can separate the types of harm resulting from the activity of "collecting" personal information into two categories. The first category relates to a feeling of being under surveillance or observation.[1212] The second category of harm relates to an individual

---

renseignements, un droit d'en prendre connaissance. Pour qu'il y ait 'collecte' de renseignements ou de documents, il faut que ces documents ou renseignements aient été communiqués à une entité, à une personne qui a le droit d'en prendre connaissance."

[1209] See section 1.2.1 entitled "Increase in Volume of Information" which elaborates on this issue.

[1210] See section 3.2.2.1 entitled "Identifiability Replaced by Negative Impact (Objective Harm)" which elaborates on this issue.

[1211] See section 3.1.2.1 entitled "Harm resulting from the Disclosure (1960s-1970s Concerns" which elaborates on this issue.

[1212] This would be triggered by the knowledge and the awareness that one is being monitored (or at least the impression that he or she is). This feeling can also be triggered if an individual's personal information is collected excessively by an organization, without a legitimate purpose.

who is not aware that certain information is collected about him or her, in which case the type of harm resulting from the collection is more of a dignitary type.

3.1.1.1.1. Knowledge of Collection: Psychological Harm (Big Brother Metaphor)

Concerns resulting from the emergence of new technical devices and their impact on the collection of data are not new.[1213] The early 1970s ushered in numerous sophisticated electronic devices, which greatly increased the possibilities of surreptitious supervision.[1214] Surveillance technology has continued to expand almost exponentially ever since.[1215] In section 2.2.1.4.3(b)(i), I elaborate on why protecting the privacy of individuals is important and in section 3.1.1.1.1(a), on how and why surveillance may be harmful for individuals.

Calo suggests that the subjective category of privacy harm, which would include the harm resulting from the collection and the disclosure of personal information, is the unwanted perception of observation, broadly defined: "Watching a person directly—their body, brain waves, or behavior—is observation."[1216] This type of harm is mostly relevant in the context in which the individual is in fact aware (or believes) that his or her information is being collected, either in a continuous way (surveillance), or excessively.[1217] Therefore, a first type of harm relating to the collection of personal information will result when an individual is aware of the collection of his or her information,[1218] when the collection is continuous (or potentially continuous), or when it

---

[1213] *Report of the Committee on Privacy*, *supra* note 3 at 202-03, para. 655: "In some cases we have recommended that there should be legislation to create either a new offence in order to deal with new threats to privacy, for instance new technical surveillance devices."

[1214] *Ibid*. at 6, para. 18: "To some extent the new public concern on this subject is the direct result of new technological developments. Numerous sophisticated electronic devices have been invented and marketed, which greatly increase the possibilities of surreptitious supervision of people's private activities and of spying upon business rivals."

[1215] See section 1.2.2 entitled "New Types of Information and Collection Tools" which elaborate on this issue.

[1216] Calo, "The Boundaries", *supra* note 443 at 1144.

[1217] By excessively, I mean a collection of personal information with no legitimate purpose or justification, information which is not "necessary" or "relevant" for the intended use. See section 2.1.1.1.2 entitled "Ignoring Legitimate Reasons for Collecting, Using and Disclosing Information" which elaborates on the issue of legitimate reasons for collecting information. See also section 3.2.2.3 which elaborates on the fact that information collected and used shall be relevant for the intended purpose.

[1218] Unless the individual did consent to the collection.

is excessive. This type of harm is mostly of a psychological and of a subjective nature: some may talk about "great consumer discomfort" in the surveillance aspect of new technologies,[1219] in the feeling of being embarrassed,[1220] others in feelings of anxiety and discomfort resulting from the continuous monitoring, feelings of "uneasiness",[1221] a feeling of being "extremely uncomfortable",[1222] a "feeling of being monitored" or a "feeling that their moral autonomy to project their moral identity is compromised".[1223]

(a) Upon a Continuous Collection (Surveillance)

Two metaphors have been used when discussing the privacy harm resulting from the constant monitoring of individuals: the Big Brother metaphor and the Panopticon metaphor.

A commonly used analogy is the so-called "Big Brother" metaphor, used to describe the type of harm resulting from the data collection or, more specifically, the feeling of being under surveillance. This metaphor finds its source in the totalitarian state and government portrayed in George Orwell's *Nineteen Eighty-Four*, that exploited technology to control citizens and strip them of their privacy, dignity and autonomy.[1224] In this novel, a surveillance device, the "telescreen", was installed in each and every household. The telescreen was a television that citizens could watch and, in turn, enabled "Big Brother" (the Thought Police) to see what the citizens were doing themselves. These telescreens were similar to surveillance cameras in the sense that citizens did not know whether they were being monitored at any given moment, but there was *always* the possibility that they were in fact being watched.[1225]

[1219] Hariton, Lawford & Palihapitiya, *supra* note 197 at 4.

[1220] See Swire, *supra* note 1042 at 473: "If I know I am under surveillance, I might (…) restrict my activities, so that nothing embarrassing or otherwise harmful could be detected."

[1221] Solove, "A taxonomy", *supra* note 339 at 498-99.

[1222] *Ibid*. at 493-94.

[1223] Van Den Hoven & Vermaas, *supra* note 1036 at 294-95: "The focus of attention should not merely be on the information that is generated, stored, and reused by RFID tags, but also on the fact that with those tags, users may feel actively monitored from all sides, and may feel that their moral autonomy to project their moral identity is compromised."

[1224] George Orwell, *Nineteen eighty-four* (New York: Harcourt, 1949).

[1225] *Ibid*. at 4: "You had to live—did live, from habit that became instinct—in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized."

Schwartz compares Internet "surveillance" to Orwell's telescreen, concluding that cyber-surveillance is even more harmful since it (the Internet) "creates digital surveillance with nearly limitless data storage possibilities and efficient search possibilities."[1226] Solove suggests that the collection of information on the Internet can be readily analogized to the telescreen since as individuals surf the Internet, information about them is being collected: "we are being watched, but we do not know when or to what extent."[1227] He raises that journalists,[1228] politicians,[1229] jurists,[1230] and legal scholars[1231] have described the problem created by the accumulation of personal information in databases with the metaphor of Big Brother.[1232] Instead of one single Big

---

[1226] Schwartz, *Cyberspace*, *supra* note 355 at 1657, n° 294.

[1227] Solove, "Privacy", *supra* note 1 at 1415.

[1228] *See, e.g.,* William Branigin, "Employment Database Proposal Raises Cries of 'Big Brother'", *The Whashington Post* (3 October 1995) at A17; James Gleick, "Big Brother Is Us: Our Privacy is Disappearing, But Not by Force. We're Selling it, Even Giving it Away", *The New York Times* (29 September 1996) (magazine) at 130.

[1229] To respond to the computerization of records, in 1984 a House committee held hearings called "1984 and the National Security State." Priscilla M. Regan, *Legislating privacy: technology, social values, and public policy* (Chapel Hill: University of North Carolina Press, 1995); *see also* U.S., *Cong. Rec.*, vol. 140, at H9797, H9810 (27 September 1994) (Rep. Kennedy) (concerning the Consumer Reporting Reform Act of 1994, Senate Bill 783): "For tens—if not hundreds—of thousands of consumers, the promise of the information highway has given way to an Orwellian nightmare erroneous and unknowingly disseminated credit reports."; Tod Robberson, "Plan for Student Database Stirs Opposition in Fairfax", *The Washington Post* (9 January 1997) at A1: "'This thing is Orwellian', said board member Carter S. Thomas (Springfield): 'It triples the amount of data that can be collected on individual students, teachers and even janitors'."

[1230] *See J. Roderick MacArthur Found. v. FBI*, 102 F. (3d) 600 at 608 (D.C. Cir. 1996) (Tatel, J., dissenting): "Congress passed the Privacy Act to give individuals some defenses against governmental tendencies towards secrecy and 'Big Brother' surveillance.'"; *McVeigh v. Cohen*, 983 F. Supp. 215 at 220 (D.D.C. 1998): "In these days of 'big brother,' where through technology and otherwise the privacy interests of individuals from all walks of life are being ignored or marginalized, it is imperative that statutes explicitly protecting these rights be strictly observed."

[1231] See Charles N. Faerber, "BookVersus Byte: The Prospects and Desirability of a Paperless Society" (1999) 17 J. Marshall J. Computer & info. L. 797 at 798: "Many are terrified of an Orwellian linkage of databases allowing any individual to leave home without a wallet or purse but with a retinal pattern or other biometric identifier and then to perform any conceivable financial or documentary transaction."; Bryan S. Schultz, "Electronic Money, Internet Commerce, and the Right to Financial Privacy: A Call for New Federal Guidelines" (1999) 67 U. Cin. L. Rev. 779 at 797: "As technology propels America toward a cashless marketplace where financial transactions are conducted with the aid of computer record-keeping, society inches closer to fulfilling George Orwell's startling vision of a nation where 'Big Brother' monitors the who, what, where, when, and how of every individual's life."; Alan F. Westin, "Privacy in the Workplace: How Well Does American Law Reflect American Values" (1996) 72 Chi.-Kent L. Rev. 271 at 273. Westin is stating that Americans would view the idea of government data protection boards to regulate private sector databases as "calling on 'Big Brother' to protect citizens from 'Big Brother.'"; Wendy Wuchek, "Conspiracy Theory: Big Brother Enters the Brave New World of Health Care Reform" (2000) 3 Depaul J. Health Care L. 293 at 303.

[1232] Solove, "Privacy", *supra* note 1 at 1394-95.

Brother, today there would be various "Little Brothers" (referring to private sector entities) collecting personal data.[1233]

Others are referring to the Panopticon metaphor to illustrate the modern privacy concerns triggered by online monitoring practices.[1234] The Panopticon metaphor, in reference to Jeremy Bentham's idea of the ideal prison design (a hemispherical building with a central view point in the middle) is another way of illustrating the type of harm that results from the constant collection of information (or surveillance).[1235] The Panopticon is a transparent construction allowing for and facilitating constant surveillance by placing guards in a central tower, thereby creating a sense of "conscious and permanent visibility that assures the automatic functioning of power".[1236] Bentham suggested that the mere assumption on the part of inmates that they were always being monitored would constrain them to act in the required ways. As a matter of fact, the harm is not necessarily in the activity of collecting *per se*, but it is in the knowledge of the collection, or from the mere belief that one is being observed.[1237]

[1233] See Dorothy Glancy, "At the Intersection of Visible and Invisible Worlds: United States Privacy Law and the Internet" (2000) 16 Santa Clara Computer & High Tech. L.J. 357 at 377. Dorothy Glancy is describing privacy problem created by the private-sector as the "little brother" problem; Marsha Morrow McLauglin & Suzanne Vaupel, "Constitutional Right of Privacy and Investigative Consumer Reports: Little Brother Is Watching You" (1975) 2 Hastings Const. L.Q. 773; Hon. Ben F. Overton & Katherine E. Giddings, "The Right of Privacy in Florida in the Age of Technology and the Twenty-First Century: A Need for Protection from Private and Commercial Intrusion" (1997) 25 Fla. St. U. L. Rev. 25 at 27*:* "In his book, *1984*, we were warned by George Orwell to watch out for 'Big Brother.' Today, we are cautioned to look out for 'little brother' and 'little sister.'"; Thomas L. Friedman, "Foreign Affairs: Little Brother", *The New York Times* (26 September 1999) at s. 4 at 17; Wendy R. Leibowitz, "Personal Privacy and High Tech: Little Brothers Are Watching You" (1997) Nat'l L.J. at B16; See also Thompson, *supra* note 257: "Does the Law Recognize the 300 Million Little Brothers Problem? The section above should suggest it, but her it is expressly: we no longer live in a nation of Big Brother; we live in a nation of 300 million Little Brothers."

[1234] Katyal, *supra* note 1044 at 319: Sonia Katyal argues that from both an architectural as well as a philosophical perspective, cyberspace networks, particularly of the peer-to-peer variety, bear much similarity to the Panopticon. See Van Den Hoven & Vermaas, *supra* note 1036.

[1235] See for example: Thompson, *supra* note 257: "We've moved from the Panopticon—where the guards can see everything—to a suburb of glass houses where everyone can see each other. This is a powerful development for politics (we can now watch the watchers), but it has changed inter-personal privacy as well. What laws (if any) should be updated to reflect this new reality? Or should we all just get used to living in public (…) The power of the Internet is increasingly moving toward making sure that everybody knows what everybody does. Is this the right direction?"

[1236] Michel Foucault discussed, in 1977, Bentham's idea of the Panopticon as the ideal prison design in the context of his study on punishment and surveillance and this has shaped in a certain way the discussions about privacy since that period. See Oscar H. Gandy, Jr., *The panoptic sort: a political economy of personal information* (Boulder, Colo.: Westview, 1993).

[1237] The perception that one may be under surveillance, even if there is no actual "collection" of information, may create the same type of harm than if there was such collection. See Calo, "The

To illustrate this, studies show that customers purchasing certain "awkward" products were reported to experience measurably higher levels of discomfort when a dummy camera was trained on the register.[1238]

Calo explains that the type of psychological harm resulting from the collection of personal information (or monitoring) may not always occur instantaneously; there may be a delayed reaction. For example, many subjective privacy harms (such as an employer's hidden surveillance camera) will be backward looking, once the individual becomes aware of the collection of images (or surveillance) that took place.[1239]

The concern resulting from this kind of harm was already very much present in the late 1960s and early 1970s. Most of the documents produced by privacy experts (including Alan Westin's 1967 book on *Privacy and Freedom*) and from the Council of Europe or other organizations, during this period, referred to new surveillance technologies. These included phone-tapping, electronic eavesdropping, surreptitious observation, hidden television-eye monitoring, truth measurement by polygraphic devices, personality testing for personnel selection, the illegitimate use of official statistical and similar surveys to obtain private information, and subliminal advertising.[1240] Some argue that in the 1970s and 1980s, it was the fear of panopticism, mixed with the image of government as Big Brother, that lead to the adoption of strong DPLs in Europe in order to prevent the centralization of monitoring, surveillance, and power at the expense of individual freedom.[1241] I am of the view that this particular type of harm

---

Boundaries", *supra* note 443 at 14: "But actual observation need not occur to cause harm; perception of observation can be enough."

[1238] *See* Thomas J.L. van Rompay et al., *supra* note 1111, discussed in Calo, "The Boundaries", *supra* note 443 at 19: "Even where we know intellectually that we're interacting with an image or a machine, our brains are hardwired to respond as though a person were actually there. This reaction includes the feeling of being observed or evaluated. People pay more for coffee on the honor system, for instance, if eyes are depicted over the collection box. Our attitude, behavior, even our physiology can and does change in circumstances where no real person is there."

[1239] Although there is a different kind of harm that may result from the fact that an individual is monitored without his or her knowledge. This last kind of harm is of a dignitary type, and is further discussed in section 3.1.1.1.2 entitled "No Knowledge of Collection: Dignitary Harm".

[1240] Westin, *Privacy and Freedom*, *supra* note 45; See also Council of Europe, *Report on human rights*, *supra* note 42 at s. III, para. 3-6.

[1241] See Van Den Hoven & Vermaas, *supra* note 1036 at 290-91.

(the feeling of being observed or under surveillance) was not specifically addressed by DPLs, as further discussed in section 3.1.1.2.2.

At the time, the main concern was that, more and more, personal information was to be collected using an impersonal method (for instance using computers and databanks).[1242] It is reasonable to maintain that the FIPs regulating the activity of "collection" were in fact aiming in part at promoting transparency. Given that the harms triggered by the activities of "using" personal information or "disclosing" this information are more easily addressed by DPLs than the mere "collection" of information,[1243] a concurrent goal when regulating the activity of "collection" was arguably to limit the circulation of personal information and therefore, the risks of harm that individuals could sustain as a result of the "use" and "dissemination" (disclosure) of their personal information. One way to limit this circulation was to ensure that organizations would not be able to collect personal information in excess of what was necessary for the initial intended purpose, as detailed below.

(b) Upon an Excessive Collection

There is another category of harm that results when the collection of personal information is deemed to have become excessive. Individuals will, as a matter of fact, react negatively to a collection that seems to be irrelevant for the organization collecting it. This concern is not a new one. Documents from the early 1970s produced in the context of the adoption of DPLs, such as the Report of the Secretary's Advisory Committee on Automated Personal Data Systems in the U.S., raise this very issue:

[1242] U.S. Department of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *supra* note 57 at Appendix B, "Computers and Privacy": The Reaction in Other Countries: "Concern about the effects of computer-based record keeping on personal privacy appears to be related to some common characteristics of life in industrialized societies. In the first place, industrial societies are urban societies. The social milieu of the village that allowed for the exchange of personal information through face-to-face relationships has been replaced by the comparative impersonality of urban living. Industrial society also demands a much more pervasive administration of governmental activities-the collection of taxes, health insurance, social security, employment services, education-many of which collect and use personal data in an impersonal way."

[1243] See section 3.1.1.2.2 entitled "Surveillance: Dataveillance not Specifically Addressed" which details why DPLs are not properly addressing the harm triggered by the surveillance, monitoring or tracking of individuals.

> "The personal data that organizations collect for administrative purposes should be limited, ideally, to data that are demonstrably relevant to decision making about individuals. A substantial amount of personal data, however, appear to be collected because at some point someone thought they might be "useful to have," and found they could be easily and cheaply obtained on an application form, or some other record of an administrative transaction. (….) We found that decisions to collect personal data are being made without careful consideration of whether they will in fact serve the purposes for which they are supposedly being collected."[1244]

In his taxonomy of privacy harm, Solove refers to these types of harms as "interrogation", defined as the pressuring of individuals to divulge information,[1245] and "identification", a type of harm resulting from the association of data with a particular human being.[1246] As an illustration of the type of harm resulting from an excessive collection under "interrogation", Solove brings up the loud public outcry when the U.S. census began including more and more questions relating to personal affairs, such as marital status, literacy, property ownership, health, and finances in the late nineteenth century.[1247] A similar issue came up recently in Quebec, when it was requested by some that the 2011 form pertaining to the census should be shorter than the previous forms, arguing that longer forms were triggering an excessive collection, in breach of the privacy of the individuals concerned.[1248]

[1244] U.S. Department of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *supra* note 57 at s. IV.

[1245] Solove, "A taxonomy", *supra* note 339 at 500: "When asked a probing question that people find unwarranted, a frequent response is a snippy reply: 'None of your business!' Why do such questions evoke such a response? Why do people take offense even at being asked certain questions—let alone being compelled to answer them? Understood broadly, these examples all involve a similar practice—what I call 'interrogation.' Interrogation is the pressuring of individuals to divulge information."

[1246] *Ibid*. at 499.

[1247] An editorial in *The New York Times*, as well as editorials in other papers, decried, in the 1870s, the "inquisitorial" nature of the census. See Robert Ellis Smith, *Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet* (Privacy Journal, 2000), discussed in Solove, "A taxonomy", *supra* note 339 at 499. See also Solove, "Privacy", *supra* note 1 at 1401.

[1248] Radio-Canada, "Le questionnaire court reste obligatoire" (30 June 2010), online: Radio-Canada.ca <http://www.radio-canada.ca/nouvelles/National/2010/06/29/003-recensement-fin-obligation.shtml>; Radio-Canada, "Québec désapprouve à son tour" (15 July 2010), online: Radio-Canada.ca <http://www.radio-canada.ca/nouvelles/National/2010/07/15/003-recensemement-opposition-qc.shtml>. The government argued that the long version of the form was very useful for the government and that few Canadians had in fact complained about their privacy. See Radio Canada, "Trois plaintes en dix ans" (15 July 2010), online : Radio-Canada.ca <http://www.radio-canada.ca/nouvelles/National/2010/07/14/004-recensement-vie-privee.shtml>.

"Identification", on the other hand, would enable an organization to verify or confirm the identity of an individual. Various organizations may request individuals to disclose their personal identification numbers (driver's license, social insurance numbers, etc.) to verify their identity. While identification has various benefits (reducing fraud and enhancing accountability) there may be strong negative reactions to identification systems since identification is "the association of data with a particular human being."[1249] Although proposed many times in various countries (including Canada), a national identification card has been explicitly rejected in light of the privacy concerns that have emerged.[1250]

The type of harm resulting from an excessive collection would also have a psychological component, in the sense that it can create some discomfort since identification would "reveal, distort, and intrude."[1251] Excessive collection creates discomfort (even if the information is barely disseminated) since it is the activity of "collecting" this data that is problematic in the first place.[1252] Excessive collection often occurs with the conscious awareness of the individual but the monitoring or collection of personal information can be clandestine. In such a case, the type of harm will be different, and mostly associated with a dignitary type of harm, as detailed below.

[1249] As Clarke observes: "In the context of information systems, the purpose of identification is more concrete: it is used to link a stream of data with a person." Roger Clarke, "Human Identification in Information Systems: Management Challenges and Public Policy Issues" (1994) 7 Info. Tech. & People 6 at 8, online: <http://www.rogerclarke.com/DV/HumanID.html>.

[1250] See Standing Committee on Citizenship and Immigration, *A National Identity Card For Canada?* (Ottawa: Communication Canada, 2003) at Appendix B ("Preliminary Research on National ID Documents in Other Countries"). Already back in 1973, it was decided in the U.S. that a standard universal identifier (SUI) should not be established now or in the foreseeable future. See U.S. Department of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *supra* note 57 at s. IV.

[1251] Solove, "A taxonomy", *supra* note 339 at 513.

[1252] *Ibid*. at 500. Solove also suggests that collection excessive information can create harm, the intensity of which is in direct link with the degree of coerciveness involved: "People take offense when others ask an unduly probing question—even if there is no compulsion to answer. One explanation may be that people still feel some degree of compulsion because not answering might create the impression that they have something to hide. (…) Interrogation forces people to be concerned about how they will explain themselves or how their refusal to answer will appear to others. Interrogation resembles intrusion in its invasiveness, for interrogation is a probing, a form of searching."

3.1.1.1.2. No Knowledge of Collection: Dignitary Harm

In 1972, the Scottish *Report of the Committee on Privacy* mentioned that in some cases, it had recommended creating a new offence dealing with emerging threats to privacy resulting from new technical surveillance devices.[1253] A growing concern at the time was that numerous sophisticated electronic devices had been invented and marketed, that greatly increased the possibilities of surreptitious supervision.[1254] In Quebec, prior to the adoption of the 1993 Quebec DPL, the parliamentary debates also discussed the fact that certain information could be collected through illegitimate methods, in some cases even without the knowledge or proper consent of the relevant individuals, such as through the collection of fingerprints, using lie detector tests, or other digital surveillance devices or even through hypnosis.[1255]

As discussed in section 3.1.1.1.1, the "knowledge" of the collection of information or the belief that one is being monitored is quite important in order for some type of subjective harm to take place.[1256] Philosopher Stanley Benn argues that surveillance is a *prima facie* wrong, whether overt or covert, for it demonstrates a lack of respect for its subject as an autonomous person.[1257] As a matter of fact, the type of harm resulting from the "collection" of personal information (or monitoring) of an individual without his knowledge is something that has to do with his dignity.[1258] Aggregation of

---

[1253] *Report of the Committee on Privacy*, *supra* note 3 at 202-03, para. 655.

[1254] *Ibid*. at 6, para. 18: "To some extent the new public concern on this subject is the direct result of new technological developments. Numerous sophisticated electronic devices have been invented and marketed, which greatly increase the possibilities of surreptitious supervision of people's private activities and of spying upon business rivals."

[1255] See *Les travaux parlementaires*, 34th législature, 2nd session, Commission permanente de la culture, cahier no 11 (February 23, 1993), at 66.

[1256] See also Calo, "The Boundaries", *supra* note 443 at 16.

[1257] Stanley I. Benn, "Privacy, Freedom, and Respect for Persons" in J. Roland Pennock & John W. Chapman, eds., *Nomos XIII: Privacy* (New York: Atherton Press, 1971) at 7 discussed in Solove, "A taxonomy", *supra* note 339 at 494.

[1258] Dignitary harm would be affecting individuals which are not aware of the fact that personal information is or may be collected about them. Conseil de l'Europe, *L'autodétermination informationnelle*, *supra* note 20 at 25: "L'invocation de la dignité humaine entend rappeler que l'Homme est un sujet et ne peut être ramené à un simple objet de la surveillance et du contrôle d'autrui. (…) Les systèmes d'information réalisent de manière croissante une surveillance globale des populations et des individus, créant un système de transparence des comportements des personnes qui peut s'avérer contraire à la dignité humaine."; See also Kang, *supra* note 734, (quoting Stanley I. Benn, "Privacy, Freedom, and Respect for Persons" in Ferdinand David Schoeman, ed., *Philosophical Dimensions of Privacy* (New York: Cambridge University Press, 1984) at 227. Kang argues that surveillance is an attack on human dignity, interfering

information[1259] can also cause similar dignitary harms because of how it unsettles the expectations of individuals that there are certain limits on what is known about them and on what others will find out.[1260]

Evidence produced in court that has been collected by hidden surveillance cameras is often rejected, such as in Quebec or in France, as this evidence is usually considered to have been obtained in breach of basic rights and freedoms (and that the use of this evidence would therefore tend to bring the administration of justice into disrepute).[1261] This illustrates that even covert collection of *personal information* may be problematic and create some type of harm, although it is a different kind of harm, and more of a dignitary one.[1262]

In the 1970s, in the context of the increase in the number of computers and electronic databanks used by organizations, DPLs were adopted with certain principles or provisions that were supposed to address the concerns pertaining to the collection of

---

with free choice because observation "brings one to a new consciousness of oneself, as something seen through another's eyes."

[1259] See section 1.2.3.2 entitled "Extensive Data-mining Capabilities" which elaborates on the issues pertaining to aggregation.

[1260] Aggregation upsets these expectations, because it involves the combination of data in new, potentially unanticipated ways to reveal facts about a person that are not readily known. See Solove, "A taxonomy", *supra* note 339 at 507.

[1261] In Quebec under article 2858 C.c.Q.: "The court shall, even of its own motion, reject any evidence obtained under such circumstances that fundamental rights and freedoms are breached and that its use would tend to bring the administration of justice into disrepute. The latter criterion is not taken into account in the case of violation of the right of professional privilege." See for example Quebec decisions (rendered by courts and arbitrators) in which employers had difficulty in using evidence obtained by covert surveillance cameras: *Syndicat des employées et employés professionnels et de bureau and others*, D.T.E. 2009T-170**;** *Syndicat des travailleuses et travailleurs du CSSS du Sud de Lanaudière (CSN) and others*, D.T.E. 2009T-253; *Syndicat des fonctionnaires municipaux et professionnels de la Ville de Sherbrooke et Sherbrooke (ville de),* D.T.E. 2009T-309; *Syndicat des employées et employés de métiers d'Hydro-Québec, section locale 1500 – SCFP (FTQ) et Hydro-Québec*, D.T.E. 2009T-273; and *Groupe Champlain inc. (Gatineau) et Syndicat québécois des employées et employés de service, section locale 298* (FTQ), D.T.E. 2009T-431 (tribunal d'arbitrage). In France, any surveillance must comply with the French labor Code L.1221-6 du Code du travail, article 6 (3) of the French DPL and the recommandations on surveillance issued by the CNIL (such as the ones entitled "La vidéosurveillance sur les lieux de travail", online : <http://www.cnil.fr/la-cnil/actu-cnil/article/article/la-videosurveillance-sur-les-lieux-de-travail/>) otherwise, evidence collected will be found illegal.

[1262] Various jurisdictions, including France and Canada are prohibiting the surveillance, tracking or the monitoring of individuals (and therefore addressing this kind of dignitary harm) by laws, regulation and guidelines, which are different than DPLs. See section 3.1.1.2.2 entitled "Surveillance: Dataveillance not Specifically Addressed" which elaborates on this issue and explains how DPLs were not meant to address the harm triggered by the surveillance of individuals.

personal information. I maintain that regulating this activity makes less sense in light of recent technological advancements as further discussed below.

3.1.1.2. Original Purpose Behind Regulating the Collection of Personal Information

As already mentioned, the discussions that took place in most of the industrialized world around the late 1960s and early 1970s revolved around the following themes: loss of individuality, loss of control over information, the possibility of linking data banks to create dossiers, and rigid decision making by powerful, centralized bureaucracies.[1263] These discussions prompted official action by various governments and other transnational or international organizations. Regulating the manner in which information could be gathered (the activity of "collecting" personal information) seemed necessary.

The documents leading to the adoption of the first DPLs demonstrate how the purposes of regulating this activity was really two-fold: (i) to prevent the use of improper methods of collection, such as the collection of information without the knowledge or consent of individuals;[1264] and (ii) to limit the circulation of information that could end up in the hands of organizations, therefore, concurrently limiting that this information be eventually "used" or "disclosed" in a harmful way to individuals.[1265] Documents from the early 1970s produced in the context of the adoption of the FIPs, such as the Report of the Secretary's Advisory Committee on Automated Personal Data Systems in the U.S., already mentioned a concern that personal information collected without a legitimate purpose could end up in the hands of organizations, which could then "use" it for new harmful purposes:

> "Most disturbing of all, we found that personal data in excess of those clearly needed for making decisions about individuals are sometimes

---

[1263] U.S. Department of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *supra* note 57 at Appendix B, "Computers and Privacy": The Reaction in Other Countries.

[1264] See Council of Europe, *Explanatory Report: Resolution (73) 22*, *supra* note 56 at para. 22.

[1265] Council of Europe, *Report on data processing*, *supra* note 66 at s. II, s. 2, para. 1.

> collected in a way that makes them seem prerequisite to the granting of rights, benefits, or opportunities."[1266]

Therefore, limiting the amount of information collected and, along with it, the possibility of having organizations "use" personal information for new and undisclosed purposes was to be addressed by regulating the activity of "collecting" information.

3.1.1.2.1. DPLs Regulating the Collection and Recent Challenges

DPLs have come up with two sets of provisions to address the two main concerns mentioned above which are discussed below. As further discussed in section 3.1.1.2.2 below, the type of psychological harm triggered by the feeling of being under surveillance was not specifically addressed by DPLs.

(a) Knowledge and Transparency

First, in order to promote the knowledge and transparency pertaining to the collection of information, DPLs usually oblige the organization to disclose the collection and obtain the consent of individuals and often favour the collection made directly from individuals as detailed below. While DPLs have attempted to address the lack of transparency and the impersonal way of collecting personal information by enforcing disclosures and consent requests, the "notice and choice model" has proven to be defective in light of modern technologies, as further discussed in section 2.1.1.2. Organizations usually inform individuals about their collection practices by disclosing their privacy policies. More than ever before, these policies are creating a lack of transparency in terms of the kind of information collected, by who and for what purpose. I elaborate in section 2.1.1.2.1 how with the volume of data exchanges and collections taking place in today's world, individuals would be faced with the prospect of constantly reviewing privacy policies and consenting to them throughout any given day; how these notices are often difficult to read and understand; and how since these notices are drafted in very broad terms regarding their use and the sharing of the data collected, users end up granting a wide array of permissions through privacy policies that they haven't read.

[1266] U.S. Department of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *supra* note 57 at s. IV.

To make matters worse, in many cases information is collected online and offline instantaneously and invisibly.[1267] According to Lawrence Lessig: "Data is collected but without your knowledge. Thus you cannot (…) choose whether you will participate in or consent to this surveillance (…) Nothing reveals whether you are being watched, so there is no real basis upon which to consent."[1268] New types of data and new types of collection tools are becoming more complex, creating additional challenges. This means that the potential risks posed by online behavioural tracking and advertising practices are not known to most individuals. Also, the aggregation of information may create even more concerns.[1269]

In order to ensure that individuals are aware of the kind of information being collected about them (therefore addressing transparency concerns) certain DPLs prohibit the collection of personal information from other sources than the individual (unless prior consent is granted). In Quebec, information may only be collected from a third person if the law so authorizes it or if the organization collecting the information has a serious and legitimate reason for doing so.[1270] In Alberta, the organization collecting personal information from a third party without the consent of the individual has certain

---

[1267] For instance, when the consumer browses for products and services online, advertisers might collect and share information about the consumer's activity, search history, websites visited, etc. When participating in an OSN, third-party applications are likely to have access to the user's information pertaining to his posts. When using location-enabled devices, various third party application providers and entities might have access to the consumer's precise whereabouts. If a consumer uses loyalty cards at a grocery store or sends in a product warranty card, his name, address, and information about his purchase may be shared with data brokers and combined with other data. See section 2.1.1.2.2(c) entitled "Technology Becoming Increasingly Sophisticated" which elaborates on the fact that individuals don't always understand why types of tools are collecting what kind of information about the due to the sophistication of recent technologies.

[1268] Lawrence Lessig, "The Law of the Horse: What Cyberlaw Might Teach" (1999) 113 Harv. L. Rev. 501 at 505: "If you walked into a store, and the guard at the store recorded your name; if cameras tracked your every step, noting what items you looked at and what items you ignored; if an employee followed you around, calculating the time you spent in any given aisle; if before you could purchase an item you selected, the cashier demanded that you reveal who you were – if any and all of these things happened in real space, you would notice. You would notice and could then make a choice about whether you wanted to shop in such a store. (…) In cyberspace, you would not. You would not notice such monitoring because such tracking in cyberspace is not similarly visible."

[1269] An individual may agree to the collection of an insignificant piece of information here or there, as it does not reveal or compromise their identity. However, the same individual may be alarmed to see what can happen once that insignificant morsel of data is aggregated or combined with other fragments of information. See section 1.2.3 entitled "New Identifying Methods" which elaborates on this issue.

[1270] Quebec DPL, *supra* note 110 at s. 6.

obligations to ensure the legitimacy of the collection.[1271] In Europe, the Directive 95/46/EC states that if the personal data has not been collected from the individual, certain information should be disclosed to the individual at the time of disclosure by the third party.[1272] Although these provisions have been adopted to ensure that individuals would be aware of what information is collected about them and by whom, the goal of transparency is once again no longer addressed within these provisions.

There is a huge amount of personal information readily available (sometimes even publicly available).[1273] The idea of having organizations collect personal information directly from individuals to limit the circulation of information made sense at a time when information was not already in such wide circulation. This availability results from the web, from the emergence of new technological tools to collect information (sometimes without the knowledge of individuals), from the fact that it is now possible to aggregate data from various sources (including from public sources), that it is more easy than ever to obtain information from third parties and that individuals themselves disclose tons of personal information online, through various blogs and OSNs. An organization may now be tempted to collect personal information from these sources instead of directly from individuals. Because of the amount of information publicly available, certain DPLs have even made it a point to exempt data publicly available from the applicability of DPLs.[1274]

Section 2.1.1.2 already explores the problems with the choice and model approach, which is not a particularly efficient nor realistic tool to address the concerns pertaining to the risk of harm resulting from the collection of information which were meant to be addressed by DPLs. Daniel J. Weitzner, a senior policy official at the National Telecommunications and Information Administration of the Commerce Department has suggested that “There are essentially no defenders anymore of the pure notice-and-

---

[1271] Alberta DPL, *supra* note 114 at Part 2, Division 3, s. 13 (3).

[1272] EC, *Directive 95/46/EC*, *supra* note 99 at art. 11 (1).

[1273] See section 1.2.1 entitled “Increase in Volume of Information” and more specifically, section 1.2.5 entitled “Increased Availability of Data” for details on this issue.

[1274] See section 3.1.2.2.3(a)(i) entitled “Publicly Available Information”, which elaborates on this issue.

choice model (…) It's no longer adequate."[1275] He proposes that Congress and the FTC should be looking at further rules that could limit how personal information is "used".

Since most collection activities take place without the knowledge of the consumer, the notice and consent model found in DPLs does not address the transparency concerns involved in regulating the activity of "collection". As further discussed in sections 2.1.1.2 and 2.2.1.5, I am not suggesting to completely abandon the "notice and choice" model but I am proposing to reassess using the notice and choice approach to data handling activities which were not meant to be protected under DPLs and to have a consent threshold in line with the risk of harm that a certain collection, use or disclosure may trigger.

There exists a whole other set of provisions found in DPLs that were meant to limit the circulation of information directly at the point of collection. These provisions are discussed below.

(b) Restriction on Excessive Collection

To limit the circulation of information that can end up in the hands of organizations (therefore, concurrently limiting that this information be eventually "used" or "disclosed" in a harmful way to individuals), DPLs usually prohibit the collection of unnecessary information.

First, most DPLs specify that it is illegal to provide a service *in exchange for personal information*. More specifically, under PIPEDA, principle 4.3.3 states that an organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that "required" to fulfill the explicitly specified and legitimate purposes.[1276] A similar principle can be found under articles 5 and 9 of the Quebec DPL.[1277] An organization may not "refuse to respond to a request for goods or services (…) by reason of the applicant's

[1275] Lohr, "Redrawing", *supra* note 538.

[1276] PIPEDA, *supra* note 63 at principle 4.3.3.

[1277] Quebec DPL, *supra* note 110 at ss. 5, 9.

refusal to disclose personal information except where collection of that information is *necessary*".[1278] The Civil Code of Quebec ("C.c.Q.") also provides that an organization establishing a file on an individual may only gather information that is "relevant" to the stated objective of the file.[1279] In France, there is also a similar "relevancy" or "necessary" requirement.[1280]

Online services, information, and entertainment are offered freely to consumers as far as they accept to be subjected to a certain degree of advertising and behaviour tracking.[1281] Some even raise the fact that among consumers, there seems to be a growing and implicit understanding that the use of their personal information is intrinsic to the provision of most online (and an increasing number of offline) services.[1282] This means that these kinds of provisions found in DPLs, which were meant to restrict the circulation of information, make much less sense in light of new Internet technologies and the emergence of new types of business models.[1283]

As discussed in section 1.2.4.1, in Canada, in the recent CIPPIC complaint against Facebook, one of the main issue was the argument that since users were not allowed to opt out of Facebook Ads, Facebook was unnecessarily requiring users to agree to such ads as a condition of service, in violation of principle 4.3.3 of PIPEDA.[1284] The finding of the privacy commissioner took into account the fact that the site is free to users and that since advertising is essential to the provision of the service, individuals who wish to use the service must be willing to receive a certain amount of advertising.[1285] Since advertisers may play a significant sponsorship role in the

---

[1278] *Ibid*. at s. 9 (3) states that: "in case of doubt, personal information is deemed to be non-necessary".

[1279] Art. 37 C.c.Q.

[1280] *Loi informatique et liberté*, *supra* note 131 at c. II, s. 1, art. 6 (3).

[1281] See section 1.2.4.1 entitled "New Business Models (Customization and Sponsored Services)" which discusses new types of business models on the web and the fact that various organizations may wish to use analytic tools to improve their products and services.

[1282] Robinson et al., *supra* note 151 at 4 which refers to the 2008 Eurobarometer results, published online: <http://ec.europa.eu/public_opinion/archives/flash_arch_en.htm>.

[1283] See section 1.2 entitled "Technological Background Affecting Personal Information" and more specifically section 1.2.4 which elaborate on this issue.

[1284] OPCC, *PIPEDA Case Summary #2009-008*, *supra* note 288.

[1285] *Ibid*. at s. 3, Finding 131: "Facebook has a different business model from organizations we have looked at to date. The site is free to users but not to Facebook, which needs the revenues from advertising

financing of mobile data services, this finding may also have an impact in the mobile space.[1286] In light of this, it is reasonable to argue that these kinds of provisions (no service or product in exchange of personal information) makes much less sense with the emergence of the Internet and that it becomes more difficult to justify regulating the activity of "collecting" personal information on the web.

To limit the circulation of information that can end up in the hands of organizations, DPLs also usually prohibit the collection of information that is not "necessary". Under PIPEDA, organizations shall collect only information "necessary" for the purposes identified[1287] and the data collected shall not be routinely updated "unless such a process is necessary to fulfill the purposes for which the information was collected."[1288] The TJX security breach case illustrates an example of excessive data collection for "identification" purposes. In the TJX case, data protection officers discovered that Home Sense was illegally collecting the driver's license numbers of its customers, upon the return of merchandise, for identification purposes.[1289] In Quebec, there is a similar principle and only the "information necessary" for the object of the file can be collected.[1290] In Alberta and B.C., there is a more general "reasonableness test": an organization may collect personal information only for purposes that are

in order to provide the service. From that perspective, advertising is essential to the provision of the service, and persons who wish to use the service must be willing to receive a certain amount of advertising."

[1286] Wireless devices are powerful communication devices with respect to immediacy, interactivity and mobility and can act as very powerful marketing communications devices. Advertisers may wish to sponsor content alerts and location-specific services which may include traffic, navigation information, proximity and directory or information services, mobile gaming, mobile-commerce and shopping support, mobile dating services and buddy lists. See Gratton, *Internet and Wireless Privacy*, *supra* note 193 at 21-29.

[1287] PIPEDA, *supra* note 63 at Schedule 1 (s. 5), principles 4.2.2, 4.4, and 4.4.1.

[1288] *Ibid*. at Schedule 1 (s. 5), principle 4.6.2.

[1289] The OPCC and the Alberta OPC did a joint report following this breach. See OPCC & Office of the Information and Privacy Commissioner of Alberta, *Findings under the Personal Information Protection and Electronic Documents Act (PIPEDA): Report of an Investigation into the Security, Collection and Retention of Personal Information, TJX Companies Inc. /Winners Merchant International L.P.* (25 September 2007), online: <http://www.priv.gc.ca/cf-dc/2007/TJX_rep_070925_e.cfm>. The main concern was found to be that such activity may go against certain DPL principles under which only "necessary" and "non excessive data" for the purpose identified may be collected by organizations.

[1290] Quebec DPL, *supra* note 110 at s. 5.

reasonable.[1291] In France, consistent with the Directive 95/46/EC on this matter,[1292] only relevant and non-excessive data may be processed.[1293]

Nowadays, people often have no other choice but to provide their personal information if they want to benefit from various public sector and private sector services. They must often disclose their personal information to gain employment, procure insurance, obtain a credit card, etc.[1294]

A main goal of DPLs limiting the kind (and volume) of information which may be collected was to avoid an excessive collection of data.[1295] Logically speaking, as data circulates in greater volume, the prospect of the "use" or "disclosure" of this data without the consent or knowledge of the relevant individuals tends to increase.

Organizations active in the online world are collecting new types of data using new types of collection tools.[1296] The data collected may be used for various purposes.[1297] Many websites and online service providers warn users through their privacy policies that they may collect some type of information in order to "improve their websites,

---

[1291] Alberta DPL, *supra* note 114 at Part 2, Division 3, ss. 11 (1) and (2); B.C. DPL, *supra* note 115 at Part 4, s. 11.

[1292] EC, *Directive 95/46/EC*, *supra* note 99 at art. 6 (1) (c).

[1293] *Loi informatique et liberté*, *supra* note 131 at c. II, s. 1, art. 6 (3).

[1294] Pomerance, *supra* note 233 at 284: "To make matters worse, it is impossible to sidestep this reality as a functioning member of society. Many daily activities require, as a condition precedent, that we surrender personal information about ourselves. For example, anyone who has tried to function without a credit card can attest to the difficulties they have encountered in accomplishing such basic tasks as booking a hotel room." See also Waldo, Lin & Millet, *supra* note 6 at 3: "To an unprecedented degree, making personal information available to institutions and organizations has become essential for individual participation in everyday life. These information demands have increasingly appeared in licensing; administration and conferring of government or private sector benefits to particular classes of people (e.g., veterans, the unemployed, those with low income, homeowners); providing of services; employment; and retailing". In the context of many online or offline services which would only be provided after sufficient personal data is released, with the consequence of the refusal of the providing of important services are denied if individuals are unwilling to supply that data, it is difficult to claim that individuals still have a real choice. See also Robinson et al., *supra* note 151 at ix.

[1295] I argue that these kinds of provisions were initially adopted mostly to limit the circulation of information. See section 3.1.1.2 entitled "Original Purpose Behind Regulating the Collection of Personal I" which elaborates on this issue.

[1296] See section 1.2.2 entitled "New Types of Information and Collection Tools" which elaborates on this issue.

[1297] See section 1.2.4 which elaborates on this issue.

products or services."[1298] It is not clear whether any service provider (online, mobile or other) can legally collect data for the purpose of better understanding their customers' behaviour if they are not providing "free" services.[1299] They may wish to collect user data through data mining, analytics and similar tools or calculations, in order to capture, analyze and correlate the data to uncover hidden patterns in the otherwise raw information. This may assist them in determining future behaviors and identify different trends and patterns over time from large amounts of data sometimes from disparate sources. This may also enable them to manage the wealth of information strategically, capitalize on the information collected and optimize the value of each customer.

The knowledge gained by organizations using analytics solutions (along with a better understanding of user behaviour) may in certain cases be translated into direct or indirect benefits for consumers. Direct benefits would include personalized services, products and advertising where online businesses may be in a position to offer the right services to the right users at the right time.[1300] Indirect benefits may include organizations upgrading their current products and services based on their users' needs, developing and deploying new applications and services or the "repackaging" of certain products and services.[1301] Online tracking tools enable websites and other online service providers to gather information to track user behaviour in order to implement personalized advertising. It is not always clear whether personal information collected in order to improve the organization's products and services is "required",

---

[1298] See Amazon.ca Privacy Notice, *supra* note 449: "We use the information you provide for such purposes as (…) customizing future shopping for you, improving our stores (…)."; See Microsoft privacy policy, *supra* note 297 which states: "Microsoft collects and uses your personal information to operate and improve its sites and services. These uses may include (…) performing research and analysis aimed at improving our products, services and technologies."; See Google privacy policy, *supra* note 297 which states: "We use the information we collect from all of our services to provide, maintain, protect and improve them, to develop new ones."; See Yahoo! Privacy Policy, *supra* note 228 which states: "Yahoo! uses information for the following general purposes: to customize the advertising and content you see, (…) improve our services (…)."

[1299] At least in Canada, if we follow the position of the OPCC in the Facebook finding discussed in section 1.2.4.1 entitled "New Business Models (Customization and Sponsored Services)".

[1300] This may potentially result in reduced costs for these users. Personalizing certain products and services may also improve the users' experience in the online and mobile world.

[1301] This could mean that their users may only be charged for the services that they actually use instead of sponsoring other users' usage of certain services that they have no interest for.

"necessary" or "relevant" in accordance with Canadian or French DPLs, especially since certain jurisdictions (for instance, the *Commission d'Accès à l'information* in Quebec also known as the "CAI") has interpreted this "necessity" principle quite restrictively.[1302]

While it is debatable whether it is "necessary" to collect data for "analytic" purposes, the resulting harm inflicted on the average user may be minimal.[1303] This, once again, illustrates how the provisions found in DPLs that regulate the activity of "collecting" personal information may be creating more problems than they are solving. This is especially true if we consider that DPLs don't address the main type of harm resulting from the collection of personal information. Under the proposed approach, this kind of collection or use of information for analytic purposes may be acceptable and not covered under DPLs if it is not harmful to individuals. This issue is further discussed in section 3.2.3.2.3.

3.1.1.2.2. Surveillance: Dataveillance not Specifically Addressed

As illustrated above, DPLs are only addressing the types of harms pertaining to the collection of information to a limited degree. As discussed in section 3.1.1.2, the intended purpose of DPLs was to address certain types of harms detailed in section 3.1.1.2.1, namely: psychological and dignitary. However, the harm resulting from the

---

[1302] There are some Quebec decisions elaborating on this notion of "necessary" or "relevant" information. Firstly, the personal information referred to at section 5 of the Quebec DPL must be more than useful or relevant, it must be absolutely necessary for the object of the file according to *X et Ordre des comptables agréés du Québec*, AZ-95151513 (C.A.I. enquête) at 6 [*Ordre des comptables*]; According to one decision: [TRANSLATION] "In law, the word 'necessary' has a very rigorous and rigid meaning. It denotes exclusively what is absolutely indispensable. In everyday language, we have a tendency to use the word 'necessary' to denote what is simply convenient or useful. However, in law, 'necessary' means something that is absolutely indispensable, that one cannot do without." See *X. et Aventure Électronique inc.*, AZ-96151506 (C.A.I.) at 7-8 [*Aventure Électronique*]; According to Judge Filion of the Court of Quebec, "[TRANSLATION] it is not a question of determining what is necessary as such, but rather one must look, in the context of the protection of personal information, and each situation, what is necessary to accomplish each particular goal". See para. 64 from *A. v. C.*, AZ-50195726 (C.A.I.), para. 63 [*A. v. C.*]. The CAI has explained what kind of information would be considered to be "necessary" information for a landlord evaluating potential tenants. This decision illustrates that, while a landlord is justified in wanting to determine the payment habits and general behavior of candidates, the information he may collect to that end is still very limited. The information that may be collected is limited to information on the potential tenant's previous landlord – in order to verify their payment history – and only their name and date of birth – in order to complete a credit check. See *Julien v. Domaine Laudance*, [2003] C.A.I. 77 [*Julien*].

[1303] The relevant test when "using" this data collected for analytic pruposes is further discussed in section 3.2.2 entitled "Risk of Objective Harm: Criteria to Take Into Account".

constant surveillance and monitoring of individuals (or tracking) further discussed in the present section 3.1.1.2.2, is not directly and properly addressed under current DPLs, nor was it meant to be.

At the end of the 1960s, the Council of Europe released a Report on human rights and modern scientific and technological developments following two motions (1967) pertaining to new technical devices for eavesdropping and modern scientific and technological developments.[1304] This Report resulted in Recommendation 509[1305] addressed to the Committee of Ministers and requested to examine whether the European Human Rights Convention offered an adequate protection to the right of personal privacy vis-à-vis these modern scientific and technical methods.[1306] A study conducted from 1968 to 1970 in response to Recommendation 509 concluded that foremost of all privacy concerns were: the ever expanding files of personal data collected from millions of citizens, the development of automated data banks and the growing use of computers in sharing, matching, and mining data.[1307] As the growing number of automated data banks and computers represented the biggest concern for policymakers at that period (the early 1970s) most of the privacy work pursued at that time focused on this main threat, and not on the threat resulting from surveillance devices.[1308]

For instance, the Lindop Report stated that with DPLs, they did not have to define privacy since the law would be limited to "data handling activities", and would therefore not have to address other privacy problems which are unrelated to data, such as

---

[1304] See Council of Europe, *Motion for a Resolution on Human rights*, *supra* note 47. These motions were referred by the Assembly to the Legal Committee and directed to the Legal Committee. Council of Europe, *Report on human rights*, *supra* note 42; Council of Europe, 16th sitting, *supra* note 50.

[1305] Council of Europe, *Recommandation (509) 68*, *supra* note 51.

[1306] This Recommendation was addressed to the Committee of Ministers requesting to examine whether the European Human Rights Convention offered an adequate protection to the right of personal privacy vis-à-vis these modern scientific and technical methods. See Council of Europe, *Recommandation (509) 68*, *supra* note 51 at para. 8 (i).

[1307] See Council of Europe, *Report on human rights*, *supra* note 42 at s. III, para. 4-6.

[1308] As detailed in section 1.1.2.1 entitled "Initial Concern: Computers and Electronic Data Banks", the privacy work undertaken at that point aimed to address the growing number of automated data banks and computers, and resulted in the elaboration of the FIPs, which were then incorporated in DPLs.

problems of "surveillance by electronic or optical devices".[1309] It is interesting to note that in 1972, the U.K. was already recommending legislation to create a new offence to address emerging threats to privacy resulting from new surveillance devices.[1310] Given that this recommendation emerged at the same time that the FIPs were being developed, perhaps this is another indication that DPLs were not meant to address the harm caused by the monitoring of individuals.

I maintain that privacy or surveillance laws may be better suited to address monitoring practices than DPLs, such as it is currently the case in many jurisdictions. Certain jurisdictions have even gone so far as to adopt guidelines or legal provisions pertaining to the surveillance of individuals. In May of 2009, the OPCC published a document entitled "Guidance on Covert Video Surveillance in the Private Sector".[1311] In 2002 and again in 2004, the CAI (Quebec) carried out extensive policy development with regards to the use of video surveillance in the public sector.[1312] The C.c.Q. prohibits keeping someone's "private life under observation by any means."[1313] The Quebec *Act to establish a legal framework for information technology*[1314] prohibits the tracking of the whereabouts of individuals.[1315] The French labour code also prohibits the constant

---

[1309] Lindop, *supra* note 96 at 204, para. 21.27: "Although every British writer on this topic, (referring to Mark Littman, Peter Frederick Carter-Ruck & Committee on Privacy, *Privacy and the Law: a report by Justice* (London: Stevens, 1970) at para. 18; the Younger Report, para. 58; and Paul Sieghart, *Privacy and Computers* (London: Latimer New Dimensions, 1976) at ch. 1) for the past eight years, has drawn attention to the difficulty of defining privacy generally, that difficulty does not apply in the case of a statute which is confided to data handling, and which need not therefore attempt to grapple with the problems of rights of entry, intrusion into the home, surveillance by electronic or optical devices, or embarrassing press publicity."

[1310] *Report of the Committee on Privacy*, *supra* note 3 at 202-03, para. 655: "In some cases we have recommended that there should be legislation to create either a new offence in order to deal with new threats to privacy, for instance new technical surveillance devices."

[1311] OPCC, *OPCC Guidance Documents: Guidance on Covert Video Surveillance in the Private Sector* (May 2009), online: <http://www.priv.gc.ca/information/pub/gd_cvs_20090527_e.cfm>.

[1312] As for the private sector, the CAI has developed no specific policy, but does recommend that the private sector apply the guidelines established for the public sector. See the guidelines: Commission de l'Accès de l'information, *Rules for use of surveillance cameras with recording in public places by public bodies* (June 2004) available on the CAI website: <http://www.cai.gouv.qc.ca>.

[1313] Art. 36 (4) C.c.Q.

[1314] RSQ, c. C-1.1.

[1315] *Ibid*. at art. 43.

monitoring of employees at the workplace,[1316] and the CNIL recently published a guide on the use of video surveillance in the workplace.[1317] This is a clear indication that DPLs were not meant to address the kind of (psychological) harm resulting from the constant monitoring of individuals, as more adequate laws or tools (other than current DPLs) have since been adopted to regulate these activities.

As discussed in section 1.2.3, recent technological advancements are taking surveillance, monitoring and physical tracking practices to new levels.[1318] Some are referring to the new forms of monitoring or surveillance as dataveillance, a method of watching not through the eye or the camera, but by collecting facts and data, including personal information.[1319] As discussed mentioned, a type of harm according to some has to do with the online monitoring of individuals: in the event that individuals are aware of it, then the harm would be assimilated to the feeling of being under surveillance.[1320] In the context of new technologies and the Internet, this may translate into an individual feeling uncomfortable, knowing that his or her online surfing activities and habits are either monitored or recorded or an employee being aware that his or her

---

[1316] See French Labor code (Code du travail) 122-45, 121-8. No personal information of an employee or potential employee may be collected unless the individual has been made aware of the existemce of the collecting device.

[1317] CNIL, "La vidéosurveillance sur les lieux de travail", online : <http://www.cnil.fr/la-cnil/actu-cnil/article/article/la-videosurveillance-sur-les-lieux-de-travail/>.

[1318] See also Pomerance, *supra* note 233 at 277 [footnotes omitted]: "The field of electronic surveillance has (…) become much more sophisticated. According to one author: 'the line between science and science fiction is continually being redrawn'. Technology possesses a unique ability to invade a citizens' privacy in ways that were previously unimaginable. By transcending the normal limits on sensory perception, technology allows the state to see what could not previously be seen; hear what could not previously be heard and learn what could not previously be learned. Technology can transform a fluid and transient event into a permanent and reviewable record. It permeates walls, fences, and other barriers without the need for physical intrusion. As many have observed, it poses the greatest threat to privacy of all."

[1319] Roger Clarke refers to dataveillance as the "systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons"; Roger Clarke, "Information Technology and Dataveillance" (November 1987) at 3, online: <http://www.anu.edu.au/people/Roger.Clarke/DV/CACM88.html>; See also Roger Clarke, "Introduction to Dataveillance and Information Privacy, and Definitions of Terms" (16 September 1999), online <http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html>. Colin Bennett suggests that dataveillance is a term used to describe the surveillance practices that the massive collection and storage of vast quantities of personal data have facilitated. Colin J. Bennet, "The Public Surveillance of Personal Data: A Cross-National Analysis" in David Lyon & Elia Zureik, eds., *Computers, surveillance, and privacy* (Minneapolis: University of Minnesota Press, 1996) 237.

[1320] See section 3.1.1.1.1 entitled "Knowledge of Collection: Psychological Harm" which discusses this issue.

movements throughout the city are recorded through his or her mobile phone's location data tracker (GPS or other).[1321] I also discuss in section 3.1.1.1.1(a) that many are referring to the Big Brother metaphor or the Panopticon metaphor to illustrate the modern privacy concerns triggered by online monitoring practices.

The type of psychological harm triggered by the monitoring or the surveillance discussed in section 3.1.1.1.1(a) is sometimes difficult to apply in the context of new Internet technologies. This is because many users are **unaware** that they are being monitored, due either to the subtlety or complexity of the surveillance technology.[1322] The FTC, in its recent 2012 Report, states that: "the collection and commercial use of consumer data in today's society is ubiquitous and often invisible to consumers."[1323] The ensuing paranoia of being under constant surveillance can lead to dignitary harm.[1324] Certain jurisdictions are opting not to regulate online monitoring activities through the use of DPLs; an indication that other tools may be better suited for the task

---

[1321] FTC Chairman Jon Leibowitz states: "Imagine that you were walking through a shopping mall, and there was someone that was walking behind you and taking notes on everywhere you went and sending it off to every shop or anyone who was interested for a small fee. That would creep you out; that would be very disturbing, I think, for most people." See Bob Garfield, "FTC Privacy Review Could Mean Trouble for Online Marketing: A Worst-Case Scenario: Online Advertising Would Be Legislated Into Oblivion" (19 April 2010), online: AdAgeBlogs <http://adage.com/columns/article?article_id=143343>. Chris Jay Hoofnagle raises similar concerns: "Imagine being followed in a shopping mall by a marketer who watches what you browse and buy and then recommends products. You might find this useful at times, but some consumers might never want to be followed." Hoofnagle, "Machiavellis", *supra* note 498; Solove, on the issue of harm and surveillance, suggests that the fact that the monitoring is "continuous" raises additional privacy concerns: "What is the harm if people or the government watch or listen to us? Certainly, we all watch or listen, even when others may not want us to, and we often do not view this as problematic. However, when done in a certain manner—such as continuous monitoring—surveillance has problematic effects. For example, people expect to be looked at when they ride the bus or subway, but persistent gawking can create feelings of anxiety and discomfort." Solove, "A taxonomy", *supra* note 339 at 493-94.

[1322] See section 2.1.1.2.2(c) entitled "Technology Becoming Increasingly Sophisticated" which elaborates on this issue of sophisticated new technologies. Many argue that consumers are not always fully aware of the degree to which their online behaviour is tracked or that they may be under surveillance when they use their wireless phone (location tracking) or when they are shopping at a store (RFID tracking). The Article 29 Working Party has expressed great concern over the implications of such online tracking techniques, since disclosures are often not clear on these practices and their implications. See Article 29 Data Protection Working Party, *Opinion 2/*2010, *supra* note 191 at 22: "So far, the ways in which the industry has provided information and facilitated individuals to control whether they want to be monitored have failed. Notices provided in general terms and conditions and/or privacy policies, often drafted in rather obscure ways fall short of the requirements of data protection legislation. (…)."; According to the PIAC, since consumers are unaware of the extent of behavioural targeting using their personal information, this precludes any real capacity to formulate a complaint. And this would be a cruel catch-22 since PIPEDA is a complaints-driven regime. PIAC, *supra* note 448 at 5.

[1323] FTC, *Recommendations* 2012, *supra* note 381 at 2.

[1324] See section 3.1.1.1.2 entitled "No Knowledge of Collection: Dignitary Harm" which elaborates on this issue.

at hand. As a matter of fact, online tracking and behavioural practices have raised many studies and public consultations notably in Canada.[1325] In the U.S., the FTC has been proposing a "do-not-track" framework to address these concerns.[1326] Perhaps this is another illustration that DPLs (and the consent-based model) are not properly suited to address the kind of harm triggered by the online tracking and monitoring practices now taking place.

3.1.1.3. Applying the Approach to the Collection of Information

Understanding the ultimate purpose of regulating the activity of collecting personal information, along with the resulting harms, can be useful when attempting to ensure that DPLs are applied consistent with the initial intention of the legislator. The main types of harm relating to the activity of collecting personal information are, on the one hand, psychological, stemming from the collection of data (either continuous or excessive) and the dignitary type of harm resulting from the collection of information that proceeds without the knowledge of individuals. As we have seen in section 3.1.1.2.2, DPLs are not a great fit for addressing this type of psychological harm. I have also elaborated on why DPLs are ineffective when it comes to protecting the interests of individuals from a collection that takes place without their knowledge, therefore creating dignitary harm.

More often than not, the harm to individuals will take place at the "use" or "disclosure" level; as noted by the Secretary's Advisory Committee in its 1973 report on Automated Personal Data Systems.[1327] An organization collecting personal information without actually using or disclosing it may be less likely to create a concrete *risk of harm* to individuals that can be addressed with DPLs. Although the collection of personal

---

[1325] OPCC, *Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting, and Cloud Computing* (May 2011), online: <http://www.priv.gc.ca/resource/consultations/report_201105_e.cfm>.

[1326] See FTC, *Recommendations* 2012, *supra* note 381.

[1327] U.S. Department of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *supra* note 57 at s. III: "An individual's personal privacy is directly affected by the kind of disclosure and use made of identifiable information about him in a record."

information can constitute a harmful activity, not all information collection will automatically be harmful.[1328]

Since the harm resulting from the collection of information is not properly addressed in this Information Age and era of technological advancements, I argue that we should focus on regulating information that may be potentially harmful to individuals upon being used or disclosed. Section 3.1.2.1 discusses the kind of subjective harm that may take place at the "disclosure" level having to do with humiliation and embarrassment. Section 3.2.1.2 discusses the kind of objective harm that may take place at the "use" level that has to do with discrimination, a financial or economic loss or physical harm.

More data collection means "more data" in the hands of certain organizations and therefore, greater risk that this data will be either used or disclosed without the proper authorization (or the fear that a security breach may happen). This is in fact the reason behind imposing retention limits. I argue that we should focus on regulating the collection of personal information only when it creates a risk of harm relating to the "disclosure" of information, or its anticipated "use".[1329] The graphic detailed on page 247 summarized the proposed approach.

The first step in deciding whether information collected should be governed by DPLs is to determine the risk of harm that would result from the disclosure of this information; for instance, if there is a security breach and the information is disseminated to third parties or the public, as the case may be. This determination can be made by following the steps in the test detailed under section 3.1.2.2.[1330] If there is no risk of subjective harm that would result from the disclosure of information, then the information should not be governed by the relevant DPL, as there is no need to disclose its collection to the relevant individual and obtain his or her prior consent. If there is a risk of subjective

---

[1328] Solove, "A taxonomy", *supra* note 339 at 488-89: "The collection of this information itself can constitute a harmful activity. Not all information collection is harmful, but certain kinds of collection can be."

[1329] Otherwise, the information collected by organizations should not be regulated by DPLs.

[1330] For example, the fact that the information is of "intimate" nature or not, whether and the extent to which it is "identifiable" to the individual, and whether the information is readily "available" (or the extent that the information is made more available post disclosure) will all be elements that should be take into account when evaluatinh such risk of harm according to the proposed test.

harm that would result from the disclosure, then the collection should be disclosed to the relevant individuals, who should be made aware of the fact that a certain organization is collecting data, which may be harmful to them upon being disclosed.

The second part of the test relates to the intended use of the information collected. It is often the use of the data, for instance to judge or evaluate the individual, or make decisions that profoundly affect that individual's life that will create a more tangible (objective) risk of harm.[1331] The relevant test to evaluate this objective harm is further discussed in section 3.2.2. Will the use of the personal information create a palpable impact or prejudice towards the individual concerned? If the answer is negative, then the information should not be governed by the DPL and there would be no need to disclose its collection to the individual and obtain his or her prior consent. However, if the answer is positive, then the individual should be informed of the collection and consent to it.[1332]

***

Information collection creates problems often through the use or the disclosure of the information collected, as detailed in sections 3.1.2 and 3.2.2. The collection "per se" or the means by which personal information is gathered is an activity that is not as efficiently regulated by DPLs. Although the collection may increase the risk of harm resulting from the "disclosure" or "use" of the personal information, the type of harm that the collection in itself usually triggers is more likely to be associated with some type of psychological harm (such as the feeling of "being under surveillance") or some type of dignitary harm. Since DPLs were not meant to address the first kind of harm (feeling of being under surveillance), and that they have proven to be inadequate in addressing dignitary issues (through the notice and choice model) I argue that we should focus on the risks of harm which may take place at the "disclosure" and "use" levels. These types of harm are discussed next.

[1331] Also, with aggregation techniques, certain judgments, evaluations or decisions about an individual may be made based on data which is incomplete or inaccurate. See sections 3.2.2.2 entitled "Accuracy of Information Used" and section 3.2.2.3 which elaborate on the relevancy issue.

[1332] The information would also have to be accurate and relevant for the use. See section 3.2.2.2 entitled "Accuracy of Information Used" and section 3.2.2.3 entitled "Relevancy of Information Used" which elaborate on this issue.

3.1.2. Subjective Harm Resulting from the Disclosure of Information

A second activity that is regulated by DPLs is the disclosure (or dissemination) of personal information. The notion of disclosure is not specifically defined by the French and Canadian DPLs analyzed in this thesis, but it usually refers to the giving of information, the making available of information, the exchange of information or the sharing of knowledge.[1333] Solove refers to this activity as "information dissemination," where the data holders transfer the information to others or release the information, resulting in the data moving further away from the control of the individual.[1334] I also elaborate, in section 1.2.5, on the fact that in many situations, the information disclosed by a party may have in fact been already available to a certain extent, an activity which I refer to as making information "increasingly available". This activity is included as a *disclosure* for the purpose of this analysis.

Concerns about the dissemination of information are not new. As discussed earlier, Brandeis and Warren's unease at the turn of the last century regarding loss of privacy was prompted by the technological and media developments of their time. Photography allowed for an easier way of taking images of individuals and the development of a new form of sensationalist journalism (also known as "yellow journalism") led to a dramatically increased circulation of personal information.[1335] As further discussed in section 1.2.5, some argue that with information now circulating more rapidly and inexpensively than ever before, mainly due to the Internet and other modern technologies, a parallel can be made between current concerns triggered by the Internet and Brandeis and Warren's concerns.

I will first discuss the kind of concerns and harms that DPLs were initially meant to address in the context of the disclosure of personal information (particularly as a result

---

[1333] See Gautrais & Trudel, *supra* note 1 at 96-97. These authors discuss the meaning of the verb "communicating" and provide references on this issue, namely Henry Campbell Black, *A Dictionary of law* (New York: Lawbook Exchange, 1891): "Information givem; the sharing of knowledge by one with another (…)"; These authors also refer to Bryan A. Garner, ed., *Black's law dictionary*, 8th ed. (St. Paul, Minn.: Thomson West, 2004): "Communication 1. The expression or exchange of information by speech, writing, gestures, or conduct; the process of bringing an idea to another's perception. 2. The information so expressed or exchanged."

[1334] Solove, "A taxonomy", *supra* note 339 at 488-89.

[1335] See section 1.1.1.1 entitled "First Wave: Right to be Let Alone" and section 1.2.5 entitled "Increased Availability of Data" which discuss these issues.

of the proliferation of computers used by private and public sector organizations and the use of electronic databases). I will then discuss certain types of criteria that may have an impact on the risk of subjective harm resulting from the disclosure of personal information. Then, I will apply the proposed approach to practical business cases, including behavioural marketing practices.

3.1.2.1. Harm resulting from the Disclosure (1960s-1970s Concerns)

Already in the late 1960s and early 1970s, the activity of disclosing information relating to the "intimate private life" of individuals was causing important privacy concerns.[1336] As discussed at length earlier, the initial focus at the time was the protection of *personal information* contained in electronic databases.[1337] The initial concern was that the availability of personal information, and the ease with which it could be traded or disclosed, could have devastating effects on the lives of individuals. The 1972 *Report of the Committee on Privacy* (Europe*)* summarizes the three concerns pertaining to the dissemination of personal data in the context of computers, centralized databases and mass media: (i) information could be disclosed for a new purpose;[1338] (ii) personal information would be used for marketing purposes;[1339] and (iii) with mass media, intimate details of the lives of individuals could be made available to the public.[1340]

The disclosure of *personal information* is often what we have in mind when we think of "privacy". As a matter of fact, when academics attempt to define "privacy", more often than not they refer to the "disclosure" of personal information. Alan F. Westin suggests that "privacy is the claim of individuals, groups, or institutions to determine for

---

[1336] See for example documents of the early 1970s leading to the adoption of Convention 108: Council of Europe, *Resolution (74) 29*, *supra* note 13 at Principle 3 of Annex.

[1337] See section 1.1.2 entitled "Control over Personal Information and Fair Information Practices" which discusses the context of the adoption of FIPs and DPLs.

[1338] *Report of the Committee on Privacy*, *supra* note 3 at 6, para. 19: "Computers have been designed which facilitate the centralisation of information about people's private affairs and its dissemination for purposes other than those for which it was supplied."

[1339] *Ibid*.: "And, accompanying these technical developments, there has been a spectacular growth in the collection and distribution of information as a commercial activity, which has given rise to anxiety in connection with the granting of credit, mail-order business and other forms of promotion."

[1340] *Ibid*.: "Furthermore, but by no means least important, there has been a fairly steady flow of complaints about intrusions into privacy by the mass information media. (…) This may involve the reporting of intimate details of the lives of individuals which would not normally be thought of as being in the public domain."

themselves when, how, and to what extent information about them is communicated to others."[1341] According to him, the "right of individual privacy", would also be the right of the individual to decide for himself (with only extraordinary exceptions in the interests of society) when and on what terms "his acts should be revealed to the general public".[1342] Charles Fried suggests that privacy seems to be about limiting the knowledge of others about oneself.[1343] In 1967, the Office of Science and Technology of the Executive Office of the President (U.S.) in the report on "*Privacy and Behavioral Research"* articulated the view that the right to privacy was the right of the individual to decide for himself how much he will "share with others his thoughts, his feelings, and the facts of his personal life".[1344]

3.1.2.1.1. Harm Directly Linked to Disclosure: Subjective (and Psychological)

The type of harm that may result from the disclosure of personal information is subjective in nature, as it often relates to an emotional or psychological type of harm. In 1972, the Scottish Justice Committee stated that:

> "(…) the notion of privacy has a substantial emotive content in that many of the things which we feel the need to preserve from the curiosity of our fellows are feelings, beliefs or matters of conduct which are themselves irrational."[1345]

Warren and Brandeis in their famous article about privacy and the right to be let alone, referred to the disclosure of private facts in new press, contending that privacy involved "injury to the feelings."[1346] William L. Prosser ("Prosser") discusses how the common law recognizes a tort of privacy invasion in cases where there has been a "[p]ublic

---

[1341] Westin, *Privacy and Freedom*, *supra* note 45 at 7.

[1342] *Ibid*. at 373.

[1343] See Fried, "Privacy", *supra* note 79 at 482. He states that privacy is not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves.

[1344] Office of Science and Technology of the Executive Office of the President, *Privacy and Behavioral Research* (Washington, D.C.: 1967) at 8.

[1345] Justice Committee on privacy, "Privacy and the Law" at 5, para. 18, discussed in *Report of the Committee on Privacy*, *supra* note 3 at 17, para. 47.

[1346] Warren & Brandeis, *supra* note 5 at 197. See also at 198: "our system (…) does not afford a remedy even for mental suffering which results from mere contumely and insult".

disclosure of embarrassing private facts about the plaintiff".[1347] According to Calo, the subjective category of privacy harm (which is included in the activity of collecting and disclosing personal information) is the unwanted perception of observation, broadly defined.[1348] Observation may include the activity of collecting personal information but this also includes the disclosure of personal information.[1349] Calo suggests that many of the harms we associate with a person seeing us, such as "embarrassment, chilling effects or a loss of solitude", flow from the mere belief that one is being observed.[1350] Ruth Gavison ("Gavison") refers to an observation with an "inhibitive effect on most individuals that makes them more formal and uneasy."[1351] The Article 29 Working Party, when discussing serving behavioural advertising using "sensitive" data, discusses the possible "awkward situations" which may arise if individuals receive advertising that reveals, for example, sexual preferences or political activity.[1352] They therefore also refer to a type of harm which is of a subjective nature, and which has an emotional component. Recently, in *Jones v. Tsige*,[1353] the Court of Appeal for Ontario hinted that there was a subjective component to an invasion of privacy, assimilated to "distress, humiliation or anguish" (which is therefore subjective in nature). This court mentioned that "proof of harm to a recognized economic interest is not an element of the cause of action", therefore implying that a subjective kind of harm may take place upon an invasion of privacy, even in the absence of an objective (financial) harm.[1354]

In his *taxonomy of privacy,*[1355] Solove discusses the type of harm which can result from the dissemination of information; one of the broadest groupings of privacy harms according to him.[1356] Solove includes the following harms in this group (some of which

---

[1347] William L. Prosser, "Privacy" (1960) 48 Cal. L. Rev. 383 at 389.

[1348] Calo, "The Boundaries", *supra* note 443 at 16.

[1349] *Ibid*. Calo states that "So, too, is reading a report of their preferences, associations, and whereabouts".

[1350] Ryan Calo, "People Can Be So Fake: A New Dimension to Privacy and Technology Scholarship" (2010) 114 Penn. St. L. Rev. 809 at 842-48.

[1351] Gavison, *supra* note 1049 at 447.

[1352] Article 29 Data Protection Working Party, *Opinion 2/*2010, *supra* note 191 at 20-21.

[1353] 2012 ONCA 32 [*Jones*].

[1354] *Ibid*. at para. 71.

[1355] Solove, "A taxonomy", *supra* note 339.

[1356] *Ibid*. at 525.

are not examined in this thesis because they don't relate to DPLs specifically): breach of confidentiality, disclosure, exposure, increased accessibility, blackmail, appropriation, and distortion.[1357] His analysis suggests that the kind of harm resulting from the dissemination of information is more often than not of a psychological nature. For instance, the harm from a breach of confidence would have to do with the "feeling of being betrayed" in a relationship of trust.[1358] The disclosure of information can result in damage to the reputation of the person involved; particularly upon the disclosure of a private matter that is "highly offensive to a reasonable person" and "is not of legitimate concern to the public."[1359] Solove is of the opinion that a "disclosure" of information must result in the release of "embarrassing secrets or discrediting data" before courts will consider it to be harmful.[1360] An "exposure" involves divulging certain physical and emotional attributes about a person that people view as deeply primordial; this often creates "embarrassment and humiliation such as grief, suffering, trauma, injury, nudity, sex, urination, and defecation".[1361] According to Solove, we have developed social practices to conceal aspects of life that we find animal-like or disgusting (for example: nudity or going to the bathroom).[1362] Individuals being "exposed" could therefore experience a severe and sometimes "debilitating humiliation and loss of self-esteem."[1363]

As already mentioned, certain Canadian jurisdictions have recently introduced breach notification obligations or intend to do so.[1364] At the federal level, Bill C-12 was

---

[1357] While the first four types of harm are included one way or another in this section 3 below, the last three types aren't because they don't relate to DPL specifically. For example, "blackmail" is usually regulated by criminal laws, "appropriation" is regulated by laws addressing one's right to his image (although which are in certain cases be indirectly related to DPL and the activity of disclosing personal information such as someone's picture) and distorsion, is usually regulated by defamation laws. See Solove, "A taxonomy", *supra* note 339 at 523.

[1358] *Ibid*. at 525.

[1359] *Ibid*. at 529.

[1360] *Ibid*. at 525.

[1361] See Anita L. Allen, "Lying to Protect Privacy" (1999) 44 Vill. L. Rev. 161 at 177: "Sex is an area in which we encounter our desires, prejudices and shame, and cloak these emotions in privacy."

[1362] Solove, "A taxonomy", *supra* note 339 at 534.

[1363] *Ibid*. at 535.

[1364] See section 2.2.1.3.2(a)(iv) entitled "Subjectivity in Security Measures to Adopt and Retention Obligations" which elaborates on the fact that Alberta has recently adopted a breach notification obligation, and that in Canada, at the Federal level, Bill C-12 proposed would also provide for an obligation to notify

introduced in 2011 proposing a new provision requiring organizations to notify the individuals involved in the event that a security breach creates "a real risk of significant harm".[1365] "Significant harm" is defined in part as including subjective types of harm such as "humiliation (and) damage to reputation or relationships".[1366] Having already adopted a breach notification obligation a few years ago, Alberta published an Information Sheet (no. 11), entitled *Notification of a Security Breach*, in April of 2010.[1367] In this document, a similar concept is defined, that of "significant harm", which also has a "subjective" component since it is defined as: "humiliation or damage to one's professional or personal reputation".[1368]

3.1.2.1.2. Harm Indirectly Linked to Disclosure of Information

Certain types of harms are associated with the potential disclosure of personal information but are not directly caused by the disclosure itself. These include the fear that personal information may be disclosed or that, once disclosed, it will be used. Another form of harm may arise when information disclosed is "used" in ways that are harmful to the relevant individuals.

(a) Fear of a Disclosure or that Information Disclosed will be Used

The fear that personal information *may* be disclosed and potentially used by third parties upon disclosure presents a psychological harm that is somehow linked to the activity of "disclosure".[1369] To illustrate this kind of harm, we can refer to the U.S. case

---

upon a security breach taking place. Quebec also intends to have such a notification obligation in the near future. See Commission d'accès à l'information du Québec, *Rapport quinquennal 2011 : Technologies et vie privée à l'heure des choix de société* (Québec: Gouvernement du Québec, 2011) at 37-42, recommandation n°7.

[1365] *Safeguarding Canadians' Personal Information Act*s, *supra* note 506 aimed to amend PIPEDA, was re-introduced by the Government of Canada on September 29, 2011.

[1366] See *ibid*. at Clause 11.

[1367] Service Alberta, *PIPA Information Sheet 11: Notification of a Security Breach* (April 2010).

[1368] *Ibid*. at 2-3.

[1369] For example, see ICO, *Data Protection Strategy*, *supra* note 986 at 7-8: "Such individual harm can present itself in different ways. Sometimes it will be tangible and quantifiable, for example the loss of a job. At other times it will be less defined, for example damage to personal relationships and social standing arising from disclosure of financial circumstances. Sometimes harm might still be real even if it is intangible, for example the fear of identity theft that comes from knowing that the security of your financial information has been compromised."

Doe v. Southeastern Pennsylvania Transportation Authority[1370] in which the plaintiff (Doe) who was HIV positive had disclosed his condition to two doctors at his work but to nobody else. His employer maintained a prescription drug program with a drug supplier. This supplier had mistakenly provided the employer with the names corresponding to the prescriptions. Doe began to fear that co-workers had found out about his condition. The U.S. court held that the constitutional right to information privacy had not been violated in this case because there was no evidence of a disclosure by the employer of confidential information to the other employees (the "fear" of a potential disclosure not being recognized as a real harm).[1371]

Personal information that has been disclosed to unauthorized third parties may then be "used" in harmful ways by these parties. For example, the disclosure of someone's location data may constitute a threat to their security, for instance victims of stalking or domestic abuse, or even police officers and prosecutors who fear retaliation from criminals.[1372] In the case of a security breach at a bank, the customers may fear that they may soon become the victims of identity theft.[1373]

It can be more difficult to link this kind of indirect harm (which is based on "the fear of harm" or potential harm caused by an eventual disclosure or use of personal information) to the specific data handling activity of disclosing information. For example, in the U.S., in *Reeves v. Equifax Information Services*,[1374] a federal trial court denied a credit agency defendant's motion for summary judgment where the alleged harm was the "emotional distress" associated with the knowledge that a credit report remained uncorrected. As a matter of fact, there was no harm directly linked with the disclosure of the credit report information (since there had not yet been a disclosure) and there was no illegal use of the information. Instead, there was a type of

---

[1370] 72 F. (3d) 1133 (3d Cir. 1995) [*Doe*].

[1371] *Ibid*. at 1139-40. Although he began to perceive that people were treating him differently, he was not fired (in fact, he was given a promotion) and he had offered no proof that anybody else knew, and accordingly, the court weighed his privacy invasion as minimal.

[1372] See section 3.2.1.2.3 entitled "Physical Harm" which elaborates on this kind of harm.

[1373] See section 3.2.1.2.1 entitled "Financial Harm (Information-based)" which elaborates on this kind of harm.

[1374] No. 09-CV-00043, 2010 BL 113325 (S.D. Miss. May 20, 2010).

psychological harm pertaining to the fear that this information, if disclosed, would be used in ways that may be harmful.

(b) Harm Caused by the Use of Information Disclosed

Information disclosed or released can be "used" in a host of unforeseeable ways that are potentially harmful to individuals.[1375] Solove argues that individuals may therefore want to protect information that makes them vulnerable or that can be "used" by others to harm them physically, emotionally, financially, and reputationally.[1376] As a matter of fact, sometimes data may be viewed as "sensitive" based on how it may be used upon being disclosed. Financial data, for instance, may easily be used to create some more objective type of harm to the individual, such as fraud or identity theft.[1377] Location information may be used by stalkers or criminals to physically harm their victims.[1378] For example, in *Remsburg v. Docusearch, Inc.*,[1379] a man obsessed with Amy Lynn Boyer purchased her Social Security number and employment address from a database company called Docusearch, went to her workplace and murdered her. The court concluded that "threats posed by stalking and identity theft lead us to conclude that the risk of criminal misconduct is sufficiently foreseeable so that an investigator has a duty to exercise reasonable care in disclosing a third person's personal information to a client".[1380]

The disclosure of information may trigger a certain type of psychological harm (section 3.1.2.1.1). However, once the information is "used", an objective kind of harm emerges

---

[1375] See section 3.2.1 entitled "Objective Harm Resulting from the Use of Information (1960s-1970s Concerns)" which elaborates on this issue.

[1376] Solove, "A taxonomy", *supra* note 339 at 530: "many people have good reason to keep their addresses secret, including victims of stalking and domestic abuse attempting to hide from those that threaten them, police officers and prosecutors fearing retaliation by criminals, celebrities desiring to avoid harassment by paparazzi, and doctors who perform abortions desiring to protect their family's safety". As an exemple, he states: "People want to protect information that makes them vulnerable or that can be used by others to harm them physically, emotionally, financially, and reputationally."

[1377] See section 3.2.1.2.1 entitled "Financial Harm (Information-based)" which elaborates on this kind of harm.

[1378] See section 3.2.1.2.3 entitled "Physical Harm" which elaborates on this kind of harm.

[1379] 816 A. (2d) 1001, 1005-06 (N.H. 2003) [*Remsburg*].

[1380] *Ibid*. at 1008. See also section 3.2.1.2.3 entitled "Physical Harm" which elaborates on this kind of harm.

which is only indirectly related to the disclosure. For instance, reputational damage is one example of a type of harm resulting from the disclosure of information which may trigger a subjective harm (embarrassment upon the disclosure) as well as more objective harm (financial, discrimination) if the information disclosed is in fact used.

Canadian courts have indirectly (somewhat instinctively) acknowledged the following distinction: subjective harm resulting from the "disclosure" of the information vs. the objective harm resulting from the "use" of disclosed information. In a few recent cases, they have refused to grant damages following illegal disclosures, because the damages related to the fact that the information was used (after it was disclosed), triggering the financial (objective) damages. More specifically, in two recent decisions rendered by the Federal Court of Canada, the court had to evaluate the damages suffered by employees dismissed as a result of a "disclosure" of personal information by a third party to the employer. In both cases, the employers based their decision on personal information disclosed to them without the consent of the employees. Although the illegal data handling activity at stake was the "disclosure" of personal information, the court felt that sufficient evidence of subjective harm was not put forward in either case; therefore, no damages were granted to the plaintiffs. In *Randall v. Nubodys Fitness Centres,*[1381] the court took the position that the financial harm claimed in connection with the dismissal was objective in nature (and therefore linked to the "use" of the information by the employer instead of being linked to the illegal "disclosure" activity).[1382] Therefore, the court refused to grant damages to the plaintiff.[1383] In the second case, *Stevens v. SNF Maritime Metal Inc.*,[1384] the Federal Court also refused to grant damages to the plaintiff, in part because while the illegal activity was in fact the "disclosure" of Stevens' personal information, his damages, instead of being subjective

---

[1381] *Randall*, *supra* note 599.

[1382] An employee who had a corporate membership in a gym discovered that the gym disclosed the frequency of his visits to the employer. After being dismissed, he felt that his relationship with his employer had become damaged by reason of this disclosure by the gym. Following the Privacy Commissioner's favourable finding, he made an application under s. 16 of PIPEDA for $85,000 in damages.

[1383] The plaintiff did not provide any evidence that the disclosure by the gym was linked to the applicant's dismissal and therefore, the court dismissed the application and Mr. Justice Mosley articulated the view that an award of damages pursuant to section 16 of the PIPEDA is not be made lightly: "Such an award should only be made in the most egregious situations. I do not find the instant case to be an egregious situation."

[1384] *Supra* note 599.

and privacy-related, were of an objective nature (financial damages).[1385] The court mentioned that the information disclosed by the third party "was not deeply personal or intimate"[1386] and that there was no evidence pertaining to the "standing or community perception or similar features of a breach of privacy claim".[1387] Instead, Stevens' damages were objective in nature (financial, caused by a wrongful termination) and therefore linked to the "use" of this information by his employer to dismiss him.

These cases illustrate the importance of properly qualifying the data handling activity triggering the risk of harm (collection, use or disclosure) and of understanding the purpose behind DPLs regulating each data handling activity. Furthermore, these cases also point to a reluctance on the part of courts to hold the initial "disclosers" of information responsible for the actions of third parties following the disclosure. One possible reason for this reluctance is that courts instinctively make the distinction between an objective harm that relates to the "use" of information and the subjective harm that relates to the "disclosure" of information.[1388]

While, in certain cases, information disclosed could be used to harm individuals (location information used by stalkers, financial information used by identity thieves, etc.), I maintain that the fact that the information is evaluated through the "availability" test detailed in section 3.1.2.2.3 should to a certain extent address these kinds of objective harms that may take place, which objective harms are usually regulated by

---

[1385] The facts of this case are as follows: an employee (Stevens) of an organization that collected and recycled scrap metal was tasked with delivering the scrap metal to a buyer on behalf of his employer. He opened a personal account with the buyer and had the proceeds of any delivery credited to his own account as opposed to his employer's. The buyer disclosed Stevens' personal account information to his employer who fired him. The Privacy Commissioner found that PIPEDA had been violated with the disclosure of Stevens' personal account information to his employer and Stevens then filed a s. 14 application seeking s. 16 damages in the amount of $148,000.

[1386] In *Stevens*, *supra* note 599, Mr. Justice Phelan states: "The Applicant's claim, in excess of $148,000, is out of proportion to the privacy invaded. The information disclosed was not deeply personal or intimate. It was commercial and the type of information frequently spoken about in a social context. Therefore, I find that the damages claimed are not those for breach of the Act but for wrongful termination. To the extent (if any) that privacy is involved, it is minimal and the Applicant has put forward no other evidence of impact on his standing or community perception or similar features of a breach of privacy claim."

[1387] See section 3.1.2.1 entitled "Harm resulting from the Disclosure (1960s-1970s Concerns" which discusses the subjective harm pertaining to a disclosure of *personal information.*

[1388] See section 3.1.2.1 entitled "Harm resulting from the Disclosure (1960s-1970s Concerns" which discusses the subjective harm pertaining to a disclosure of *personal information* and see section 3.2.1 entitled "Objective Harm Resulting from the Use of Information (1960s-1970s Concerns)" which elaborates on this risk of objective harm at the "use" level.

criminals laws (which are outside the scope of this thesis). More specifically, the fact that financial information is not already available would trigger the fact that the information would be subject to the relevant DPL, since it may trigger a risk of harm upon being disclosed.

3.1.2.2. Risk of Subjective Harm: Revisiting the Sensitivity Criteria

The type of harm arising from the disclosure of personal information has typically been addressed by DPLs: (i) providing a measure of transparency and control to individuals, through enforcing consent requests prior to the disclosure of personal information;[1389] and (ii) forcing organizations handling personal information to protect the information, using appropriate security measures that take into account the sensitivity of the information.[1390]

In order to be harmful to individuals, a disclosure of personal information would have to create some type of humiliation or embarrassment, as discussed in previous section 3.1.2.1.1. This *risk of harm* is highly contextual and can be difficult to isolate.[1391] In order to alleviate this problem, I propose three different criteria relating to the information which may be essential to the identification of this kind of harm: whether the information is "identifying" the individual and to what extent; the "intimate" nature of the information; and the extent of its "availability" to third parties or the public upon being disclosed. Before elaborating on these three criteria ("identifiability", "intimate" nature and "availability"), I will explain why I have decided to avoid using the terms "sensitive" (mentioned in several DPLs) as well as "private data".

Certain European DPLs, including the French DPL, have incorporated categories of "sensitive" data, similar to article 8 of Directive 95/46/EC.[1392] These laws all acknowledge that certain categories of personal information (more specifically the ones

---

[1389] Section 2.1.1.2 entitled "Notice and Choice Approach Challenged" which elaborates on this issue.

[1390] See section 2.2.1.3.2(a)(iv) entitled "Subjectivity in Security Measures to Adopt and Retention Obligations" which elaborates on this issue.

[1391] See section 2.2.1.4.1 entitled "Providing More Flexibility ("Privacy" and "Harm" are Contextual)" which elaborates on this issue.

[1392] See *Loi informatique et liberté*, *supra* note 131 at c. II, s. 2, art. 8 (II) (1) ; See also for example, *Loi fédérale sur la protection des données*, 235.1, 1992 (Suisse) at art. 3 [*Loi fédérale Suisse sur la protection des données*].

"revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life") are more privacy sensitive and therefore more likely to harm individuals in cases of unauthorized processing. Ohm suggests that:

> "Regulators should perhaps also take into consideration the sensitivity of the data. It makes sense to treat medical diagnoses differently than television-watching habits, for example, because the path to harm for the former is shorter and more direct than for the latter."[1393]

One could argue that since certain DPLs already provide examples of "sensitive" information, we can simply restrict the application of DPLs to cases involving such information. But what does it mean for a certain piece of data to be "sensitive" in the context of the disclosure of certain information? Sensitivity is often contextual[1394] and as a matter of fact, various academics are proposing more contextual-based approaches in order to determine the sensitivity of the data in light of the Internet and modern technologies.[1395] The Explanatory Report of the Resolution 1974, which lead to the adoption of Convention 108 in Europe, entertained the idea of placing non-sensitive or "neutral" data within the purview of DPLs.[1396] This Resolution (74) 29 suggested that the more sensitive the data, the more potential *harm* to the individual.[1397] At the same time, as already discussed in section 2.1.2.3.2, the Lindop Report concluded that the notion of data "sensitivity" was a subjective issue and that it was not possible to either simply compile a complete list of what kind of data is "sensitive" or put together

---

[1393] Ohm, *supra* note 562 at 1768.

[1394] See section 2.2.1.4.1 entitled "Providing More Flexibility ("Privacy" and "Harm" are Contextual)" which elaborates on this issue. See also PIAC, *supra* note 448 at 9. Robinson et al., *supra* note 151 at 28.

[1395] See section 2.1.2.3.2 entitled "Pre-determined Categories of Sensitivite Data Challenged" which discusses this issue.

[1396] Council of Europe, *Explanatory Report: Resolution (74) 29*, *supra* note 65 at para. 28: "Principle No. 7 - 28. This principle does not apply to 'neutral' information, which may circulate freely and to which consequently any person can have access. As a matter of fact, the proper functioning of public services may call for the free circulation of certain categories of information such as that pertaining to the identification of persons."

[1397] *Ibid*. para. 18: "Principle No. 3 18. Although the provisions of this principle should not be disregarded when non-sensitive information is being handled, the principle deals particularly with information which is inherently sensitive (for example because it relates to the individual's conduct in his own home, his sexual life or his opinions) or becomes sensitive in the context in which it is used (for example, police or health). It has been emphasised that the processing of sensitive information should be governed by special rules in view of the damage which individuals might suffer in case of misuse. (…)"

objective standards of "sensitivity".[1398] PIPEDA is consistent with the views of this report as it is much more flexible on this issue of sensitivity, when it states: "Although some information (…) is almost always considered to be sensitive, any information can be sensitive, depending on the context."[1399]

In certain situations, information will be considered "sensitive" because it may be "used" in a harmful way against individuals. This issue is discussed in section 3.2.1.2. This is simply to illustrate the fact that there is a distinction to be made between data that may be harmful upon being disclosed because it creates embarrassment or humiliation (subjective type of harm discussed in section 3.1.2.1.1) as opposed to data that is "sensitive" because it may be "used" in a harmful way.[1400]

I agree that the notion of "sensitivity" is relevant in the context of evaluating the *risk of harm* upon the disclosure of personal information, and that this risk of harm is indeed usually contextual. But I have already discussed elsewhere (see section 2.1.2.3.2) how focusing only on the nature of the information is not a viable option.[1401] I maintain that analyzing the information at stake in light of its "identifiability" to an individual, its "intimate" nature, and its "availability", is the first step in determining if the information to be disclosed is sensitive in a given context, and may trigger the subjective kind of harm discussed in section 3.1.2.1.1. The test which I propose would concurrently be useful in ensuring that DPLs protect only data that they should protect, avoiding the potential over-inclusiveness and the under-inclusiveness further discussed in sections

---

[1398] Lindop, *supra* note 96 at 153-54, para. 18.25.

[1399] PIPEDA, *supra* note 63 at Schedule 1 (s. 5), principle 4.3.4.

[1400] This issue is further discussed in section 3.2.1.2 entitled "Types of Objective Harm" which elaborates on this issue.

[1401] I already discuss in section 2.1.2.3.2 entitled "Pre-determined Categories of Sensitivite Data Challenged" how in the context of the Internet, with the increase in the volume in data exchanges and disclosures and the social changes through Web 2.0 and OSNs under which online users voluntarily disclose and share their personal information (see section 1.2 entitled "Technological Background Affecting Personal Information" which elaborates on this issue), this principle (of pre-determined categories of sensitive data) may be challenged. For example, images posted online (for example on OSNs) often reveal racial origin, and names may be typical to certain ethnicities and/or religions. A photograph showing the ethnic origin of an individual would be regarded as sensitive data irrespective of the context or purpose in which the photograph was published. See Robinson et al., *supra* note 151 at 28; See also Wong & Garrie, *supra* note 187 at 582.

2.1.2.1.1 and 2.1.2.1.2. It could be the first step towards evaluating a piece of information in its "total context", using a more complete contextual approach.[1402]

Another avenue to reducing the inclusiveness of DPLs in the context of the disclosure of personal information could be to make a distinction between "private" and "public" data. Certain authors, in an attempt to circumscribe the application of DPLs, suggest that DPLs should only apply to "private data."[1403] As already mentioned, certain DPLs have even decided to make exemptions for publicly available data which would no longer be governed by DPLs.[1404] Some have outlined the fact that this distinction "private" vs. "public" was not present in certain DPLs, implying that perhaps it should have been.[1405] As early as the 1970s, the Lindop Report suggested that: "Privateness" is clearly not an attribute of the data itself, for the same data may be regarded as very private in one context and not so private in another.[1406] Trudel agrees that the degree to which a situation is public or private varies according to the context and circumstances. He points out that some Internet interactions are public while others presuppose privacy.[1407]

[1402] See section 2.2.1.2 which discusses the difference between the proposed approach and a "contextual" approach.

[1403] See Trudel & Benyekhlef, *supra* note 367 at 12: "Ainsi, la définition des renseignements personnels assujettis à la loi pourrait se lire ainsi: 'Est un renseignement personnel tout renseignement portant sur un élément de la vie privée d'une personne.' ou encore: 'Est un renseignement personnel tout renseignement concernant une personne ou permettant de l'identifier mais qui n'a pas un caractère public.'" See also Lindop, *supra* note 96 at 153, para. 18.24: "Paragraph 37 of the White Paper invites us to say 'how personal information should be defined', and that was therefore one of the questions on which we asked our witnesses to submit their views. (..) Some attempted a distinction between (…) 'private' and 'public' information."

[1404] See section 3.1.2.2.3(a)(i) entitled "Publicly Available Information" which elaborates on this issue.

[1405] Trudel & Benyekhlef, *supra* note 367 at 3: "La loi reprend ici la définition de 'renseignements nominatifs' de l'article 54 de la Loi d'accès. Mais contrairement à l'article 55 de la Loi d'accès, aucune distinction n'est faite entre un renseignement personnel à caractère public en vertu de la loi et un renseignement nominatif. Ici, tous les renseignements personnels ont le même statut et sont protégés de la même façon."

[1406] Lindop, *supra* note 96 at 10, para. 2.07.

[1407] Trudel, "Privacy Protection", *supra* note 164 at 318-19: "In order to establish protection that balances all basic rights, we have to take into account the fact that public and private situations lie along a continuum. In cyberspace, nothing is purely public or strictly private, just as nothing is completely black or white. The degree to which a situation is public or private varies according to the context and circumstances."

While I agree that the notion of "private data" is an element to consider in the overall test to determine whether a certain disclosure of information is potentially harmful, I maintain that when we discuss the notion of "private data", we may be in fact referring to at least two different things. First we may be talking about the "nature" of the information. For example, the Lindop Report discussed drawing a distinction between what they called "public" and "private" information, with public information including matters such as the data subject's name, address, and sometimes age and marital status as well.[1408] Second, we may be talking about information that is "available" to certain individuals, or even "publicly" available. For example, in some jurisdictions, there are certain documents that are considered "public".[1409] The Lindop Report also discussed drawing a distinction between information which has at some time been "published" and information which has not.[1410]

I argue that the proposed test detailed in this section which may be used in order to determine if the disclosure of personal information may create a risk of subjective harm, will in fact take into account the two sides of this notion of "private data". The fact that the information is of an "intimate nature" is usually included in what we have in mind when we think of information that pertains to the private life of an individual. Whether the information is or is not "available" prior to a disclosure of this information is also relevant in assessing whether or not this information is "private". This criterion is

---

[1408] Lindop, *supra* note 96 at 270, paras. 31.02-31.03.

[1409] As an example, in the U.S., confidential records include tax, social welfare and criminal history records, while public records include property records, birth, death, marriage certificates, court records, motor vehicle records, and voter registration records. See Solove, "Privacy", *supra* note 1 at 1457. In Quebec, certain information is also "public" by law. See for example *An Act respecting access to documents held by public bodies and the protection of personal information,* R.S.Q., chapter A-2.1,

section 55 which states: "55. Personal information which, by law, is public is not subject to the rules for the protection of personal information set out in this chapter."

[1410] Lindop, *supra* note 96 at 270, para. 31.04: "Nor is it, in our view, helpful to draw a distinction between information which has at some time been 'published' and information which has not. Such a distinction overlooks two important facts of life: the fact that no one can know everything, and the fact that people forget even what they once knew. Many things are published in newspapers or broadcasts, but by no means everyone reads them, sees them, or hears them – or necessarily remembers them later even if he once knew them."; *Ibid*. at 270, para. 31.05: "The truth is that any piece of information about any data subject will at any given time be known only to a finite number of people. The number may be large or small, but (with very few exceptions) it will never comprise the whole of the population of the United Kingdom. Moreover, as time passes the number will necessarily become smaller – by death and by forgetting – unless the information is circulated anew. In short, personal information is not just either 'public' or 'private': there is a wide range of possible knowledge among the public for any given item."

directly linked with the kind of harm that may result upon the *personal information* being disclosed.

Nissenbaum discusses how the principle of restricting access to personal information usually focuses on data that is "intimate", "sensitive", or "confidential":

> "This principle does not focus on who the agent of intrusion is but on the nature of information collected or disseminated—protecting privacy when information in question meets societal standards of intimacy, sensitivity, or confidentiality. (…) Several prominent philosophical and other theoretical works on privacy hold the degree of sensitivity of information to be the key factor in determining whether a privacy violation has occurred or not. These works seek to refine the category of so-called "sensitive information" and explain why the sensitivity of information is critical in defending privacy against countervailing claims."[1411]

In order to address the risk of the subjective harm discussed above under section 3.1.2.1, which may be triggered by the activity of "disclosing" personal information, I argue that we need to evaluate the information at stake in light of three very specific criteria: namely whether the data to be disclosed is "identifiable" to an individual, is of an "intimate" nature, and whether it has been made "available" to others and the extent of its availability. I note that these criteria are very close to what Nissenbaum prescribes. Basically, the sensitivity of the data can be determined by the sum of the risk of harm resulting from the "identifying" aspect of the data (the more identifying to a unique individual, the greater the risk of harm), the "intimate" nature of the data (the more intimate, the greater the risk of harm), and the "availability" of the data (the less available it was pre-disclosure, and the more available it will be post-disclosure, the greater the risk of harm) upon this data being disclosed.

3.1.2.2.1. Identifiability of Information

Based on the definition of *personal information*, information is only covered by DPLs if the information in question can "identify" an individual, which is the usual metric for establishing appropriate limits within data protection regimes. I maintain that this metric

[1411] Nissenbaum, *supra* note 230 at 128.

can be over-inclusive,[1412] under inclusive,[1413] and that there are various uncertainties surrounding this notion of "identifiable individual".[1414] But I believe that this metric remains relevant when evaluating the type of harm that may take place at the "disclosure" level,[1415] although the fact that the information is "identifiable" is only one of the three criteria that are relevant when evaluating the subjective kind of harm that may take place at this level.

Section 3.1.2.1 discusses that the kind of harm that may arise following the disclosure of information is subjective and psychological, akin to feelings of embarrassment and humiliation. For this kind of harm to take place, I argue that the data disclosed must be one or all of three things: first, it must be of an "intimate nature" (section 3.1.2.2.2); second, it must have been "available" in a limited way to the party accessing it at the time of disclosure (section 3.1.2.2.2); third, it must also be able to "identify" the individual. The higher the link between the data and the "identity" of a unique individual, the higher the risk for subjective harm to arise upon disclosure.[1416]

For example, if data relating to the sexual orientation of an individual (data of an "intimate" nature) is disclosed on a public blog in Quebec, that is accessed by hundreds of thousands of individuals, the risk of harm for the individual concerned will be greater if his name and address are included or mentioned together with this information. The risk would be lower if, instead, only his name, his address or worse, only his street name (i.e. "a man living on X street is homosexual") were disclosed. In

---

[1412] Any data can technically or potentially be covered by DPLs in light of the Information Age and modern technologies since it is usually technically possible to make a link between an individual and certain data. See section 1.2.3 entitled "New Identifying Methods" and section 2.1.2.1.1 entitled "Potentially Over-Inclusive Definition" which elaborate on this issue.

[1413] See section 2.1.2.1.2 entitled "Potentially Under-Inclusive Definition" which elaborates on this issue.

[1414] See section 2.1.2.2 which elaborates on this issue.

[1415] My opinion is different when evaluating data at the "use" level. See section 3.2.2.1 entitled "Identifiability Replaced by Negative Impact (Objective Harm)" which elaborates on this issue.

[1416] But it is only one of three criteria since once could claim to feel embarrassed by very intimate information being made available to a broad group of individuals, and this, even if their identity is not known. Judge Posner in the caselaw *Northwestern Memorial Hospital v. Ashcroft*, commented on the fact that a privacy breach may still occur even if a person cannot be identified by name on the Internet. *Northwestern Memorial Hospital v. Ashcroft*, 362 F. (3d) 923 at 929 (7th Cir. 2004), Posner, J. [*Ashcroft*]: "Imagine if nude pictures of a woman, uploaded to the Internet without her consent though without identifying her by name, were downloaded in a foreign country by people who will never meet her. She would still feel that her privacy had been invaded."

this last case, the identifiability of the individual depends on how densely populated the street is. If only a handful of people live on the street in question, needless to say, the chances of identifying the person go up. However, if we are talking about Madison Avenue or Sunset Boulevard, it may be like trying to find a needle in a haystack.[1417]

The notion of "identity", which implies that personal information is in fact "identifiable", has been the subject of much debate and controversy and is interpreted differently between jurisdictions (and sometimes even within the same jurisdiction).[1418] The notion of "identifiability" is therefore a complex issue and also a subjective one. Moreover, while the European system does in fact have a test to provide guidance on what should be taken into account when determining what counts as "identifiable" information with recital 26 (contrary to Canada), the handful of cases that address the interpretation of the Directive 95/46/EC's Article 2 (a) (definition of *personal data*) in conjunction with recital 26 *"all the means likely reasonably to be used*" reveal that European courts have approached this issue in a number of ways, leading to contradictory and confusing conclusions.[1419] To add to all the uncertainty surrounding this notion of the "identifiable individual", the Article 29 Working Party also maintains that the European test is a dynamic one, and should consider the state of the art in technology at the time of the processing, and the possibilities for development during the period for which the data will be processed.[1420] All this to say that there is huge subjectivity (on top of the various

---

[1417] I realize that this notion of "identifying" and harm can be highly contextual. If this information is published on a public blog in Quebec but relates to a man located in France, then the chance of identifying this man are even more difficult (the information being released outside of this man's network), therefore greatly reducing the *risk of harm*. But things can be different if the man in question is a celebrity. Then a broader audience may actually know of him or may be interested in this information, therefore potentially increasing the *risk of harm* resulting from this disclosure. But this thesis is only discussing general criteria pertaining to the information which may be relevant in assessing this risk of harm.

[1418] See section 2.1.2.2.1 entitled "Notion of Identifiable Individual" which elaborates on this issue.

[1419] See section 2.1.2.2.1 entitled "Notion of Identifiable Individual" and section 2.1.2.2.2 "Identifying a Device or an Object" which discuss this issue. For a detailed analysis of these cases, see Lundevall-Unger & Tranvik, *supra* note 641.

[1420] Article 29 Data Protection Working Party, *Opinion 4/2007*, *supra* note 100 at 15: "Identification may not be possible today with all the means likely reasonably to be used today. If the data are intended to be stored for one month, identification may not be anticipated to be possible during the 'lifetime' of the information, and they should not be considered as personal data. However, it they are intended to be kept for 10 years, the controller should consider the possibility of identification that may occur also in the ninth year of their lifetime, and which may make them personal data at that moment. The system should be able to adapt to these developments as they happen, and to incorporate then the appropriate technical and organisational measures in due course."

uncertainties discussed in section 2.1.2.2) when having to determine whether a piece of information is "identifiable".

Various authors are proposing potential guidance on some of the issues raised above. For example, the work performed by Bercic and George is examining how knowledge of relational database design principles can greatly help to understand what is and what is not *personal data*.[1421] Lundevall-Unger and Tranvik propose a different and practical method for deciding the legal status of IP addresses (with regard to the concept of *personal data*); a test that can apply to other types of data as well.[1422] Briefly, their proposed method consists of two steps: (i) first a legality test under which illegal means of linking "names and faces" to IP addresses are not taken into account when assessing whether or not IP addresses are personal data (only legal methods of identification should form the basis of these decisions); and (ii) second, a "likely reasonable" test. More specifically, the question of *personal data* should be resolved by assessing the costs (in terms of time, money, expertise, etc.) associated with employing legal methods of identification.[1423] In a more recent article, Professors Schwartz and Solove argue that the current approaches to PII are flawed and propose a new approach called "PII 2.0," which accounts for PII's malleability.[1424] Based upon a standard rather than a rule, PII 2.0 would be based upon a continuum of "risk of identification" and would regulate information that relates to either an "identified" or "identifiable" individual (making a distinction between the two categories), and they establish different requirements for each category.

[1421] Bercic & George, *supra* note 574. These authors suggest that, in relational database theory, there would be a record structurally consisting of two parts: (i) the record identifier (primary key) and (ii) data related to it. The identifier is usually unique or full, which means that an individual is identified uniquely (e.g. name and surname, often together with added information such as residence) or a unique number such as one provided by the government. They suggest to make a distinction between "explicit" identifier (name, surname, and residence if needed) and "implicit" identifier (such as a social security number or national ID number). They suggest to also make a distinction between "full" and "partial" identifiers when qualifying data and determining whether information is "personal".

[1422] Lundevall-Unger & Tranvik, *supra* note 641.

[1423] *Ibid*. at 6: "if the costs of employing these methods are exceedingly high, then the likelihood of identifying who is using which IP address is low. Hence, IP addresses are not personal data. But if the costs are more modest, then the chance of identifying individual Internet users increases, and we should conclude that IP addresses are indeed personal data. It is our contention that this method may not only simplify the issue of IP addresses as personal data. It may also provide a general and overarching framework for evaluating the sometimes contested and uncertain relationship between natural persons, identifiability and information."

[1424] Schwartz & Solove, *supra* note 529.

My contribution in providing guidance on this notion of "identifiability" in the context of the Internet and related technologies is two-fold. First, the notion of "identifiable individual" should be interpreted differently depending on the purpose behind the data handling activity regulated by the DPLs. Regulating the "disclosure" and the "use" of personal information serve very different ends; protecting against subjective harm in the case of the former and objective harm for the latter. Accordingly, interpreting the notion of "identifiability" will vary in light of the data handling activity at stake.[1425] Secondly, when evaluating the *risk of harm* pertaining to the disclosure of personal information, we need to interpret this notion in light of the other two criteria which are relevant when evaluating the overall subjective harm following disclosure: the "intimate" nature of the information,[1426] and its "availability".[1427] For instance, the higher the risk of harm based on the previous criteria (data revealing "intimate" information which may or may not have been previously "available"), the less stringent the link between data and an identifiable individual for certain information to qualify as "personal".[1428]

For example, an organization intending to disclose information of an "intimate" nature that is not readily "available" could consider that this data is *personal information* even if the data relates to a small group of individuals (such as "the five employees using this computer") instead of a unique individual. This data ("intimate" and not "available") could also qualify as *personal information* even if the link between the data and the individual is not extremely accurate (for instance the data is a dynamic IP address which relates to one or two devices) and even if only great sums of money and efforts would need to be used in order to make a perfect and accurate link between the data and the individual (or the small group to which the data relates). I will now provide additional details on how the proposed method would actually work.

[1425] See section 3.2.2.1 entitled "Identifiability Replaced by Negative Impact (Objective Harm)" which discusses the interpretation proposed in the context of the "use" of information.

[1426] See section 3.1.2.2.2 entitled "Intimate Nature" which elaborates on this criteria.

[1427] See section 3.1.2.2.3 entitled "Availability" which elaborates on this criteria.

[1428] For instance, if the data reveals information of an "intimate" nature (for example health information), which information is not otherwise "available", then the link between a unique individual and this health information does not need to be very precise and accurate for this data to qualify as "personal". If the information evaluated is trivial (not of an "intimate" nature) and readily available, then the link between this data and a unique individual would have to be more precise and accurate in order for this information to qualify as "personal".

(a) Notion of Identifiability

I will discuss in this section whether "identifying" should be interpreted taking into account illegal methods for identifying individuals; what kind of efforts should be undertaken in order to determine if certain data is "identifiable"; and whether the potential correlation with other available or potentially available information should be taken into account.

(i) Identifying Using Illegal Methods?

An important issue is whether the data should be evaluated taking into account the possibility of an illegal act or a security breach rendering certain pieces of data "identifiable".[1429] I already discuss, in section 2.1.2.2.1(a), how this issue is not yet resolved.[1430] Taking the position that illegal means should be taken into account when evaluating if certain data qualifies as "personal" may trigger a very burdensome framework in the sense that this may lead to all kinds of data qualifying as *personal*, regardless of whether their disclosure may create a *risk of harm* to individuals.[1431]

I argue that when assessing if certain information qualifies as *personal,* one should focus on the extent of the risk of subjective harm that may arise following disclosure. This risk should then be taken into account when determining whether to consider any illegal means involved in making certain data "identifiable". For example, if the data to be disclosed is not of an "intimate" nature and is widely "available", illegal means should not be taken into account in assessing if this information qualifies as *personal information*. On the other hand, if the information is of a very "intimate" nature and is not "available", then one should be more reluctant to dismiss considering the illegal means which may be used to determine if this data is "identifiable" or not.

[1429] For instance, whether the mere possibility (such as a third party giving illegal access to identifying information) be enough to qualify strings of non identifying numbers as *personal information*.

[1430] While some (courts and authors) argue that illegal means should be taken into account when evaluating whether data is personal, others disagree and believe that illegal means of linking "names and faces" to data should never be taken into account when assessing whether or certain information is personal information and that only legal methods of identification should form the basis of these decisions. See section 2.1.2.2.1(a) entitled "Identifiable Taking Into Account Illegal Means?" which elaborates on this issue.

[1431] The consequence of having an over-inclusive interpretation of the definition of personal *information* is further discussed in section 2.1.2.1.1(d) entitled "Consequences of Over–Inclusiveness".

This question of illegal means was raised in a recent case where key-coded clinical trial data, which had been anonymized, was to be transferred from Europe to the United States. While some European agencies interpreted this as a transfer of *personal information* because the clinical trial data had not been "reversibly anonymized", or because the trial participants could be identified by the U.S. pharmaceutical company who had been in illegal contact with someone from the European clinical trial investigator, others disagreed.[1432] While the data was *identifying* for the European company, it was potentially anonymous for the U.S. based partner (unless we consider that illegal means should be taken into account when determining whether this information is personal). Using the proposed approach, since the information was of an "intimate" nature (i.e. health data)[1433] and not already "available"[1434] to the U.S. company, I maintain that the notion of "identifiability" should be interpreted less rigidly because the *risk of harm* upon this data being disclosed, once identified, is on the high side. Perhaps therefore, since it may be relatively easy to make a link between the clinical data and an individual, even using illegal methods, the key-coded clinical data should have been considered as being *personal information* even for the U.S. company.

The proposed approach can also be illustrated using the case of "IP addresses". These addresses by themselves may not qualify as *personal information* (for instance, if we don't take into account the illegal means of identifying the individual behind IP addresses).[1435] If these addresses are linked with a profile that contains information of an "intimate" nature, then perhaps "illegal means", which may be used to put a name and a face to the profile behind an IP address, should be taken into account. The threshold to "identify" the individual should be lower (the information being considered as "personal" more easily) if the disclosure of this kind of "intimate" data is potentially much more "harmful". On the other hand, if by using the IP address as a point of

---

[1432] See Lundevall-Unger & Tranvik, *supra* note 641 at 15. These authors refer to the EC, *Commission Decision 2000/520/EC*, *supra* note 674. Patrick Lundevall-Unger and Tommy Tranvik also refer to Morgan & Boardman, *supra* note 675 at 40.

[1433] See section 3.1.2.2.2 which elaborates on this criteria.

[1434] See section 3.1.2.2.3 which elaborates on this criteria.

[1435] ISPs are usually prohibited by law to disclose the identity of the subscribers to which IP addresses have been assigned to.

collection, other more trivial information is collected (information that does not qualify as "intimate") the IP address and the information linked with this address may not be considered as *personal information.* Moreover, the illegal means of linking this profile with an actual person should not be taken into account in the overall assessment, given that the risk of harm is rather minimal. In the hands of the relevant ISP, that also has access to subscriber information, the information in question would be considered as *personal*. However, the same information in the hands of another website that collects trivial information in connection with dynamic IP addresses (which it then uses for operational issues, such as remembering the language of its users or visitors) would not be considered as *personal information*.

(ii) Efforts to Identify

Section 2.1.2.2.1(b) details the fact that it is not always clear what kind of costs and efforts (or even resources) need to be used or taken into account when determining if certain data is "identifiable". I also discuss the fact that European courts, various academics and industry players don't agree on what "identifiability" actually means. While some take the position that the only relevant criteria for evaluating the status of IP addresses is the effort (or costs) involved in the identification process (while making no distinction between legal and illegal methods)[1436] others believe that the concept of *personal information* should be defined pragmatically, based upon the "likelihood of identification,"[1437] to avoid being regulated by a burdensome framework that protects every single piece of data in circulation.

Using the proposed method of interpretation, as the risk of subjective harm increases, the "effort and costs" necessary to consider this data as "identifiable" tend to decrease. Interestingly, certain industry players are already suggesting or implying that the extent of the *risk of harm* (upon the information being disclosed) should be taken into account

---

[1436] District Court Berlin-Mitte, No. 5 C 314/06, *supra* note 668. The plaintiff claimed that an Internet portal operator, by storing dynamic IP addresses, did not comply with the *German Data Protection Act* since these addresses had to be regarded as *personal data* given that the portal operator's log files could reveal information about the Internet users' political or religious beliefs. See also Stockholm Lænsrætt, No. 593-2005, *supra* note 669.

[1437] Fleischer, "IP addresses", *supra* note 610: "As long as there is little or no chance of disclosure by the controller to a third party of information that could lead, in combination with data held by that person, to re-identification of individuals, then this approach seems more than reasonable."

when determining whether certain information qualifies as *personal*.[1438] Certain authors have also articulated similar views: Lundevall-Unger and Tranvik propose that the "likely reasonable" test in recital 26 of the Directive 95/46/EC refers to the proportionality principle, which is well established in European Community Law. The word "necessary" in Article 5 of the Treaty, according to Unger and Tranvik, is synonymous with "likely reasonable" in recital 26 of the Directive 95/46/EC, in the sense that both terms point towards the same type of assessment: the weighing of pros and cons so that a balanced and fair result can be achieved.[1439] The "likely reasonable" test, therefore, would have to assess the effort and costs associated with linking "names and faces" to various pieces of information (like IP addresses) as well as the "privacy risks" that this linking may entail.[1440] The "privacy risks" which are referred to by these authors share some similarities with the "risk of subjective harm" test which I propose to take into account when interpreting the notion of "identifying".

Lundevall-Unger and Tranvik argue that in the context of IP addresses, the "likely reasonable" test should primarily consist of the effort and costs associated with putting "names and faces" to certain pieces of data with cost factors including "time, money, expertise, manpower, etc."[1441] They argue that the higher the costs, the less likely it is that the information consists of *personal data* (and the other way around).[1442] But more interestingly, these authors are also of the opinion that the nature of the information in question and the retention period should play a role in the evaluation. They maintain that it is, for instance, reasonable that the threshold-value, the point where anonymous information becomes *personal information* (and vice versa), should be lower when we are talking about "sensitive information" compared to when we are dealing with more trivial information.[1443] Similarly, extending the retention period may facilitate the

---

[1438] *Ibid*.

[1439] Lundevall-Unger & Tranvik, *supra* note 641 at 18: "Particularly, Article 5 of the European Community Treaty provides that action taken by the Community shall not go beyond what is 'necessary' to achieve the objectives of the Treaty."

[1440] *Ibid*.

[1441] *Ibid*. at 20.

[1442] *Ibid*.

[1443] *Ibid*.

collection of additional information that will make the original data "identifiable".[1444] Their views are consistent with the proposed approach, which maintains that if the data is of an "intimate" nature and not already "available", then the point where information becomes "personal information" is lower then if we are dealing with information which is not of an "intimate" nature nor already "available".

In other words, if "connecting the dots" between information and the identity of an individual is relatively easy, then the information will most likely be considered as *personal*.[1445] Using the proposed approach, if an anonymous IP address includes or is linked to profile information which is of an "intimate" nature and, or, includes information which is not generally "available", then the data (including the IP address) may be considered as *personal information*, even if the efforts or costs to link this information to a unique individual is relatively important or costly, because the disclosure of this information, if linked to an individual, may trigger a higher risk of subjective harm.

The challenge, then, is to identify the factors (effort and costs) that should be weighed against the potential "privacy risks" or what I refer to as the "risk of subjective harm" test. I leave it to better minds than mine to determine these factors, but I suggest that the simple rules which should be adhered to are the following: as the effort and costs increase, the less likely it is that information will qualify as *personal*, and as the "intimate" nature of the information and its non "availability" increases, the more likely it is that the information will qualify as *personal*.

[1444] See *Letter from the Article 29 Working Party to search engine operators (Google, Microsoft, Yahoo!)* (26 May 2010), online: <http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2010-others_en.htm>. See also generally the Article 29 Data Protection Working Party, *Opinion 1/2008*, *supra* note 207.

[1445] For example, information may be disclosed (published) about a former criminal case without mentioning any name (or other identifier) linked to the individuals involved. If, for example, this case won much public attention in the past, then it would not seem unreasonably difficult to gain additional information (e.g. by looking up newspapers from the relevant time period) allowing one to find out the identity of the individuals involved. In such case, as suggested by Article 29 Working Party, it would seem justified to consider the information as being information about identifiable persons and as such, *personal information*. Article 29 Data Protection Working Party, *Opinion 4/2007*, *supra* note 100 at 14.

(iii) Taking Into Account Potential Correlation

Trivial bits and pieces of very common information may rarely qualify as "identifiable" *personal information*. Consider the name "John Smith" for instance. There may be well over 1000 people in Canada and over 100 people in Quebec that share this name. Therefore, "John Smith" will in fact very rarely relate to an identifiable individual. According to the Article 29 Working Group, the question of identifiability depends on the circumstances of the case:

> "(…) the extent to which certain identifiers are sufficient to achieve identification is something dependent on the context of the particular situation. A very common family name will not be sufficient to identify someone - i.e. to single someone out - from the whole of a country's population, while it is likely to achieve identification of a pupil in a classroom. Even ancillary information, such as "the man wearing a black suit" may identify someone out of the passers-by standing at a traffic light. So, the question of whether the individual to whom the information relates is identified or not depends on the circumstances of the case."[1446]

Also, the information "by itself" will rarely create a risk of subjective harm upon its disclosure. If someone was to post the name "John Smith" on a website, it would not create any type of harm unless the website included additional details. It is the correlation between "John Smith" and another piece of information, such as being afflicted with a particular disease or being a member of special interest group, that may in fact create a risk of subjective harm upon being disclosed.

The definition of *personal information*, as it now stands, does not provide clear guidance as to whether correlation is needed for certain information to qualify as *personal*.[1447] Furthermore, what pool of data should be taken into account when assessing this correlation: data actually available to the data controller, data "likely to become available" to the data controller, or data in the hands of third parties as well?[1448] Moreover, it has now become considerably easier to link certain data to

---

[1446] *Ibid*. at 12-13.

[1447] See section 2.1.2.1.1(b) entitled "Correlation Required to Identify an Individual" which elaborates on this issue.

[1448] See section 2.1.2.2.1(d) entitled "Identifying alone or in correlation with other data?" which elaborates on this issue.

individuals, simply from the sheer availability of enormous amounts of data on the Internet, from the correlation of data across various online services and from the use of new identification tools.[1449]

When assessing the notion of "identifying", data availability and correlation should be prime factors. Certain legislators have in fact taken the position that the disclosure of the name of an individual by "itself" creates no harm. The Quebec public sector DPL actually takes the position that the name of an individual is not *personal information*, except where it appears "in conjunction" with other information concerning this individual (or where the mere mention of this individual's name would disclose something personal concerning him or her).[1450] Therefore, in interpreting the notion of "identifiability" which is necessary in assessing whether the disclosure of certain pieces of data will create a *risk of harm*, correlation is a key factor.[1451] This point is further illustrated by van den Hoven with the following example:

> "Let's consider the following two claims C1: "*X* is in a restaurant *A* at time *ti*" and C2: "*Y* is in Restaurant *A* at time *tr".* Is C2 about X? C2 presents itself obviously as information *about* Y. When looked at in isolation, "*Y* is in Restaurant at time *ti*" does not tell you anything about X, but when combined with C1, it does provide information about X which was not contained in C1. Good detective stories often present information to the reader which is seemingly irrelevant to the crime or to the biography of the protagonist, but later turns out to be, in an unexpected sense, *about* the murderer or his victim. As the story unfolds and the plot unravels, the insignificant piece of information is situated in a context where it suddenly picks out an individual. We suddenly see how the insignificant and seemingly irrelevant piece of information suddenly applies to the protagonist."[1452]

[1449] See section 1.2.3 entitled "New Identifying Methods" which elaborates on this issue.

[1450] *An Act respecting Access to documents held by public bodies and the Protection of personal information*, R.S.Q., c. A-2.1, s. 56.

[1451] The privacy threat is in the aggregation of consumer records, as outlined by Stan Karas who suggests that single retailer's consumer file may be extensive, but its scope is unlikely to be comprehensive enough for a true representation of our consumer identities and that the true danger is in the compilation of our transactional data. See Karas, *supra* note 362 at 39.

[1452] Van den Hoven, "Information Technology", *supra* note 642 at 307.

The true impact of data-mining can only be meaningfully assessed when taking into consideration other data available.[1453] Data volume will play a role in increasing the potential for identification because it increases the potential for data correlation.[1454] As the volume of data increases so too do the chances for identifiability. A good illustration of this can be made using the 2006 AOL breach discussed in section 1.2.1.3. While a single piece of data by itself may be meaningless (in this case, a single "web search") it may nevertheless be possible, because of the volume of data available (i.e. "all searches made" by a given profile over a three month period) to actually make the link between these searches and an identifiable individual, even if the name of the individual is not revealed. In the AOL breach, since part of the information was considered to be of an "intimate" nature (online searches made),[1455] this correlation (or potential correlation) was definitely to be taken into account when qualifying the information, especially given that this correlation did not require much work.

Clearly, the more work required to make a link between a piece of information and an individual, the less likely that information may be considered as being "identifying". To have one piece of a complex puzzle is one thing – but the ease with which additional pieces can be obtained must always be given consideration;[1456] in light of the overall risk of harm that may take place upon the information being disclosed. For example, upon the merger of organizations, this correlation should be taken into account

---

[1453] Ian Kerr and Jenna McGill share similar views. They argue that: "In fact, as new and emerging information technologies continue to come before the courts, we predict that the current reductionist inclination which asks whether the intercepted data is, *on its own*, meaningless will and ought to give way to the very opposite approach, namely: whether the bundle of information that is made available by means of the search, *once assembled,* ought to attract a reasonable expectation of privacy." Kerr & McGill, *supra* note 625 at 430-31.

[1454] See section 1.2.3 entitled "New Identifying Methods" which elaborates on this issue. See also Ohm, *supra* note 562 at 1766-67: "Most privacy laws regulate data quality but not quantity. Laws dictate what data administrators can do with data according to the nature, sensitivity, and linkability of the information, but they tend to say nothing about how much data a data administrator may collect, nor how long the administrator can retain it. Yet, in every reidentification study cited, the researchers were aided by the size of the database. (…) Thus, lawmakers should consider enacting new quantitative limits on data collection and retention. They might consider laws (…) limiting the total quantity of data that may be possessed at any one time." See also Article 29 Data Protection Working Party, *Opinion 1/2008*, *supra* note 207 at 19. The Article 29 WP is arguing that search engines should store queries for a maximum of six months.

[1455] See section 3.1.2.2.2 which elaborates on this issue.

[1456] Kerr & McGill, *supra* note 625 at 430-31. Ian R. Kerr and Jenna McGill articulate the position that the jigsaw nature of the data/information/knowledge/wisdom chain and the importance of each piece of the puzzle in telling a story despite the fact that no single piece could do so on its own should be recognized.

especially since the link can be made effortlessly.[1457] In such cases, if a business transaction triggers the merging of databases which will result in highly identifiable profiles, perhaps this information (each database and definitely, the "resulting profiles") should be considered as personal; depending, of course, on the intimate nature and availability of the information.[1458] Therefore, we need to evaluate the ease with which correlation can occur, along with the "intimate" nature of the information and whether it is already "available".[1459]

(b) Dealing with New Types of Data

I will discuss in this section how this notion of "identifiability" should be interpreted with new types of data: first when qualifying the information, and second, when the data relates to a group (instead of to a unique individual). I will also elaborate on the kind of accuracy required between certain data and an individual for this data to qualify as *personal*.

(i) Qualifying the Information

The first step in determining "identifiability" begins with the proper qualification of information. In section 2.1.2.2.2(a), I already discuss how certain data (which may qualify as "identifiers" or "points of collection") may not always be considered as *personal information* by courts or industry players. The Comité consultatif produced a report in which they propose that the notion of "identity" can mean three different things: (i) first, characteristic traits, such as age, information pertaining to family, hobbies, employer, professional qualifications, movements, purchases, etc; (ii) second, a point of collection or an identifier that may allow a linkage to different data and biographical characteristics from the same person (this could mean a permanent cookie, a client number, a number identifying a terminal); (iii) third, a point of contact that would enable a third party to take the initiative to contact an individual (by email,

---

[1457] Article 29 Data Protection Working Party, *Opinion 2/*2010, *supra* note 191 at 9: "Other scenarios that can lead to identifiability are mergers, data losses and the increasing availability on the Internet of personal data in combination with IP addresses."

[1458] See section 2.1.2.2.2(a) entitled "Dealing With New Types of Data" which discusses the concerns which took place in the context of the merger between Abacus and Double click.

[1459] In the sense that according to the proposed interpretation, the more important is the *risk of subjective harm*, the less work is required for the data to qualify as "personal".

mail, fax, phone, etc.).[1460] The Comité consultatif suggests that with time and throughout its life cycle, the status of a certain piece of data may change: For example, a dynamic IP address may be a point of collection for a short period.[1461] They suggest that an address may be both a point of collection as well as a point of contact, and the vulnerability of postal addresses would result from the fact that this kind of data would accumulate the three properties above.[1462]

Nowadays, "points of collection" or "identifiers" can also be supermarket loyalty cards, RFID tags or mobile coupons that track customers.[1463] The definition of *personal information* found in most DPLs does not specify whether these identifiers (or points of collection) constitute *personal information*. When discussing the notion of "identifiability", it is important not to ignore the fact that devices acting as "points of collection" or "identifiers" (such as IP addressees, RFID tags, cookies, wireless devices, etc.) may reveal very "intimate" data.[1464]

The first step in ascertaining a risk *of harm* with the disclosure of information under the "identifiability" criteria, is to begin with determining the kind of information in question (biographic information, point of collection, point of contact, or some or all of the above criteria). We can't be too quick to disregard an IP address as *personal information* simply because it belongs to a device instead of an individual (which may or may not be "identifiable"). For example, an IP address may be a simple point of collection with no additional information attached to it and therefore, less harmful if disclosed; therefore, it should not qualify as *personal information* (if not linked to any biographic or contact information). An IP address leading to a device may also not be considered

[1460] Conseil de l'Europe, *L'autodétermination informationnelle*, *supra* note 20 at 30-31.

[1461] *Ibid*. at 31.

[1462] *Ibid*.

[1463] Article 29 Data Protection Working Party, *RFID technology*, *supra* note 196 at 5-6; Ariana Eunjung Cha, "Mobile coupons track customers" *The Washington Post* (27 June 2010), online: The Washington Post <http://www.washingtonpost.com/wp-dyn/content/article/2010/06/26/AR2010062600223.html>; See also E. Murphy, "Tracking Grocery Hot Spots", *Portland Press Herald* (27 January 2004).

[1464] Article 29 Data Protection Working Party, *RFID technology*, *supra* note 196 at 7: "Belongings of a person are very personal and hold information whose knowledge by third parties would invade the privacy of the person who owns the object. The following examples illustrate this hypothesis. Consider the case where anyone in possession of a reader can detect banknotes, books, medicines or valuable objects of passers by. The knowledge of this information by third parties will invade the privacy of the person who owns the object."

personal information if it doesn't reveal "intimate" details (for instance, it is only used to remember the preferred language of its website users and is not otherwise made available to third parties).[1465] An IP address coupled with biographic information becomes more "sensitive", especially when linked with biographic information that is of an "intimate" nature and becomes more "sensitive" if this information was not already "available". In this case, the IP address (together with the information linked to it) would clearly qualify as *personal information*. This IP address would become even more potentially harmful when associated with a point of contact (such as an email address, a user account or a physical address).

(ii) Group vs. Individual and Accuracy of Identification

Recent technological advancements have opened the way for data to be collected by a certain device that may be associated with a group of individuals; for instance, an IP address linked to a computer used by a few co-workers, family members or library users (vs. a unique individual). It is not always clear in such cases whether the IP address is "identifiable", as detailed in section 2.1.2.2.2. In order to determine when data belonging (or potentially belonging) to a group of individuals should be covered by the definition of *personal information*, one should take into account its intimacy and availability. For example, while information of a very "intimate" nature which is not otherwise "available" should be considered *personal* even if it belongs to a small group of individuals (ex: a handful of individuals using the same computer), this should not be the case if the information is more trivial and more easily "available". In this last case, the information should only be considered as *personal information* if it can be linked to a unique individual, since the risk of harm is much lower.

Another issue further discussed in section 2.1.2.2.2(c) is that it is not always clear how accurate the link must be between certain information and an individual in order for the data to qualify as "identifying". The name of an individual is indeed the most common identifier. In practice, the notion of an "identified individual" usually implies a reference to the individual's name. As discussed in section 2.1.2.1.1(b), in order to ascertain this identity, the name of the person sometimes has to be combined with other pieces of

[1465] And this, regardless of whether it may be easily identifiable (for instance, if it is linked with this user's account).

information (date of birth, parents, an address or a photograph) to prevent confusion between that individual and possible namesakes.[1466] With regards to the notion of "indirectly" identified or identifiable persons, as detailed in article 2 of the Directive 95/46/EC, the Article 29 Working Party articulates the view that this category typically relates to the phenomenon of unique combinations, whether small or large in size.[1467] The Directive 95/46/EC comes in with "one or more factors specific to his physical, physiological, mental, economic, cultural or social identity". The Article 29 Working Party maintains that while some characteristics are so unique that someone can be identified with relative ease ("present Prime Minister of Spain"), a combination of details on a categorical level (such as age category, regional origin, etc.) may also be pretty conclusive in some circumstances, particularly if one has access to additional information of some sort.[1468]

Using the proposed approach, if the information evaluated (or the bundle of information) reveals information of an "intimate" nature (i.e. John Smith from Montreal who suffers from AIDS)[1469] and this information is not "available",[1470] then the fact that the data relates to a small group of individuals (for example ten individuals named John Smith who live in Montreal) may be sufficient to argue that this data is *personal*. As a matter of fact, since the information linked to the name John Smith is of a very "intimate" nature (i.e. being afflicted with AIDS) and not in circulation or "available" (see

---

[1466] The Article 29 Working party illustrates this idea with an example. Article 29 Data Protection Working Party, *Opinion 4/2007*, *supra* note 100 at 13: "For example, the information that a sum of money is owed by Titius can be considered to relate to an identified individual because it is linked with the name of the person. The name is a piece of information that reveals that the individual uses that combination of letters and sounds to distinguish himself and be distinguished by other persons with whom he establishes relations. The name may also be the starting point leading to information about where the person lives or can be found, may also give information about the persons in his family (through the family name) and a number of different legal and social relations associated with that name (education records, medical records, bank accounts). (…) All these new pieces of information linked to the name may allow someone to zoom in on the flesh and bone individual, and therefore through the identifiers the original information is associated with a natural person who can be distinguished from other individuals."

[1467] The Article 29 Working Party articulates the view that in cases where *prima facie* the extent of the identifiers available do not allow a particular individual to be singled out, that this individual might still be "identifiable" because that information combined with other pieces of information (whether the latter is retained by the data controller or not) will allow the individual to be distinguished from others. See *ibid*.

[1468] *Ibid*.

[1469] See section 3.1.2.2.2 which elaborates on this issue.

[1470] See section 3.1.2.2.3 which elaborates on this issue.

test under section 3.1.2.2.3), then the interpretation of the notion of "identifiability" should be interpreted less stringently. On the other hand, let us consider the *John Smith* who is a resident of Montreal and subscribes to the Montreal Gazette, a general interest newspaper. Even though there may be three John Smith*s* who fall into this category, the disclosure of this information would not present a considerably high risk of harm and therefore the data should not be considered as *personal*.

In light of the approach proposed in this thesis, the "identifiability" criteria has to be interpreted more "softly" if the data is otherwise "sensitive" (in the sense that its disclosure is potentially harmful since it is of "intimate" nature, not already "available" and "identifiable"). The more "intimate" and the less "available" the information, the less important this "accuracy" factor (i.e. accuracy in identifying a unique individual) will actually play in the evaluation of the information. On the contrary, if the information is not of a very "intimate" nature, or it is "intimate" but it is already "available", then this "accuracy" factor will be more important to get to the point of qualifying the data as *personal*.

With the approach proposed, the notion of "identifiability" is linked with the fact that the data may be of an "intimate" nature and "available". These two criteria will be explored in greater length, starting with the "intimate" criterion.

3.1.2.2.2. Intimate Nature of Information

As discussed in section 3.1.2.1.1, the type of harm resulting from the "disclosure" of personal information is subjective, is of a psychological nature and invokes such emotions as embarrassment or humiliation. Therefore, another important criterion that is necessary to ensure that the data is in fact protected, has to do with information which, upon being disclosed, would create some type of embarrassment or humiliation. This means that the data should be of an "intimate" nature. Rarely would individuals be embarrassed by the disclosure of their name or some other random piece of information, such as the fact that they are a subscriber to a local (and common) newspaper and that they enjoy running in their free time. To trigger the feeling of humiliation or embarrassment, the data usually needs to focus on something of an

"intimate nature".[1471] For instance, the following facts, once disclosed, may cross that threshold of intimacy: subscription to a magazine targeting homosexuals, attending nudist beaches, or suffering from an embarrassing disease. These bits of data are more likely to create some unwanted feelings upon their disclosure to third parties or to the public.[1472]

(a) Evidence that Intimate Data is to be Protected

Various older as well as more recent sources confirm that DPLs were intended to regulate "intimate" data at the disclosure level.

(i) Evidence from Old Documents

Warren and Brandeis were specifically concerned with protecting information about "the private life, habits, acts, and relations of an individual."[1473] Prosser discussed how the common law recognizes a tort of privacy invasion in cases where there had been a "[p]ublic disclosure of embarrassing private facts" or an "[i]ntrusion (. . .) into [an individual's] private affairs."[1474]

Documents produced in the context of the elaboration of the FIPs and the adoption of the first DPLs imply that information of an "intimate" nature was to be regulated in order to address the kind of harm associated with a disclosure. In the late 1960s, the conclusions of the Nordic Conference on the Right of Privacy (1967) referred to the kind of harm resulting from an attack on the honour and reputation of an individual and

---

[1471] Trudel & Benyekhlef, *supra* note 367 at 5 : "Pour établir s'il y a atteinte à la vie privée, il est nécessaire de déterminer si une divulgation d'information ou une intrusion porte sur un élément de la vie privée. D'où la nécessité de tenter de circonscrire le domaine de la vie privée. Le domaine de la vie privée regroupe certains types d'informations qui y sont, en principe, rattachées."

[1472] See Calo, "The Boundaries", *supra* note 443 at 16. Calo provides interesting examples to illustrate the kind of harm that may take place with the activity of disclosing data: "A person may feel embarrassed in the moment by a single act of observation, as when she walks through a back-scatter device in airport security that creates a picture of her naked body. Or she may feel an ongoing sense of regret about an embarrassing revelation lingering somewhere online." In Calo's examples, we can see that it is the disclosure of personal information (or the "making available" of this information) that are of "intimate nature" (intimate parts of the individuals' body) which causes this subjective privacy harm.

[1473] Warren & Brandeis, *supra* note 5 at 216.

[1474] Prosser, *supra* note 1347 at 389.

the "disclosure of irrelevant embarrassing facts relating to his private life".[1475] In Europe, Resolution 428 (1970) *containing a declaration on mass communication media and human rights* suggested that the right to privacy was the protection of one's "private, family and home life" which consisted, among other things, of the "non-revelation of irrelevant and embarrassing facts, unauthorized publication of private photographs, (…) [and the] protection from disclosure of information given or received by the individual confidentially."[1476]

In the early 1970s, the U.K. *Report of the Committee on Privacy* mentioned that there had been a fairly steady flow of complaints about intrusions into privacy by mass media, reporting "intimate details" of the lives of individuals which would not normally be thought of as being in the public domain.[1477] At the same period, the Explanatory Report pertaining to Resolution (74) 29 (which led to the adoption of Convention 108) referred to the protection of information which is inherently sensitive, "for example because it relates to the individual's conduct in his own home, his sexual life or his opinions."[1478]

(ii) Examples in More Recent DPLs

Certain European DPLs (notably in France) have included categories of "sensitive" data, similar to article 8 of Directive 95/46/EC, and acknowledge that certain types of personal data are more privacy sensitive and more likely to harm the data subject in cases of unauthorized processing.[1479] These categories include data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life". The categories

---

[1475] *Report of the Committee on Privacy*, *supra* note 3 at 327-28, Appendix K, Definitions of Privacy, (ch. 4): "2. (…) The right of the individual to lead his own life protected against (…) the disclosure of irrelevant embarrassing fact relating to his private life (…)."

[1476] Council of Europe, PA, *Resolution 428 containing a declaration on mass communication media and human rights* (1970) at para. 2 [Council of Europe, *Resolution 428*]: "The right to privacy consists essentially in the right to live one's own life with a minimum of interference. It concerns (…) non-revelation of irrelevant and embarrassing facts (…)."

[1477] *Report of the Committee on Privacy*, *supra* note 3 at 6, para. 19.

[1478] Council of Europe, *Explanatory Report: Resolution (74) 29*, *supra* note 65 at para. 18.

[1479] *Loi informatique et liberté*, *supra* note 131 at c. II, s. 2, art. 8 (II) (1). See also for example, *Loi fédérale Suisse sur la protection des données*, *supra* note 1392 at art. 3; EC, *Directive 95/46/EC*, *supra* note 99 at art. 8, para. 1.

of so-called inherently "sensitive" information are usually of an "intimate" nature.[1480] Interestingly, these categories are similar to the categories or elements determined by Quebec courts as relating to the intimate or the private life of individuals.[1481]

Organizations that manage personal information as part of their business are usually bound to protect the information against security threats and guard the information against unauthorized access, loss, or disclosure in accordance with DPLs.[1482] In Europe, the *European Communities (Data Protection) Regulations* were introduced, effective as of April 1st, 2002, in order to clarify and build upon the existing obligation set forth by the Directive 95/46/EC to keep personal data secure. In particular, these rules clarified what was meant by "appropriate security measures" and stated that in deciding what level of security was appropriate, organizations handling data must have regard to the "nature" of the personal data in question, and the "harm" that might result from its unauthorized use, disclosure or loss.[1483] More specifically, these regulations specify that medical files, personnel files, or private telecommunications are "sensitive" information and that information such as "name, address, or membership of a local drama group" are "non sensitive".[1484] I submit that the first kinds of information are also of an "intimate" nature and the second kind, not usually viewed as being "intimate".

In Canada, PIPEDA suggests that the form of the consent sought by the organization may vary, depending upon the circumstances and the type of information, and that in determining the preferred form of consent, organizations shall take into account the sensitivity of information.[1485] It goes on to say that any information can be sensitive depending on the context, and provides the following example:

[1480] See section 3.1.2.2.2(c) entitled "Information Inherently Intimate" that elaborates on this issue.

[1481] See Trudel, "Privacy Protection", *supra* note 164 at 322.

[1482] See section 2.2.1.3.2(a)(iv) entitled "Subjectivity in Security Measures to Adopt and Retention Obligations" which elaborates on this issue.

[1483] EC, *Security Measures*, *supra* note 1068.

[1484] *Ibid*.: "Organisations dealing with personal data of a private or sensitive nature – such as people's medical files, personnel files, or private telecommunications – naturally need to have very robust standards of security in place. Organisations that hold personal data with a lower privacy value – such as name, address, or membership of a local drama group – do not need to go to such great lengths, but must still have reasonable security measures in place."

[1485] PIPEDA, *supra* note 63 at principle 4.3.4.

> "For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive."[1486]

It is interesting to note that when referring to the "special-interest" magazine, PIPEDA is in fact referring to information of an "intimate" nature.

In the U.S., there is no general DPL overseeing all commercial activities of organizations (such as there are in Canada and France) although so-called "sensitive" information is accorded special recognition through a series of sectoral privacy statutes. These statutes have been adopted to restrict the disclosure of certain information and to prevent the ensuing risk of subjective harm discussed above. More specifically, the particular categories of information most likely to require protection against disclosure to third parties are the following ones: government records,[1487] academic records,[1488] cable company records,[1489] video rental records,[1490] motor vehicle records,[1491] and personal health information.[1492] Various U.S. states would also restrict the disclosure of particular forms of information, such as medical data and alcohol and drug abuse.[1493] These various statutes, which restrict the disclosure of specific kinds of personal information, have focused on data of an "intimate" nature, not

---

[1486] *Ibid*. at principle 4.3.4.

[1487] *The Privacy Act of 1974*, 5 U.S.C. § 552a(e)(10) (2000) is prohibiting governmental agencies from disclosing information about an individual without his or her prior written consent.

[1488] *The Family Educational Rights and Privacy Act of 1974*, 20 U.S.C. § 1232g(b)(1) (2000) is requiring educational agencies or institutions that receive government funding not to disclose students and education records without written consent.

[1489] *The Cable Communications Policy Act of 1984*, 47 U.S.C. §§ 551(b)-(c) (2000) is limiting the extent to which a cable service may collect or disclose PII about subscribers.

[1490] *The Video Privacy Protection Act of 1988*, 18 U.S.C. § 2710(b)(1) (2000) is creating civil liability for video stores that disclose PII about any customer and protects against unconstrained dissemination of video rental records.

[1491] *The Driver's Privacy Protection Act of 1994*, 18 U.S.C. §§ 2721-2725 (2000) is restricting the use of personal information contained in state motor vehicle records.

[1492] *The Health Insurance Portability and Accountability Act of 1996*, 42 U.S.C. §§ 1320d–1320d-8 (2000) [*Health Insurance Portability and Accountability Act of 1996*] is protecting the privacy of personal health information in transactions.

[1493] *The California Health and Safety Code* § 199.21 (West 1990) (repealed 1995) is prohibiting the disclosure of HIV test results; *The New York Public Health Law* § 17 (McKinney 2001) is permitting the release of medical records of minors relating to sexually transmitted diseases and abortion upon written request, but prohibiting the disclosure to parents without consent; The 71 PA. STAT. ANN. § 1690.108 (West 1990) is prohibiting the disclosure of all records prepared during alcohol or drug abuse treatment.

simply any kind of data that may identify an individual. This illustrates how the subjective harm resulting from the disclosure of personal information usually pertains to data of an "intimate" nature, if U.S. specific statutes focus on this kind of information uniquely.

(iii) Case Law

Case law rendered in the context of addressing the subjective harm resulting from the disclosure of information confirms that the information that is in need of protection is or should be information of an "intimate" nature. In Quebec, it is legal to disclose personal information such as names, telephone numbers, geographical addresses or email addresses to a third party wishing to use this information for purposes of commercial or philanthropic prospection upon certain requirements being complied with. One of the requirements is that the disclosure shall not "infringe upon the privacy" of the individuals concerned.[1494] In one case, this requirement of "infringing upon the privacy" was interpreted to mean the disclosure of "health" information.[1495] In the recent case of Jones v. Tsige,[1496] the Court of Appeal for Ontario illustrates that in the case of an invasion of privacy (what I refer to as a subjective harm), the fact that the information disclosed is of "intimate" nature is crucial:

> "These elements make it clear that recognizing this cause of action will not open the floodgates. A claim for intrusion upon seclusion will arise only for deliberate and significant invasions of personal privacy. Claims from individuals who are sensitive or unusually concerned about their privacy are excluded: it is only intrusions into matters such as one's financial or health records, sexual practices and orientations, employment, diary or private correspondence that, viewed objectively on the reasonable person standard, can be described as highly offensive."[1497]

In the U.K. case *Durant v Financial Services Authority,*[1498] the Court of Appeal came to the conclusion that the definition of *personal information* was to be interpreted more

---

[1494] Quebec DPL, *supra* note 110 at s. 22.

[1495] *Deschênes c. Groupe Jean Coutu*, PV 98 08 42 (C.A.I.) [*Deschênes*].

[1496] *Jones*, *supra* note 1353.

[1497] *Ibid*. at para. 72.

[1498] *Supra* note 590.

narrowly. The court articulated the view that what makes data "personal"[1499] is information which: "is biographical in a significant sense; has to have the individual as its focus; and has to affect an individual's privacy whether in his personal family life, business or professional activity".[1500] The U.K. Court of Appeal refers to a type of data which is close to data which is of "intimate" nature. In *Stevens v. SNF Maritime Metal Inc.*,[1501] the Federal Court of Canada took the position that the individual had not put into evidence the fact that his personal information disclosed in breach of PIPEDA triggered a subjective harm, since the information at stake was not "deeply personal" or "intimate".[1502]

While the usual metric in DPLs to establish whether certain information is protected is the notion of an "identifiable individual",[1503] courts (such as the ones in Canada and even in the U.S.) have adopted a rather different threshold in the context of the "reasonable expectation of privacy". In *R. v. Plant*,[1504] Sopinka J. of the Supreme Court of Canada establishes the framework for evaluating informational privacy claims. According to Sopinka a reasonable expectation of privacy depends on whether the information in question reveals "a biographical core of personal information (…) [that] (…) would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual".[1505] Under section 8 of the Canadian Charter of Rights and Freedoms[1506] ("Canadian Charter"), information is therefore only worthy of

---

[1499] Within the meaning of personal data under Directive 95/46/EC and the *Data Protection Act 1998*, *supra* note 686.

[1500] Please note that the case has been taken before the European Court of Human Rights as a breach of Article Eight of the European Convention of Human Rights, article Eight which states that everyone has the right to respect to his private and family life, his home and his correspondence.

[1501] *Supra* note 599.

[1502] Mr. Justice Phelan states : "The Applicant's claim, in excess of $148,000, is out of proportion to the privacy invaded. The information disclosed was not deeply personal or intimate. It was commercial and the type of information frequently spoken about in a social context. Therefore, I find that the damages claimed are not those for breach of the Act but for wrongful termination. To the extent (if any) that privacy is involved, it is minimal and the Applicant has put forward no other evidence of impact on his standing or community perception or similar features of a breach of privacy claim."

[1503] See section 1.1.3 entitled "Definition of Personal Information: Origin and Background" which elaborates on the definitions.

[1504] 84 C.C.C. (3d) 203, [1993] 3 S.C.R. 281, 24 C.R. (4th) 47, 1993 CarswellAlta 94, 1993 CarswellAlta 566 (S.C.C.) [*Plant*, cited to S.C.R.].

[1505] *Ibid*. at p. 16.

[1506] *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*.

constitutional protection if it forms part of a "biographical core" of intimate details or lifestyle choices.[1507] In the course of his judgment, Sopinka J. sets out a number of factors that govern the determination of when state acquisition of information triggers or offends the Canadian Charter*,* but the "nature" of the information figures prominently in the analysis.[1508] In other words, as explained by Ian Kerr and Jenna McGill, "as long as identifiable information about an individual is *deemed not to be* core biographical information, there is no reasonable expectation of privacy for that information."[1509]

Canadian courts, in the context of analyzing the expectation of privacy of individuals, have already decided to focus on data of an "intimate" nature instead of "all data that can identify an individual". I argue that this is because only information of an "intimate" nature can trigger the subjective harm to individuals upon being disclosed.

As discussed in section 2.1.1, many authors including academics are suggesting to focus on "private" or "intimate" data when attempting to limit the scope of DPLs and concurrently, in order to address the potential over-inclusiveness of DPLs discussed in section 2.1.2.1.1. For example, Solove, referring to Richard Murphy's definition of personal information (which is consistent with the definition of *personal information* discussed herein),[1510] claims that it is too broad because there is a significant amount of information identifiable to us that we do not deem as "private".[1511] In his own words: "For example, the fact that a person is a well-known politician is identifiable to her, but is not private. Murphy's definition thus provides no reasonable limitation in scope".[1512]

[1507] In *Plant*, the question was whether the police could access a suspect's electricity consumption records from a public utility without a warrant. Sopinka J., writing for the majority, held that accessing this information did not interfere with a reasonable expectation of privacy. Therefore, no warrant was required.

[1508] Pomerance, *supra* note 233 at 288.

[1509] Kerr & McGill, *supra* note 625 at 413-14. This test has been criticized by Ian R. Kerr and Jenna McGill because each piece of information could be evaluated individually, and through the reductive process, there would be no piece of information left which would reveal a "biographical core" of information. See also Pomerance, *supra* note 233 at 287: "it is by no means clear that data-mining would be found to offend section 8 of the Charter, given that: 1) any single piece of information, standing alone, might not be sufficiently intimate, personal or private to trigger section 8 protection; and 2) because much of the information that is accessed or 'mined' is within the public domain".

[1510] Murphy, *supra* note 584 at 2383.

[1511] Solove, "Conceptualizing", *supra* note 23 at 1111.

[1512] *Ibid*. at 1112.

As discussed earlier, according to Inness, "it is the *intimacy* of this information that identifies a loss of privacy" and not all personal information is private.[1513]

When Trudel and Benyekhlef were mandated to evaluate the Quebec DPL a few years after its enactment, they suggested that the definition of *personal information* was over-reaching in the context of the Internet.[1514] They suggested that when assessing the potential privacy breaches resulting from information disclosures, we should first determine whether the information in question relates to an element of the individual's "private life".[1515] They proposed that perhaps only "private information" should be protected and that other types of data could circulate freely, especially since they may have certain value for society.[1516] In a more recent article, Trudel confirmed his view that the right to privacy concerns information that affects an individual's independence and ability to exercise control over information concerning "intimate relationships and life choices."[1517]

With the emergence of new types of data, it is not always clear when the standard definition of *personal information* actually applies.[1518] In response to these concerns, the Article 29 Working Party, in a working document on information generated by RFID tags, notes the following:

> "data relates to an individual if it **refers** to the identity, characteristics or behaviour of an individual or if such information is **used** to determine or influence the way in which that person is treated or evaluated."[1519]

This comment is consistent with the proposed approach. At the "use" level, I maintain that the test should be whether *such information is used to determine or influence the*

[1513] Inness, *supra* note 587 at 58.

[1514] Trudel & Benyekhlef, *supra* note 367.

[1515] *Ibid*. at 5.

[1516] *Ibid*. at 3-6.

[1517] Trudel, "Privacy Protection", *supra* note 164 at 325-26: "Logically, not everything about an individual belongs to his or her private life. The right to privacy concerns information that affects an individual's independence and ability to exercise control over information concerning intimate relationships and life choices."

[1518] See section 2.1.2.2 and more specifically, section 2.1.2.2.2 entitled "Identifying a Device or an Object", which elaborate on the uncertainty as to whether new types of data qualify as personal information.

[1519] Article 29 Data Protection Working Party, *RFID technology*, *supra* note 196 at 8.

way in which that person is treated or evaluated (and this is further discussed in section 3.2.2) while at the "disclosure" level, the test is whether "*data (...) refers to the identity, characteristics or behaviour of an individual".* This illustrates how, at the "disclosure" level, the kind of data to be protected is a special kind of data (and not all personal information). The data that should be regulated by DPLs is data that says something about the individual (data which refers to the "identity, characteristics or the behaviour of an individual*"),* which is close to the notion of "intimate" nature.

In 2009, the RAND Corporation reviewed Directive 95/46/EC, concluding that one of its main weaknesses was the fact that the link between the concept of "personal data" and real privacy risks was unclear.[1520] It suggested that possible criteria or avenues for determining the risk involved in specific categories or acts of data processing include:

> "the privacy sensitive nature of the data being processed, and more specifically whether the nature of this data causes it to be more likely to result in harm, considering the full context of the data processing (e.g. the processing of health related information, racial information, etc)."[1521]

The "privacy sensitive nature" of the data, which RAND Corporation refers to, may be close to the data of an "intimate" nature discussed here. Ohm also suggests that regulators should take into consideration the sensitivity of the data when he is in fact referring to the "intimate nature" of the information.[1522]

All of these examples illustrate how one of the criteria that should be taken into account when determining if a disclosure of information creates a *risk of harm* is whether the data in question is of an "intimate" nature. As discussed in section 3.1.2.2, I prefer to refer to data which is "intimate", "available" and "identifiable" than data which is "sensitive", since the sensitivity of the data depends on these three criteria.

[1520] Robinson et al., *supra* note 151 at ix; See also, *ibid*. at 27: "The scope of the Directive has been criticised because the relationship between privacy protection and data protection is vague: not all acts of personal data processing as covered by the Directive have a clear or noticeable privacy impact, and we must ask if this is a weakness in its focus. Should the impact on privacy be a relevant criterion for determining the applicability of data protection rules? The impact of the Directive is not defined in terms of situations with a privacy impact, but rather to acts of personal data processing."

[1521] *Ibid*. at 50.

[1522] According to him, it makes sense to "treat medical diagnoses differently than television-watching habits, for example, because the path to harm for the former is shorter and more direct than for the latter". Ohm, *supra* note 562 at 1768.

(b) How to Determine if Information is of an Intimate Nature?

Section 2.2.1.4.1 elaborates on the fact that *privacy* and *harm* are contextual. Determining exactly which information is of an "intimate" nature can be a challenge, as it is often a subjective assessment, one that may vary from one individual to another, between different segments of society, between societies in different countries, and between different periods of time in the same society. Nissenbaum suggests that drawing lines in the case of intimate and sensitive information is difficult and can be controversial, that these lines are neither static nor universal, and that interpretations of what counts as a "person's private sphere" may change with time.[1523]

Renée M. Pomerance is of the view that if privacy protection depends on whether something is "inherently private", this opens the door to a subjective interpretation.[1524] She argues that "intimacy", as it is currently defined (referring, in Canada, to the test set forth in *R. v. Plant*), may not be the best way of charting the zone of constitutional enforcement for the main reason that to some extent, intimacy lies in the eye of the beholder,[1525] and that: "reasonable people can, and often will, disagree about what is inherently private. The divide between the majority and the dissent in *R.v. Plant* supports this proposition."[1526]

While the notion of "intimate" data can be a subjective assessment, the nature of the data is only the first part of the test that I propose to use to determine whether a disclosure of information may create a risk of subjective harm to the individual concerned. The availability of the data is an equally crucial component.[1527] Let us

---

[1523] She suggests that the case of wiretaps in the United States illustrates variability across time: in 1928, in *Olmstead v. United States*, 277 U.S. 438 (1928), rev'd *Katz v. United States*, 389 U.S. 347 (1967). The U.S. Supreme Court initially ruled that wiretapping did not constitute a breach of private space. By 1967, however, in what is understood as an overturning of that ruling, in *Katz v. United States,* 389 U.S. 347 (1967), the Court concluded that tapping a person's phone does constitute an unacceptable intrusion into inviolate space. She states: "at least one change this shift reflects is a change in belief about what constitutes a person's private sphere". Nissenbaum, *supra* note 230 at 131-32.

[1524] Pomerance, *supra* note 233 at 288-89.

[1525] *Ibid*.

[1526] *Ibid*.

[1527] See section 3.1.2.2.3 entitled "Availability" which elaborates on this issue. For example, if someone's age is kept confidential and has never been disclosed, the fact that this data (someone's birth date) is not necessarily inherently of "intimate" nature, it may still be considered as harmful upon being disclosed once it passes through the "availability" test.

suppose, for instance, that someone has been publicly proclaiming his homosexuality on various online blogs, to the point where it has become common knowledge. Despite its inherent sensitivity, the sheer availability of the data nullifies the risk of harm that would be triggered by disclosure and the protection of the information becomes unnecessary. Adding the "availability" component to the overall test, will limit the protection of certain data that were not meant to be protected by DPLs.

Certain types of data are usually considered part of people's private area according to most individuals, as suggested by the European *Report of the Committee on Privacy* (1972):

> "At any given time, there will be certain things which almost everyone will agree ought to be part of the 'private' area which people should be allowed to preserve from the intrusion of others, subject only to overriding interest of the community as a whole where this plainly outweighs the private right. Surrounding this central area there will always be a 'grey area' on which opinions will differ, and the extent of this grey area, as also that of the central one, is bound to vary from time to time."[1528]

This central area is a good starting point.[1529] While what constitutes information of an "intimate" nature may in fact vary across times, societies, and cultures, I note that since the first DPLs were adopted or were in the process of being adopted in the early 1970s, the notion of "sensitive information" has endured in both Europe and in North America and the same kind of data has been considered as "intimate" ever since, as illustrated below.

(c) Information Inherently Intimate

Although identifying data as "intimate" is a subjective assessment, categories of data that have been found to be inherently sensitive, and qualify as "intimate" information, have been the same across various jurisdictions (U.S., Canada and Europe) for the relatively long period of over forty years. Authors, courts and lawmakers usually agree that aspects of the "intimate life" often include things pertaining to the following, which

---

[1528] Justice Committee on privacy. "Privacy and the Law" at 5, para. 18, reported in *Report of the Committee on Privacy*, *supra* note 3 at 17, para. 47.

[1529] As this notion is also close to the notion of "core biographical information".

provide for a good basis for the *risk of harm* test that I propose to take into account at the disclosure level.

(i) Medical and Health

The Lindop Report (U.K., 1978) referred to the fact that sensitive information included the individual's medical history, and the medical information of an individual, such as the fact that a woman was pregnant.[1530] More recently, in both Canada and Europe, private life still includes things relating to medical and health conditions. In France, the processing of data concerning health is prohibited, in line with the Directive 95/46/EC on this matter.[1531] In Europe, the *Security Measures for Personal Data: A Guide to the New Data Protection Rules* provides that organizations dealing with personal information "of a private or sensitive nature" such as "people's medical files", need to have very robust standards of security in place.[1532] In Canada, PIPEDA states that some information "such as medical records" are almost always considered to be sensitive,[1533] and specific health data protection laws have also been adopted in certain Canadian jurisdictions.[1534] The OPCC has articulated the view that since medical or health information was sensitive, it should not be used in online behavioural advertising.[1535] In Quebec, case law confirms that private life includes things relating to the anatomy and the intimate life of an individual.[1536] The CAI (Quebec) has even recently issued a decision stating that a pharmacist breached the privacy of individuals

---

[1530] Lindop, *supra* note 96 at 153-54, para. 18.25 and at 143, para. 17.20.

[1531] *Loi informatique et liberté*, *supra* note 131 at c. II, s. 2, art. 8 (I). See also EC, *Directive 95/46/EC*, *supra* note 99 at art. 8.

[1532] EC, *Security Measures*, *supra* note 1068.

[1533] PIPEDA, *supra* note 63 at Schedule 1 (s. 5), principle 4.3.4.

[1534] Alberta has adopted a *Health Information Act,* RSA 2000, c H-5; Saskatchewan, a *Health Information Protection Act,* SS 1999, c H-0.021; Manitoba, a *Personal Health Information Protection Act,* CCSM c P33.5; Ontario, a *Personal Health Information Protection Act,* 2004, SO 2004, c 3, Sch A.; New Brunswick, a *Personal Health Information Privacy and Access Act,* SNB 2009, c P-7.05; Newfoundland and Labrador, a *Personal Health Information Act,* SNL 2008, c P-7.01; and Nova Scotia, a *Personal Health Information Act,* Chapter 41 of the Acts of 2010.

[1535] OPCC, *Online Behavioural*, *supra* note 275: "The information collected and used is limited, to the extent practicable, to non-sensitive information (avoiding sensitive information such as medical or health information)."

[1536] Trudel, "Privacy Protection", *supra* note 164 at 322: "Generally, private life includes things relating to (…) health (…)."

when it disclosed the fact that his clients were "diabetics" to a third party marketer.[1537] In the United States, sensitive information is accorded special recognition only through a series of key privacy statutes. The disclosure of information from health records is restricted by such statutes.[1538] In the U.S., the recently released Boucher Bill, introduced in May of 2010, defines "sensitive information" as data which includes: "Medical records, including medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional".[1539] U.S. attorney Stan Karas illustrates how health data may prove to be sensitive and create some type of embarrassment or humiliation if exchanged in the context of online consumer profiles: "Even most ardent direct marketers would have a hard time justifying sharing information about purchases of pregnancy kits, Depends, or girdles."[1540]

(ii) Family Life and One's Home

The European Convention on Human Rights adopted in 1950 states, at article 8 that: "Everyone has the right to respect for his private and family life, his home and his correspondence".[1541] In Europe, Resolution 428 (1970) *containing a declaration on mass communication media and human rights* suggested that the right to privacy consisted of the protection of one's "private, family and home life."[1542] In the early 1970s, Resolutions leading up to the adoption of Convention 108 in Europe, addressed the fact that data pertaining to family life and one's home were of an "intimate" nature. More specifically, Resolution (73) 22 stated that "Examples of information concerning a person's intimate private life include information about his behaviour at home."[1543] The Explanatory Report of Resolution (74) 29 also suggested that inherently sensitive

---

[1537] *Deschênes*, *supra* note 1495.

[1538] See *Health Insurance Portability and Accountability Act of 1996*, *supra* note 1492 which is protecting the privacy of personal health information in transactions.

[1539] Rick Boucher, *A bill to require notice to and consent of an individual prior to the collection and disclosure of certain personal information relating to that individual*, 1st Sess. H. R., 111th Cong., (3 May 2010).

[1540] Karas, *supra* note 362 at 4.

[1541] *European Convention for the Protection of Human Rights and Fundamental Freedoms*, *supra* note 7.

[1542] Council of Europe, *Resolution 428*, *supra* note 1476 at para. 2: "The right to privacy consists essentially in the right to live one's own life with a minimum of interference. It concerns private, family and home life (…)."

[1543] See Council of Europe, *Explanatory Report: Resolution (73) 22*, *supra* note 56 at para. 19.

information included "the individual's conduct in his own home".[1544] Years later, private life still generally includes things relating to family life and one's home in North American jurisdictions such as Quebec.[1545]

(iii) Love, Sex and Sexual Orientation

The Resolutions (73) 22 and (74) 29 leading up to the adoption of Convention 108 in Europe, suggested that examples of information concerning a person's intimate private life included information about his sexual life.[1546] The Lindop Report (U.K., 1978) referred to the fact that sensitive information included the individual's "sexual activities."[1547] In France, the processing of data concerning sex life is prohibited, consistent with the relevant Directive 95/46/EC.[1548] In Quebec, private life includes things relating to love, sex, and intimate life.[1549] In the U.S., under the aforementioned Boucher Bill, "sensitive information" includes "sexual orientation".[1550]

(iv) Religious, Political and Philosophical Opinions

In Europe, Resolutions (73) 22 and (74) 29 both consider personal opinions to be part of an individual's intimate private life.[1551] According to the Lindop Report (U.K., 1978), trade unionists had urged that special restrictions be imposed on particular classes of information, especially information about religious or political affiliation.[1552] In France, the processing of special categories of data revealing political opinions, religious or

---

[1544] Council of Europe, *Explanatory Report: Resolution (74) 29*, *supra* note 65 at para. 18.

[1545] Trudel, "Privacy Protection", *supra* note 164 at 322: "Generally, private life includes things relating to (…) family life, one's home (…)."

[1546] See Council of Europe, *Explanatory Report: Resolution (73) 22*, *supra* note 56 at para. 19; See also Council of Europe, *Explanatory Report: Resolution (74) 29*, *supra* note 65 at para. 18.

[1547] Lindop, *supra* note 96 at 153-54, para. 18.25.

[1548] *Loi informatique et liberté*, *supra* note 131 at c. II, s. 2, art. 8 (I). See also EC, *Directive 95/46/EC*, *supra* note 99 at art. 8.

[1549] Trudel, "Privacy Protection", *supra* note 164 at 322: "Generally, private life includes things relating to love and sex (…). Private information may also include an individual's sexual orientation, anatomy and intimate life."

[1550] Boucher, *supra* note 1539.

[1551] See Council of Europe, *Explanatory Report: Resolution (73) 22*, *supra* note 56 at para. 19; See also Council of Europe, *Explanatory Report: Resolution (74) 29*, *supra* note 65 at para. 18.

[1552] Lindop, *supra* note 96 at 45-46, para. 5.34 and also at 153-54, para. 18.25.

philosophical beliefs are prohibited, in line with Directive 95/46/EC on this issue.[1553] In Quebec, private life usually also includes matters relating to an individual's religious, political and philosophical opinions.[1554] In the U.S., the recent Boucher Bill proposed suggests that "sensitive information" includes "religious beliefs".[1555]

(v) Race and ethnicity

The Lindop Report (U.K., 1978) discussed the fact that some urged that special restrictions be imposed on information about an individual's race.[1556] In France, the processing of special categories of data revealing "racial or ethnic origin" is prohibited, in line with the relevant Directive 95/46/EC.[1557] In its 2009 report, RAND Corporation also concludes that "racial information" is sensitive.[1558] In the U.S., according to the Boucher Bill, "sensitive information" includes "race or ethnicity".[1559]

(vi) Personal Affiliations

At the end of the nineteenth century, Warren and Brandeis expressed their concerns with protecting information about "the private life, habits, acts, and relations of an individual."[1560] In certain jurisdictions such as France, the processing of special categories of data revealing trade-union membership has been prohibited, consistent with the relevant Directive 95/46/EC.[1561]

[1553] *Loi informatique et liberté*, *supra* note 131 at c. II, s. 2, art. 8 (I). See also EC, *Directive 95/46/EC*, *supra* note 99 at art. 8.

[1554] Trudel, "Privacy Protection", *supra* note 164 at 322: "Generally, private life includes things relating to (…) one's (…) religious, political and philosophical opinions."

[1555] Boucher, *supra* note 1539.

[1556] Lindop, *supra* note 96 at 45-46, para. 5.34.

[1557] *Loi informatique et liberté*, *supra* note 131 at c. II, s. 2, art. 8 (I). See also EC, *Directive 95/46/EC*, *supra* note 99 at art. 8.

[1558] Robinson et al., *supra* note 151 at 48.

[1559] Boucher, *supra* note 1539.

[1560] Warren & Brandeis, *supra* note 5, at 216. See also Nissenbaum, *supra* note 230 at 119.

[1561] *Loi informatique et liberté*, *supra* note 131 at c. II, s. 2, art. 8 (I). See also EC, *Directive 95/46/EC*, *supra* note 99 at art. 8.

(vii) Financial Information

Concerns were raised by the Lindop Report of the possibility of data exchanges amongst marketers involving information drawn from "those in affluent financial circumstances".[1562] In the United States, the *Right to Financial Privacy Act of 1978*[1563] accords special status to information about financial holdings. More recently, PIPEDA states that some information, such as "income records", is almost always considered to be sensitive.[1564] In Quebec, a bank was held liable (damages were granted) for having disclosed a women's bank account information to her soon-to-be-ex-husband.[1565] In 2009, some European experts argued that special categories of sensitive data should include "financial data".[1566] Under the U.S. Boucher Bill proposed, "sensitive information" includes "financial records and other financial information associated with a financial account, including balances and other financial information".[1567]

(viii) Private Communications

The European Convention on Human Rights adopted in 1950, at article 8 (1), states that "everyone has the right to respect for (…) his correspondence".[1568] In the U.S., the *Electronic Communications Privacy Act* of 1986[1569] was enacted to extend government restrictions on wiretaps from telephone calls to include transmissions of electronic data by computer. Title I of the ECPA protects "wire, oral, and electronic communications" while in transit,[1570] while Title II of the ECPA, the *Stored Communications Act*[1571] protects "communications held in electronic storage" (on computers). The C.c.Q. (1994) states that intentionally intercepting or using "someone's private

---

[1562] Lindop, *supra* note 96 at 143, para. 17.20.

[1563] In the United States, the *Right to Financial Privacy Act of 1978*, 12 U.S.C. §§ 3401–3422 accords special status to information about individuals' financial holdings.

[1564] PIPEDA, *supra* note 63 at Schedule 1 (s. 5), principle 4.3.4.

[1565] The Court awarded $1,000 in damages. See *Demers v. Banque Nationale du Canada*, B.E. 97BE-330 (C.Q.).

[1566] Robinson et al., *supra* note 151 at 28.

[1567] Boucher, *supra* note 1539.

[1568] *European Convention for the Protection of Human Rights and Fundamental Freedoms*, *supra* note 7.

[1569] Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2510-2522).

[1570] It sets down requirements for search warrants that are more stringent than in other settings.

[1571] Codified at 18 U.S.C. ch. 121 §§ 2701–2712.

communications" is considered as an invasion of privacy.[1572] In Europe, the *Security Measures for Personal Data: A Guide to the New Data Protection Rules* (2001) provides that organizations dealing with personal information "of a private or sensitive nature" such as "people's private telecommunications", need to have very robust standards of security in place.[1573]

(ix) Location Data

The same categories of data have been considered as "intimate" and in need of protection for at least the last forty years or so, throughout various jurisdictions (Europe and Canada). With time, certain new categories of "intimate" type of data may gradually arise. For example, more recently, location data is creating privacy concerns.[1574] The physical or geographic location of an individual may, for instance, be exploited by stalkers. Furthermore, the location of an individual can disclose this individual's personal interests. Let us suppose that a gay pride parade is to take place at location X and time Y – if John Smith can be "placed" at location X during time Y, assumptions can be made about his sexual orientation (whether accurate or not).[1575] In Europe, the issue of location data has been governed by a special directive since 2002.[1576] In Canada, location data is considered *personal information* by the OPCC in part because of its potentially sensitive nature.[1577] In 2009, U.K. privacy experts mentioned that special categories of sensitive data should include location data.[1578] There have been various discussions in the U.S. about whether location information should be given the same privacy protections as medical data, because of its

---

[1572] Art. 36 (2). C.c.Q.

[1573] EC, *Security Measures*, *supra* note 1068.

[1574] See generally (regarding privacy and location-based services) Gratton, *Internet and Wireless Privacy*, *supra* note 193; Colin Bennett & Lori Crowe, *Location-Based Services and the Surveillance of Mobility: An Analysis Of Privacy Risks In Canada* (Ottawa: OPCC, 2005). See also Hariton, Lawford & Palihapitiya, *supra* note 197; Robinson et al., *supra* note 151 at 28.

[1575] See Gratton, *Internet and Wireless Privacy*, *supra* note 193 at 33-36, which elaborates on dynamic profiling using historical location data and on location-specific profiling using real-time location data.

[1576] EC, *Directive 2002/58/EC*, *supra* note 860.

[1577] OPCC, *PIPEDA Case Summary #2006-351*, *supra* note 214.

[1578] Robinson et al., *supra* note 151 at 28.

potentially sensitive or intimate nature, and certain U.S. jurisdictions have recently even begun considering regulating the collection, use and disclosure of this kind of data.[1579]

(d) Evaluating Profiles

There are also new types of data (as discussed in section 1.2.2) that may also be viewed as "points of collection" or collection tools, such as IP addresses, cookies, RFID tags or chips, wireless devices, etc. These may also be included under the category of data which is of an "intimate" nature.

An issue with profiles is that individual pieces of information, examined in isolation to determine whether they are of "intimate" nature (or that they disclose intimate details and lifestyle choices of the individual) may not qualify as such. As suggested by Ian R. Kerr and Jenna McGill: "*information can always be reduced to smaller and smaller bits of data* which, through the reductive process, eventually no longer reveal a biographical core of information." [1580] On this issue, Renée Pomerance suggests that:

> "Viewed in isolation, a single piece of data may appear innocuous. But it will often become highly revealing when entered into a composite profile. In this respect, it is like a jigsaw puzzle piece. While unintelligible on its own, the piece might disclose an integral part of the picture when slotted into its surrounding context. Even if *all* of the jigsaw pieces are uninformative on their own, they can, in combination, create something detailed, complete and recognizable. (…) As the bits are pieced together, a very clear picture can emerge. The collection of massive amounts of information can therefore strike very poignantly at the "biographical core" that defines personal identity. This is the case, even if no single item of information, standing alone, would pass the 'intimacy" threshold."[1581]

Pomerance believes that the test in the context of the expectation of privacy should not be whether the data relates to "inherently private choices of fundamental importance", whether it concerns "intensely personal considerations", or whether it discloses "core

---

[1579] See Newland, *supra* note 799: See also the Boucher Bill introduced in the U.S. in May 2010, **"**Sensitive information" which can't be collected and stored without an explicit opt-in assent includes "Precise geolocation information". Boucher, *supra* note 1539.

[1580] Kerr & McGill, *supra* note 625 at 414.

[1581] Pomerance, *supra* note 233 at 289.

biographical information".[1582] Instead, the real question should be: "whether the process as a whole does violence to the right to an inviolate personality".[1583] Framed in this way, according to Pomerance, the true impact of data-mining can be meaningfully assessed since "the cumulative effective of a series of minor intrusions can add up to a serious invasion."[1584] According to Ian R. Kerr and Jenna McGill, as new and emerging information technologies continue to come before the courts, the current reductionist inclination that asks whether the intercepted data is, *on its own*, meaningless will and ought to give way to the very opposite approach, namely: "whether the bundle of information that is made available by means of the search, *once assembled,* ought to attract a reasonable expectation of privacy."[1585] This latter approach would "recognize the jigsaw nature of the data/information/knowledge/wisdom chain and the importance of each piece of the puzzle in telling a story despite the fact that no single piece could do so on its own".[1586]

Although these authors are voicing their position and concerns in connection with the type of information to be protected under the Canadian Charter expectation of privacy test, we can draw an analogy with the evaluation of profiles in light of this criterion of "intimate" nature. The data evaluated needs to take into account the profile as a whole, in order to determine if this profile somehow could reveal information of an "intimate" nature.[1587] For example, an online profile which includes data relating to illicit websites, racy books and stigmatizing diseases should definitely qualify as being of an "intimate" nature, even if the majority of the information constituting the profile is not necessarily considered sensitive. Reidenberg and Schwartz suggest that data profiles may frequently approach the categories of sensitive data that are subject to processing prohibitions under Directive 95/46/EC.[1588] Wong suggests that it is not always possible

---

[1582] *Ibid*. at 290.

[1583] *Ibid*.

[1584] *Ibid*. at 289-90.

[1585] Kerr & McGill, *supra* note 625 at 430-31.

[1586] *Ibid*.

[1587] Paul Ohm states that "But because the database of ruin can be built almost entirely with nonsensitive data, regulators should beware not to make too much of this step in the analysis." See Ohm, *supra* note 562 at 1768.

[1588] Reidenberg & Schwartz, *supra* note 203 at 84. EC, *Directive 95/46/EC*, *supra* note 99 at art. 8.

to draw an inference of an individual's "intimate" data based on the mere fact that he or she has visited a particular website.[1589] The same reasoning can be applied to an individual that has visited a specific location. Nevertheless, once the inference or assumption is made and becomes part of the profile (regardless of whether the information is accurate or not) disclosure of the data may create a risk of subjective harm and should therefore be governed as *personal information* under DPLs.[1590]

For example, in order to determine if a profile collected as part of behavioural marketing may create a risk of harm upon being disclosed, we would need to take into account the kind of information collected (is it of an "intimate" nature?), whether the information collected is already "available" and whether the profile is "identifiable". If the profile is "used" to the detriment of an individual, then section 3.2.2 details the relevant test to follow. If the profile is used to market back to the profile, then, as I have explained elsewhere (section 3.1.2.3.1), I believe this activity to be a potential "disclosure".[1591]

With new Internet technologies, a disclosure may in certain cases relate to data associated with a device or an object that potentially belongs to an individual. While industry players have a tendency to exclude new types of data (or data generated using new collection tools) from the definition of *personal information*,[1592] there may still be a disclosure that may trigger a risk of subjective harm (even if the data relates to a device or object instead of an individual). For example, RFID tags may be used on

---

[1589] Wong & Garrie, *supra* note 187 at 581: "For example, if a user visited a Christian website, it is not necessarily true that the user was doing so for his or her religious beliefs rather than for research purposes. Certainly, repeated visits to a particular website or websites of a similar nature may indicate that the user holds particular religious beliefs. But it does not always follow that a website will necessarily correlate with a user's sensitive data as defined under Article 8(1). The DPD does not draw a distinction in ascertaining the user's intention when he or she visits a website."

[1590] See section 3.2.2.2 entitled "Accuracy of Information Used" which explains the fact that even if the information disclosed is not true, it may still trigger a subjective harm.

[1591] See section 3.1.2.2 which elaborates on the relevant test under which we need to assess whether the information used to market back to a given device ("disclosed" back) is of an "intimate" nature, "available" and "identifiable" in order to determine if the disclosure triggers a risk of subjective harm.

[1592] See section 2.1.1.2.1(b) entitled "Organizations Communicating their Practices in Conflict of Interests", and section 3.1.2.2.1(b)(i) entitled "Qualifying the Information" which elaborate on this issue.

certain objects that contain information revealing the nature of the object (since personal belongings can reveal very intimate details of a given person's private life).[1593]

In the context of new Internet technologies, if the risk of harm detailed in section 3.1.2.1 is otherwise present, meaning that the criteria pertaining to the data detailed in section 3.1.2.2 (data "identifiable", of "intimate" nature and not already "available") are also met, then information collected by new types of tools should be covered.

***

The fact that the information at stake may be of an "intimate" nature is relevant in the overall test used in evaluating the type of harm that may be triggered by the disclosure of the personal information. The "intimate" nature of the data is usually important when we are talking about a disclosure that may trigger some type of embarrassment or humiliation for the individual concerned. However, evaluating whether the disclosure of a given data or profile creates a *risk of subjective harm* is not only based on the intimate nature of the information. As part of the test which I propose, the "availability" of the data (or concurrently how the individual treats this data) is also part of the equation. I discuss the "availability" criterion next.

3.1.2.2.3. Availability of Information

In the context of the Internet, with the increase in the volume of data exchanges and disclosures[1594] and the social changes through web 2.0 and OSNs (with online users voluntarily disclosing and sharing their personal information)[1595] the principle of pre-determined categories of "sensitive" data may prove to be challenged. I already discuss in section 2.1.2.3.2 how, a photograph posted online showing the ethnic origin of an individual, would be regarded as sensitive data irrespective of the context or purpose in which the photograph was published. I also discuss how the current

---

[1593] Article 29 Data Protection Working Party, *RFID technology*, *supra* note 196 at 7: "Consider the case where anyone in possession of a reader can detect banknotes, books, medicines or valuable objects of passers by. The knowledge of this information by third parties will invade the privacy of the person who owns the object."

[1594] See section 1.2.1 entitled "Increase in Volume of Information" for details.

[1595] See section 1.2.1.2 entitled "New Ways of Using the Internet: Web 2.0" for details.

categorization of "sensitive data" (such as in Directive 95/46/EC) is not adequate since it is solely on the actual "nature" of the data.[1596]

If a given set of information is already in circulation, this will reduce the potential for subjective harm upon disclosure. Bearing in mind the other two suggested criteria which are important to establish this kind of harm at the disclosure level (information of "intimate" nature[1597] and the fact that the information is "identifiable" to a specific individual),[1598] the fact that the information is already or has been in circulation (vs. information which was never available or only available on a limited basis) is indeed relevant.

In principle, the fact that a given individual X is homosexual may initially be viewed as creating a *risk of harm* upon disclosure to third parties or to the public. The nature of the information (being "homosexual") is of "intimate" nature[1599] and this information relates to individual X, identified by first and last name (or identified by any other relevant identifiers) which makes this information "identifiable".[1600] But once this information is analyzed through the "availability" test, it can modify the outcome of the assessment of the *risk of harm* at the disclosure level. This would be the case, for instance, if the individual's sexual orientation were public knowledge (for instance the individual has disclosed this fact on his or her OSN public profile) at the time of the disclosure. As a matter of fact, a disclosure of this kind of "intimate" and "identifiable" data would therefore neither embarrass nor humiliate the individual concerned.[1601]

Certain case law rendered also confirm that information disclosed will create a *risk of harm* only if it is not already available or known to the individuals to which it is disclosed. In the U.S., if an intimate fact about a person is known to others, many

---

[1596] This would translate in the publication of any personal information on the Internet constituting the processing of "sensitive data".

[1597] See section 3.1.2.2.2 which elaborates on this "intimate" criteria.

[1598] See section 3.1.2.2.1 which elaborates on this "identifiable" criteria.

[1599] See section 3.1.2.2.2(c)(iii) entitled "Love, Sex and Sexual Orientation" which elaborates on the fact that sexual orientation is information of intimate nature.

[1600] See section 3.1.2.2.1 which elaborates on this "identifiable" criteria.

[1601] See section 3.1.2.1.1 entitled "Harm Directly Linked to Disclosure: Subjective (and Psychological)" which elaborates on the kind of subjective harm taking place upon information being disclosed.

courts conclude that it is no longer private (and concurrently that there is no harm in disclosing it or making it available). This was the U.S. case in *Sipple v. Chronicle Publishing Co.*[1602] where newspapers disclosed the fact that Oliver Sipple, who heroically saved President Ford from an assassination attempt, was homosexual. The court concluded that his sexuality was not private because it was already known in the gay community.[1603]

I maintain that in the event that information is already available to the recipient of the information, then the risk of harm that may be triggered by the disclosure of information to this recipient is less substantial. The three relevant criteria in assessing the *risk of harm* resulting from the disclosure of personal information need to be taken into account "together". Intimate data will more than likely increase the *risk of harm* upon being disclosed, however this criterion needs to be tempered with the "availability" and "identifiability" criteria, in order to allow for a proper assessment. For example, the disclosure by an organization of the sexual orientation of an individual (information of an "intimate" nature) may create a higher risk of harm (upon the disclosure of this data) if this information is also very "identifiable" (for instance, it can be linked to a unique individual) and if it was initially not "available" anywhere, for example if the individual concerned never disclosed this fact. The *risk of harm* would be diminished if the individual revealed his sexual orientation online on many occasions, or even worse, on websites that are public or accessible to all online users.[1604]

This section will first detail why the "availability" criterion is relevant in evaluating the risk of subjective harm taking place at the disclosure level, and examine how and why certain DPLs have made an attempt to limit the application of DPLs to certain data

---

[1602] 201 Cal. Rptr. 665 (Ct. App. 1984) at 666 [*Sipple*].

[1603] *Ibid*. at 669: "[P]rior to the publication of the newspaper articles in question [Sipple]'s homosexual orientation and participation in gay community activities had been known by hundereds of people in a variety of cities (…)."

[1604] If a gay individual publicly advertises on Facebook that he is "gay" and he has hundreds or thousands of friends and a public profile, then he is logically more likely not to care (not to be humiliated nor embarrassed) if this information is, for instance, used to market back to him online (for example, if this information is part of his behavioural profile). Of course, there are various distinctions within this example. For example, the fact that this information (him being gay) is only available to a few friends on a private OSN profile may change the picture, and increase the risk of subjective harm upon the disclosure of this information as it lowers the extent of the availability of this information prior to the disclosure.

which are either publicly available, or information that the individual has himself or herself made widely available. Second, given that in many situations, the information disclosed has already been available or disclosed at some level, I also discuss the criteria that may provide guidance in evaluating the *risk of harm* in the event that personal information, already available to a certain extent, is being made "increasingly available".[1605]

(a) Exemptions for Already Available Information

The availability of personal information has a direct impact on (as it may increase or decrease) the *risk of subjective harm* that accompanies the disclosure of personal information. As discussed below, certain DPLs in fact acknowledge that the *risk of harm* is lower if the information disclosed is already publicly available, as well as if it has been made available by the individual concerned.

(i) Publicly Available Information

In light of the amount of information widely available in this Information Age, certain jurisdictions have recently made it a point to exempt data publicly available from the applicability of DPLs. Under Canadian and French DPLs, personal information may only be collected, used or disclosed in a commercial context with the consent of the individual to whom it pertains, unless an exception applies. Exceptions relating to *publicly available information* are set out in certain Canadian DPLs or statutes, namely ones pertaining to Canada, B.C. and Alberta.[1606] To determine whether information is publicly available under PIPEDA, one must consider not only *what* it is but also *where* it was found.[1607] B.C.'s and Alberta's regulations are substantially similar, however, the

---

[1605] See section 1.2.5 entitled "Increased Availability of Data" which elaborates on the "increased availability" of information.

[1606] See PIPEDA, *supra* note 63 at section 7 entitled "Collection without knowledge or consent". The Alberta and the BC DPLs have similar exemption for publicly available information. See Alberta DPL, *supra* note 114 at Part 2, Division 3, s. 14 (e); B.C. DPL, *supra* note 115 at Part 6, s. 18 (1) (a).

[1607] PIPEDA has *Regulations Specifying Publicly Available Information*, *supra* note 544, which have been a force since 2001 and which exclude certain type of publicly available information. Under PIPEDA, personal information may only be collected (and used or disclosed) in a commercial context with the consent of the individual to whom it pertains unless an exception applies. Exceptions relating to publicly available information are set out in the regulations made under PIPEDA. To determine whether information is *publicly available*, one must consider not only *what* it is but also *where* it was found. The following personal information is exempted from PIPEDA's consent requirement: (a) Name, address and telephone number that can be found in a publicly available telephone directory, so long as the individual in question

requirement that information appearing in a publication be provided by the individual is relaxed in these provinces.[1608] In Alberta, it is sufficient that it be "reasonable to assume" that the individual provided the information. In B.C., the requirement is removed entirely. To rely on these exceptions, an organization would need to confirm that the contact information in its database can be found in publicly available directories and that the affected individuals had the opportunity to refuse publication in those directories.[1609] In some provinces, the organization would also need to verify that publications from which it collected information were published with the author's consent.

The Quebec legal system has no general exception to the consent requirement for personal information that is *publicly available.*[1610] It is therefore different from the federal, B.C. and Alberta schemes since the exception does not depend on whether the personal information is publicly available, but on whether it is considered "public" under law.[1611] In France, the CNIL, in reviewing directories on the Internet, has argued that data accessible to the general public does not lose its protection as "nominative" information.[1612] The situation is therefore similar to Quebec in that personal information

---

has the option of refusing the publication of his or her information; (b) Information including (but not limited to) name, title, address and telephone number found in a publicly available professional or business directory, listing or notice, so long as the organisation's collection and use of the information relates directly to the purpose for which the information was listed in the directory, listing or notice; (c) (…); and (d) Information in a publicly available hard copy or electronic publication, where the individual has provided the information.

[1608] See also the Alberta DPL, *supra* note 114 at Part 2, Division 3, s. 14 (e) and Part 2, Division 4, s. 17. In BC, see B.C. DPL, *supra* note 115 at Part 4, s. 12 (1) (e), Part 5, s. 15 (1) (3) and Part 6, s. 18 (1) (a).

[1609] *Ibid*.

[1610] Karl Delwaide & Antoine Aylwin, "Leçons tirées de dix ans d'expérience : la *Loi sur la protection des renseignements personnels dans le secteur privé* du Québec" (2005) 233 Développements récents en droit de l'accès à l'information 279 at 298.

[1611] Quebec DPL, *supra* note 110 at s. 1, para. 5. Nothing in the Quebec DPL defines the contours of this restriction or specifies under what laws an information would be considered to be public. In Quebec, certain information is also "public" by law. See for example the Quebec *Act respecting access to documents held by public bodies and the protection of personal information,* at section 55 which states*: "*55. Personal information which, by law, is public is not subject to the rules for the protection of personal information set out in this chapter." Moreover, there is no regulation identifying categories of personal information not subject to the consent requirement, such as under the federal, B.C. and Alberta schemes.

[1612] See CNIL, *17e Rapport*, *supra* note 345. Specifically, the CNIL noted that consent for disclosure of directory information in a paper format should not preclude opposition to disclosure of the same information on-line or on CD-ROM. The rationale for this distinction lies in the CNIL's concern for the risks to finality that may arise with the availability of directory information on-line.

available publicly still remains governed by the French DPL (although there is an exception in France, if the individual concerned has made his or her information publicly available).[1613]

These jurisdictions are not right or wrong in deciding to include or exclude publicly available information from the application of DPLs. On one hand, there is much less harm in disclosing already available information, so it may be a logical thing to do to provide for an exemption for this kind of data. But there are still concerns with not protecting this data since it may be combined with other available data and re-disclosed in such a way that may portray the individual in a different light or provide additional knowledge about the individual. Basically, the main concern is with the aggregation of information. This issue is discussed in great length in sections 1.2.3 and 1.2.5.

(ii) Data Made Available by the Individual

Stan Karas articulates the view that "if people tend to treat different kinds of private information differently, perhaps should the law."[1614] Some are claiming that changes with regards to how individuals view their privacy have recently taken place and contend that the social changes inherent to web 2.0 with individuals voluntarily sharing their personal information may perhaps reflect a changing mentality with regards to privacy and an important change in how individuals value their privacy.[1615] For instance, Mark Zuckerberg founder of Facebook thinks social media has changed how we think about information: "People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people…[this] social norm is just something that has evolved over time."[1616] This discussion raises an interesting point: the fact that the way which individuals treat their personal information may definitely have an impact on the type of *subjective harm* which they may sustain

---

[1613] See section 3.1.2.2.3(a)(ii) which elaborates on this issue.

[1614] Karas, *supra* note 362 at 10-11.

[1615] Robinson et al., *supra* note 151 at 15: "(..) for example individuals willing to give up personal information for small gains such as by telling personal stories to become part of a trusted community of shared interests, and sharing content increasingly via userfriendly and accessible platforms such as YouTube and SNS".

[1616] Crovitz, *supra* note 283.

upon this data being disclosed, for instance if they have themselves already rendered this information widely available to third parties or to the public.

As early as 1970, Resolution 428 *containing a declaration on mass communication media and human rights* suggested that individuals who "by their own actions, have encouraged indiscreet revelations about which they complain later on, cannot avail themselves of the right to privacy."[1617] Certain Canadian and French DPLs consider the fact that individuals have been involved in making their own data available when regulating certain situations. For instance, according to the Alberta and the B.C. DPLs, an individual is deemed to consent to the disclosure of his or her personal information in certain situations, for example if the individual voluntarily provides the information to the organization for that purpose, and it is reasonable that a person would voluntarily provide that information.[1618] The French DPL provides for certain exclusions (no consent is required) for personal data rendered public by the individual concerned.[1619]

Certain jurisdictions therefore implicitly acknowledge the fact that the disclosure of personal information, that was already made available or rendered public by the individual, may not be as harmful as the disclosure of information that has remained confidential. The problem with these exemptions, as already discussed in section 1.2.3, is the potential for aggregation or linkage of different data. With the Information Age, there is a lot of data already available or that has been made available by the individual at some point in time. Some claim that whatever is disclosed online is made available forever and to everyone:

> "Much of what occurs online, like blog posting, is intended to be an open declaration to the world, and law enforcement is within its rights to read and act on what is written."[1620]

I argue that in our Information Age, given that most personal information is or has been at some point available, we can not naively invoke that information, no matter how sensitive, somehow becomes public property simply because it has been disclosed.

[1617] Council of Europe, *Resolution 428*, *supra* note 1476 at para. 2.

[1618] Alberta DPL, *supra* note 114 at Part 2, Division 2, s. 8 (2).

[1619] *Loi informatique et liberté*, *supra* note 131 at c. II, s. 2, art. 8 (II) (4).

[1620] See MacRonin, *supra* note 267.

This would be following the privacy as secrecy paradigm, under which once a fact has been disclosed, it is no longer private. Many raise their concern with this paradigm. Solove suggests that: "In a variety of legal contexts, the view of privacy as secrecy often leads to the conclusion that once a fact is divulged in public, no matter how limited or narrow the disclosure, it can no longer remain private."[1621] Sociologist Edward Shils notes, contrary to privacy as secrecy, that individuals do not intend an act of disclosure to be limitless.[1622] Solove suggests that we often expect privacy even when in public, and that individuals want to keep things private from some people but not others:

> "Not all activities are purely private in the sense that they occur in isolation and in hidden corners. When we talk in a restaurant, we do not expect to be listened to. A person may buy condoms or hemorrhoid medication in a store open to the public, but certainly expects these purchases to be private activities." [1623]

A contrario, the fact that information (which is not necessarily of an "intimate" nature) has been kept confidential and away from circulation by the individual concerned, should be taken into account in evaluating this *risk of harm* in the context of the disclosure of this information. For example, certain individuals may have an issue with having their names and addresses in the electoral register at the public library.[1624] An individual which has been the victim of stalking in the past may keep his or her personal home address confidential, even if this information is not usually necessarily viewed as "intimate". Others may wish to keep their age confidential.[1625] While these kinds of data are not inherently "intimate" in nature, the fact that this data was kept confidential by the individual who made sure that this data was not in circulation should

---

[1621] He suggests that for example, the Court's Fourth Amendment jurisprudence adheres to the notion that matters that are no longer completely secret can no longer be private. In a series of cases, the Court has held there can be no "reasonable expectation of privacy" in things exposed to the public, even if it is highly unlikely that anybody will see or discover them. Solove, "Conceptualizing", *supra* note 23 at 1107.

[1622] *See* Edward Shils, "Privacy: Its Constitution and Vicissitudes" (1966) 31 Law & Contemp. Probs. 28 at 305, discussed in Solove, "Conceptualizing", *supra* note 23 at 1108.

[1623] Solove, "Privacy", *supra* note 1 at 1439-40.

[1624] Lindop, *supra* note 96 at 153-54, para. 18.25.

[1625] See for example: "Why you can't get old in Hollywood: Hollywood industry groups are trying to stop the Internet Movie Database from publishing their members' birth dates. A serious privacy issue — or just Tinseltown vanity?" The week (21 June 2010), online: The Week <http://theweek.com/article/index/204277/why-you-cant-get-old-in-hollywood>.

be taken into account when evaluating the *risk of harm* arising from the disclosure of this information.[1626]

The fact that the individual is aware that his or her information is available and does nothing to remove it from circulation should be equally relevant. Individuals may contribute to how the personal information of others is made available because they may, for example, disclose the information of others on blogs and OSNs. If an individual has knowledge, for example, that his or her personal information is published on a public blog or OSN and does nothing to limit this availability, then one could reasonably conclude that a new disclosure of this information already publicly available may not be very harmful to the individual.[1627]

How the individual treats his or her personal data will have an impact on the kind of subjective harm that may take place at the disclosure level. It is important to determine the extent of the increased availability (pre and post disclosure), which is relevant to the overall subjective harm assessment test. Some of the elements to consider in the event that information available is made "increasingly available" are detailed below.

(b) Determining if Increased Accessibility is Harmful

While there is definitely a link to be made between qualifying data as "intimate" and its availability, I argue that the two should be analyzed separately. While the "availability" of the data may decrease the *risk of harm* of a given disclosure of personal information, it is not because the data is available somewhere, that it is automatically no longer private or that this data should not be protected by DPLs. The Lindop Report discussed this issue as follows:

> "Equally, when data are regarded as private, that does not mean that they are, or should be, known only to the individual to whom they refer:

[1626] Under the proposed approach, organizations would need to presume that the information is not available, unless they have evidence demonstrating otherwise.

[1627] For example, if an individual is "tagged" on Facebook (identified as being the individual on a picture posted online on Facebook), is informed of this tag and never removes the tag, then it may be reasonable for an organization to assume that this individual may have implicitly consent to their personal information being available on Facebook. Individuals may have more difficulty making a case that a new disclosure of the same "already available" information on the same medium is harmful to them.

> rather it means that he wants them to be known only to him and to those others who he agrees should know them."[1628]

A few U.S. decisions reported by Solove suggest that individuals may still have some type of expectation of privacy even when in public and that therefore, the secrecy paradigm is not sustainable.[1629] Even though data is somewhat "available" doesn't automatically mean that the disclosure will not result in some type of harm for the individual.

In the Information Age, with new technologies and the web, most information that is disclosed may have been previously available to a certain extent. Instead of data being "disclosed", we can therefore speak of data being "increasingly available", further discussed in section 1.2.5. Therefore, in order to determine if a certain activity of "increased activity" creates a *risk of harm*, we need to evaluate how much more accessible or available the information will be "post disclosure". This can translate into the information being more easily available, more knowledge about an individual being available, or a higher number of interested parties accessing this information.

The fact that the information was already available or has been disclosed is irrelevant when assessing the harm of "increased accessibility". Solove suggests that "One must focus on the extent to which the information is made more accessible".[1630] An analysis of the circumstances and extent of the availability are necessary in order to properly assess the *risk of harm* resulting from the disclosure (or "increased availability") of personal information.

While various elements relating to the availability of the information would be relevant to determine if a certain risk of subjective harm is taking place under a full contextual approach (such as the identity of the recipient, his or her interest in knowing or accessing the information, the relationship of the parties, etc.), I will not discuss these criteria because they are unrelated to the information and the proposed approach is not

---

[1628] Lindop, *supra* note 96 at 10, para. 2.07.

[1629] See *McNamara v. Freedom Newspapers*, 802 S.W. 2d 901 at 903 (Tex. App. 1991); *Daily Times Democrat v. Graham*, 162 So. 2d 474 at 476 (Ala. 1964). These decisions are discussed in Solove, "A taxonomy", *supra* note 339 at 536.

[1630] *Ibid*. at 538.

a contextual approach.[1631] I will therefore discuss as much as possible elements which relate to the data itself: whether the information was already available, the fact that the user has himself or herself made this data available, whether the disclosure increased the knowledge that one may have pertaining to the individual concerned, the extent of the initial availability and the medium (online versus offline), the period for which the data has been available, the size of the audience that may access this available data, and the kind of efforts required to access the data. These are all relevant elements that need to be taken into account when determining whether a certain disclosure may create the subjective type of harm discussed in section 3.1.2.1, as discussed below.

(i) Increased Knowledge about an Individual (Aggregation – Datamining)

As we have seen in sections 1.2.5 and 3.1.2.2.3 (generally), data availability, particularly the circumstances with which information becomes available, exerts an influence over the application of DPLs. Moreover, when existing (available) data is grouped, mined or aggregated with other data sets, this process may reveal new facts about the individual concerned. The power of aggregation is different in the Information Age, one reason being that data gathering is so much more extensive than it once was.[1632] This means that aggregation of information may create even more concerns if, let's say, publicly available information can be collected without prior notice and consent.[1633]

In a 2009 finding, the Canadian OPCC refused to impute a consent requirement where "publicly available" information had been enriched by data aggregators and data miners. More specifically, in *PIPEDA Case Summary #2009-004*, the OPCC allowed enrichment of phone book information with demographic information from Statistics

---

[1631] See section 2.2.1.1 which elaborates on this issue.

[1632] The process of combining the data is easier, and the technologies and tools to analyze the data are more and more sophisticated, as detailed under section 1.2.3 entitled "New Identifying Methods".

[1633] This concern is also raised by René M. Pomerance, in Pomerance, *supra* note 233 at 293: "Although acts performed in 'public', especially is taken singly or in small numbers, may not be confidential, at least arguably a right to privacy may nevertheless be invaded through extensive or exhaustive monitoring and cataloguing of acts normally disconnected and anonymous. This, of course, is the very mischief created by data-mining, which is largely concerned with the collation of data that involves public or publicly discernable activities. Public or not, the collation of this information has the potential to invade that which is private (…)."

Canada without the necessity of obtaining the consent from the individuals concerned.[1634] The PIAC has shared its concern with this decision:

> "What the OPCC may have failed to appreciate is the fact that white pages phone book information was gathered for a completely different purpose than that to which it was put by data miners. The purpose of white pages listing information is to permit telephone subscribers to contact other subscribers easily in order to get the full benefit of the "network effect" of having all users on the phone network easily contactable. When directories were produced in machine-readable format, the CRTC allowed the provision of this information to other directory companies besides the incumbent local exchange providers on the basis of providing more competition in the directory business. This provision was hemmed in by significant privacy principles. However, the OPCC, in bestowing the title of "publicly available" upon this type of personal information (directory information) and then refusing to require consent for the new use the information after its "enrichment" with yet more personal information simply guts PIPEDA Principle 4.5. It ignores the general safeguards that the CRTC sought to uphold over the years in many decisions on directories. It allows an entire industry to be constructed with the express purpose of doing indirectly what PIPEDA forbids directly."[1635]

In France, a different outcome took place in a similar situation, when publicly available directory data was to be merged with other available information. France's Data Protection Authority, the CNIL announced on September 23, 2011 that it had found the French provider of universal telephone directory services, *Pages Jaunes,* guilty of violating several provisions of the French DPL.[1636] Pages Jaunes' web crawler function captured information contained on Facebook, Twitter and LinkedIn profiles of individuals having the same name as the individual being looked up in the directory service and "more complete profiles" were made available online without the requisite consent.[1637] The CNIL's decision illustrates that different and contradictory positions

---

[1634] OPCC, *PIPEDA Case Summary #2009-004, No Consent Required for Using Publicly Available Information Matched with Geographically Specific Demographic Statistics* (9 January 2009).

[1635] PIAC, *supra* note 448 at 6-7 [footnotes omitted]

[1636] The CNIL did not fine *Pages Jaunes*, but published a detailed warning, listing each privacy violation that the CNIL had identified during its investigation of *Pages Jaunes's* activities. See CNIL, "Carton rouge pour les Pages Jaunes" (23 September 2011), online: <http://www.cnil.fr/la-cnil/actu-cnil/article/article/carton-rouge-pour-les-pages-jaunes/> [CNIL, "Carton rouge"].

[1637] For example, if someone were to look up the telephone number of Eloïse Gratton, *Pages Jaunes* would show Gratton's phone number, and would also show information on social media sites relating to

can be taken on this issue (merging publicly available data and re-disclosing it), which is not a simple question of black or white. This French case also summarizes the concerns which remain with these kinds of exemptions for publicly available data, since many of the technologies are capable of being used in ways that erode the distinction between public and private space. According to Renée Pomerance: "Data-mining is insidious in another way. The concern arises at the point of collection, but it peaks at the point of collation."[1638] Aggregation would violate a privacy interest (or create a risk of subjective harm) when the aggregation increases what others know about a person, even if originating from public sources.

This means that the argument that there is no harm in disclosing publicly available information is very simplistic. The organization, prior to disclosing the data, must assess if the data to be disclosed has been mined, analyzed and whether the disclosure of the information will release additional information or increase the "knowledge" with regards to the individual concerned. Section 1.2.5 details the kinds of privacy concerns which can take place after already available information is made "more easily available" or when the disclosure of publicly available information, after being mined and analyzed and re-disclosed, increases the knowledge about the individual. Section 1.2.5.4 more specifically discusses the cases of researchers who collected information on Facebook, and analyzed datasets which they then wanted to release to the academic community as the results were potentially useful for various purposes. Under the B.C. DPL, there is actually an exemption for disclosing data for research purposes if this disclosure is not "harmful" for the relevant individuals, which is an assessment that needs to take into account of the linkage of the data with additional data:

> "An organization may disclose, without the consent of the individual, personal information for a research purpose, including statistical research, only if linkage of the personal information to other information is not harmful to the individuals identified by the personal information

individuals named Eloïse Gratton. The information displayed included photos, the name of employer, schools attended, geographic location, profession, etc.

[1638] Pomerance, *supra* note 233 at 284.

> and the benefits to be derived from the linkage are clearly in the public interest."[1639]

Directive 95/46/EC provides that "subject to adequate legal safeguards" and where there is clearly "no risk of breaching the privacy of the data subject", information may be processed solely for purposes of scientific research or may be kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics.[1640]

Various business models have recently been built around analyzing data already available. For instance, Mailana's Twitter analyzer discloses the twenty individuals a Twitter user most regularly interacts with.[1641] Various search engines groups all the data (pictures, email address, articles, documents, OSNs profiles, etc.) found on the web pertaining to a name searched.

Before disclosing information to another organization or to the public, the disclosing party would need to find out what kind of information the recipient of this information has (or is publicly available, as the case may be), and whether the disclosure may increase the knowledge that the recipient will have about the individual concerned. The aggregation of disclosed data together with data already in the hands of (or available to) the recipient may create a subjective harm if the resulting information increases "what others know about an individual", even if originating from public or available sources. The fact that the two sets of data, once merged, will reveal information of a more "intimate" nature, or will make the data disclosed or available even more "identifiable" should be taken into account, since this may increase the *risk of harm* upon the disclosure of already available information. I further discuss in section 3.1.2.3.2(b) the fact that the change in the medium will be relevant in assessing this risk of harm. While there may be less of a concern with search engines grouping already available information online, the issue may be different if one was making information available on the web, which information was not previously available through this medium (online).

[1639] B.C. DPL, *supra* note 115 at Part 6, s. 21 (1) (c).

[1640] EC, *Directive 95/46/EC*, *supra* note 99 at art. 13 (2).

[1641] See online: <http://web.mailana.com/demo/>; Kirkpatrick, "The inner Circles", *supra* note 334.

(ii) Type of Efforts Necessary to Access the Disclosed Data

The kinds of efforts required to access the information disclosed are also quite relevant. The Lindop Report (U.K. 1978) suggested that: "In theory, of course, much information which has once been published is accessible to anyone who is willing to spend enough time and trouble in retrieving it."[1642] Solove also illustrates the problem with another example: "Contrary to the judicial notion that any information in public records cannot be private, there is a considerable loss of privacy by plucking inaccessible facts buried in some obscure document and broadcasting them to the world on the evening news."[1643] As a matter of fact, there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information.

- "Place" of Availability

When the FIPs were initially being discussed, it was already acknowledged that the place or the area where the personal information was located had an impact on the type of harm resulting from an intrusion.[1644] The place where the personal information was previously available (prior to the disclosure) vs. the place where the information will now be available (post disclosure) will impact the *risk of harm* pertaining to the "increased availability" of the personal information.

As a general rule, though this is not always the case, offline data is not as easily accessible as online data. Most people would agree that as offline data becomes available online, the *risk of harm* tends to increase. For example, in reviewing directories on the Internet, the CNIL has argued that data accessible to the general

---

[1642] Lindop, *supra* note 96 at 270-71, para. 31.06; See also *ibid*. at 271, para. 31.07: "An example may illustrate this point. The history of a particular Jane Smith 30 years old may be quite well documented in the locality where she lived at the time. But if she now lives somewhere else – and even more of she has changed her name, for instance on marriage – her neighbours in her new locality may well known nothing about it, even though, in theory, they could look up the old newspaper and any other 'published' records in her place of origin – if they knew where that was. There is one vital datum which has never been 'published', and to which they do not have access unless Jane Smith chooses to give it to them: namely that the Jane Smith (or Jane née Smith) who now lives among them is the same Jane Smith to whom the 30-year-old records in the other locality."

[1643] Solove, "Privacy", *supra* note 1 at 1439-40.

[1644] *Report of the Committee on Privacy*, *supra* note 3 at 20, para. 67.

public did not lose its protection as "nominative" information.[1645] In this French case law, the CNIL noted that consent for the disclosure of directory information in a paper format should not preclude opposition to disclosure of the same information on-line or on CD-ROM.[1646] The rationale for this distinction lied in the CNIL's concern for the risks to finality that may arise with the "availability" of directory information, once online. Trudel suggests that if the information is available online, its physical location has much less of an impact on its accessibility, since as soon as a document is available on a server, it can be found using general Internet search tools or other specialized tools.[1647]

The ease of access should be taken into account when evaluating the *risk of harm* resulting from the disclosure of information: if the information is available online, can it be retrieved through a simple web search engine, is it available on a public profile (with no privacy settings) or, rather, is it only available on a website which is password protected?

Another issue is the fact that certain "places" have meaning, which will have an impact of the type of harm taking place at the disclosure level. Data can be more or less sensitive, depending on the context illustrated by the place of disclosure. For example, an individual's name appearing on a company intranet page listing employees has less privacy implications than the same name appearing on a "black list" related to credit ratings. So in evaluating the type of harm in the activity of disclosing the data, the place in which the data is made available will be relevant. Once information is online, the ease in accessing this information will often have a direct impact on the potential size of the audience for this data.

[1645] See CNIL, *17e Rapport*, *supra* note 345.

[1646] *Ibid*.

[1647] Trudel, "Privacy Protection", *supra* note 164 at 327-28: "Distance in space and the passage of time seem to have much less impact on the real availability of information. The Internet makes publication routine and information can easily be published outside of legitimate circles, thus the increased risk. Naturally, cyberspace is made up of both public and private spaces but the reference points that distinguish between private and public have been blurred." See also section 1.2.5.3 entitled "Spatial Shift" which elaborates on this issue.

- Size of Audience

The broadness of the audience post disclosure (vs. the audience which previously had access to this information) will be a relevant factor in determining the *risk of harm* resulting from the disclosure or "increased availability".[1648] As a matter of fact, certain courts have come to different conclusions regarding whether there is a privacy interest in information communicated to others. For example, in *Times Mirror Co. v. Superior Court*,[1649] the identity of a murder witness was disclosed in a newspaper article. Although the witness had confided in a few friends and family members, the court took the position that she had not "rendered otherwise private information public by cooperating in the criminal investigation and seeking solace from friends and relatives."[1650] In the U.S., in *Duran v. Detroit News, Inc.*,[1651] a former Colombian judge was attempting to lay low because of death threats and a bounty placed on her head by a drug lord.[1652] When a newspaper disclosed her address, the U.S. court took a different position and found no privacy interest because she had revealed it to a few people.[1653]

The fact that the information was available on a limited basis pre-disclosure vs. larger audience should be taken into account when determining if a disclosure will trigger a *risk of subjective harm*. It is not because a piece of information is available to a certain group of people, that the disclosure will not be harmful. To illustrate this thought, I already discussed the U.S. case *Sipple v. Chronicle Publishing Co.*[1654] in which after

---

[1648] The fact that only a few individuals of the information vs. hundreds or thousands of individuals has to be taken into account when evaluating the subjective harm at the disclosure level. See section 1.2.5.1 entitled "Shift in Size of Audience" which elaborates on this issue.

[1649] 244 Cal. Rptr. 556 at 558 (Ct. App. 1988).

[1650] *Ibid*. at 561, discussed in Solove, "A taxonomy", *supra* note 339 at 532. Solove also discusses other U.S. cases such as *Multimedia WMAZ v. Kubach*, 443 S.E. 2d 491 at 500 (Ga. Ct. App. 1994) in which the U.S. court found that the plaintiff's disclosure of his infection status to family, friends, and members of an HIV support group did not render this information otherwise public; and *Y.G. v. Jewish Hosp.*, 795 S.W. 2d 488 at 500 (Mo. Ct. App. 1990) in which the U.S. court held that the disclosure to doctors and other participants of the plaintiff's in vitro fertilization did not render that information public.

[1651] 504 N.W. 2d 715 (Mich. Ct. App. 1993) [*Duran*].

[1652] *Ibid*. at 718, discussed in Solove, "A taxonomy", *supra* note 339 at 531.

[1653] *Duran*, *supra* note 1651 at 720. The court found her identity to be "open to the public eye" because her work in Colombia had been disclosed in newspaper articles, and because she had occasionally used her real name in the U.S.

[1654] *Sipple*, *supra* note 1604.

newspapers "outed" Oliver Sipple, the court concluded that his sexuality was not private because it was well known in the gay community since "[P]rior to the publication of the newspaper articles in question [Sipple]'s homosexual orientation and participation in gay community activities had been known by hundreds of people in a variety of cities".[1655] Nevertheless, even though someone's sexual orientation may be common knowledge within a given community, a disclosure may open the door to a much wider circulation and therefore, may still present a certain risk of harm.[1656]

Once the data is released online, the audience and number of individuals who may access it is huge. Business models such as the Google Street View technology present a good case in point.[1657] The recent U.K. business model under which commercial CCTV footage is displayed on the Internet in order for Internet users to watch the footage and assist businesses in catching criminals is also raising privacy issues.[1658] This last business model also raises temporal issues: while CCTV footage taken from the security camera may usually be deleted by the business if there is no incident reported, once released on the Internet, it may become very difficult to keep any control on the duration of the availability of this footage. This takes us to the criteria of the "period" of availability.

- Period of Availability and Volume

The period for which the information is or has been available will also be a determining factor in evaluating the *risk of harm* resulting from the disclosure of information.[1659] The

---

[1655] *Ibid*. at 669. The court concluded that his sexuality was not private because it was well known in the gay community: "[P]rior to the publication of the newspaper articles in question [Sipple]'s homosexual orientation and participation in gay community activities had been known by hundereds of people in a variety of cities (…)." See Solove, "A taxonomy", *supra* note 339 at 531.

[1656] Information disclosed on the Internet, on a website that is accessed by many (high volume of visits), in English or in a language which is known by many individuals has to be taken into account. For example, a distinction should be made if the information is instead available in a rare dialect which is known to only a few hundreds of people (less "availability").

[1657] For details on the Google Street View service, see online: <http://www.google.com/help/maps/streetview/learn/using-street-view.html>. For details on privacy concerns with the Google Street View service (Google making available pictures online which can identify individuals), see Stephen Shankland, "Google begins blurring faces in Street View" *Cnet News* (27 August 2010), online: Cnet.com <http://news.cnet.com/8301-10784_3-9943140-7.html>.

[1658] Shah, *supra* note 319. See also Hamilton, *supra* note 319.

[1659] See section 1.2.5.2 which elaborates on the temporal shift which is now taking place with new technologies.

fact that the information was already available for months or years online will decrease this *risk of harm* versus the fact that the information was removed minutes after being made available online. In the early 1970s, the Lindop Report questioned the relevance of drawing a distinction between published and unpublished information.[1660] But it concluded that such a distinction would overlook two important facts: "the fact that no one can know everything, and the fact that people forget even what they once knew."[1661] The report went on to suggest that any piece of information about any data subject would at any given time be known only to a limited number of people.[1662] But Trudel discusses the temporal shift which has taken place on the Internet and the fact that the persistence of information entails that it can last longer than the circle in which it was legitimate and that "while it used to be taken for granted that the level of risk to privacy remained low or easy to control, as the Internet has spread, qualitative and temporal changes to the scale mean that there are greater threats."[1663] On this issue, Scheiner also suggests that part of the privacy concern nowadays relates to the fact that digital data can remain available indefinitely. Routine transactions such as credit card payments, paying tolls via transponders and opening OSN accounts all generate digital records that can be stored at very low cost (which may be often easier than having to sort and delete the information).[1664]

As a result, digital data never dies. As the "lifespan" of data increases, so too does its dissemination. Another issue that may come to light is whether the individual that ends up deleting the posted information then has the right to restrict the future use or disclosure of the information in question.[1665]

[1660] Lindop, *supra* note 96 at 270, para. 31.03.

[1661] *Ibid*. at 270, para. 31.04.

[1662] *Ibid*. at 270, para. 31.05: "The truth is that any piece of information about any data subject will at any given time be known only to a finite number of people. The number may be large or small, but (with very few exceptions) it will never comprise the whole of the population of the United Kingdom. Moreover, as time passes the number will necessarily become smaller – by death and by forgetting – unless the information is circulated anew. In short, personal information is not just either 'public' or 'private': there is a wide range of possible knowledge among the public for any given item."

[1663] Trudel, "Privacy Protection", *supra* note 164 at 328.

[1664] Greene, *supra* note 328.

[1665] Michael Zimmer, "Is it Ethical to Harvest Public Twitter Accounts without Consent?" (12 February 2010), online: Michael Zimmer.org <http://michaelzimmer.org/2010/02/12/is-it-ethical-to-harvest-public-

The volume or completeness of the data made "increasingly available" is also relevant since there is a difference between scattered pieces of information made more easily available and a fully assembled dossier that may be more harmful upon disclosure. I discuss elsewhere that the potential for correlation between data will increase the risk of harm of a given disclosure.[1666]

3.1.2.3. Subjective Harm: Applying the Approach to Recent Privacy Breaches or Activities

The approach proposed is meant to provide a framework under which only the data that may create a risk of *subjective harm* will qualify as *personal information* (and therefore, be regulated by DPLs). DPLs usually provide that the consent of the individual is necessary to the disclosure of his or her personal information.[1667] Supposing we maintain the consent-based model,[1668] then, under the approach proposed, if the risk of harm were medium to high, perhaps a more stringent type of disclosure and consent would be required. If the risk is present but is on the "low" side, then perhaps a disclosure and an opt-out type consent would be sufficient or the information should not be regulated under DPLs.

As has already been mentioned, in determining what kind of security measures to adopt and whether these measures are "reasonable", "necessary" or "appropriate" in accordance with the relevant DPL, the first step for the organization must be to determine the extent of the *risk of harm* to individuals upon the occurrence of a security breach (or a disclosure of personal information).[1669] Many have already determined

---

twitter-accounts-without-consent/>: "What if tomorrow, I decide to take my Tweet stream private. And I delete my blog posts. Does my affirmative action to purge my documents from the 'live' web mean that you (researcher) need to treat that previously archived material differently? (…) Once tweeted, a birdsong is gone forever. No deleting or taking back what's been broadcast to the world. If someone seeks privacy, they should seek another method of communication. If from the beginning, there was some kind of inherent expectation that tweets were private messages, then the situation might be different. But the whole idea of tweeting is to voluntarily publish or broadcast. It's different from, say, e-mailing or IMing."

[1666] See section 1.2.1.3 entitled "Easier Identification of Individuals" and section 1.2.3 entitled "New Identifying Methods".

[1667] See section 2.1.1.2 entitled "Notice and Choice Approach Challenged" and section 2.2.1.3.2(a)(iii) entitled "Subjectivity Pertaining to Collection, Use and Disclosure Activities" which elaborate on this issue.

[1668] Section 2.1.1.2 entitled "Notice and Choice Approach Challenged" discusses how the "Notice and Choice" approach is challenged in light of modern technologies and the Information Age.

[1669] See section 2.2.1.3.2(a)(iv) entitled "Subjectivity in Security Measures to Adopt and Retention Obligations" which elaborates on this issue.

that the "nature" of the information is relevant in assessing the risk of harm upon disclosure and that information which is not very "intimate" in nature such as "the name, address, or membership of a local drama group" does not need to be the subject of very robust standards of security.[1670] Using the purposive approach proposed, organizations will have to account for the "intimate" nature of the information in establishing the proper measures to adopt, while also assessing the other relevant criteria discussed in this section (whether the information is already "available" and whether it is "identifiable").

As discussed in section 2.2.1.3.2(a)(i), there are various "reasonable" tests under certain DPLs. For example, under PIPEDA, an organization may only disclose personal information "for purposes that a reasonable person would consider appropriate in the circumstances."[1671] Other DPLs (Alberta and B.C.) have similar reasonableness tests.[1672] I maintain that a first step in determining whether a given disclosure is "reasonable", is to determine if this disclosure will create a risk of subjective harm to the individual concerned (since the lower is this risk, the more chances that the disclosure be considered as reasonable).

I will now first discuss the type of subjective harm that may be triggered by behavioural advertising practices. Then, I will illustrate how the outcome of certain situations, case law or "privacy scandals", which can be assimilated to "disclosures" of information, would have been different if the approach proposed in this thesis had in fact been used.

3.1.2.3.1. Behavioural Marketing

Concerns pertaining to privacy intrusions and advertising are nothing new. In the 1970s, the marketing industry in the U.K. argued that the information used for marketing purposes was not particularly sensitive and should be regarded either as public information (where it derived from publicly available documents) or as

---

[1670] EC, *Security Measures*, *supra* note 1068.

[1671] PIPEDA, *supra* note 63 at Schedule 1 (s. 5), s. 5(3).

[1672] See section 2.2.1.3.2(a)(i) entitled "Reasonableness or Legitimacy Tests" which elaborate on this issue.

commercial property which companies should be free to put on the market.[1673] While the Lindop Report raised certain concerns (for instance that the information concerned was not always trivial or innocuous since items of information which were harmless in isolation could become sensitive if aggregated),[1674] it concluded nonetheless that since only a minority of people considered unsolicited marketing as "an intrusion", that the sending of unsolicited advertising was an unobjectionable practice.[1675] First, I maintain that advertising can be viewed as a "disclosure" activity, depending on the medium used to advertise, and second, that marketing back to online users is presenting new privacy concerns.[1676]

Using personal information for commercial prospection or advertising purposes can be viewed as a "use" or a "disclosure" of information. It can be viewed as a use of information in the sense that personal information is "used" to market back to the individual.[1677] It is also a potential "disclosure" of personal information since the individual targeted, upon receiving the advertisement, may suffer the subjective harm discussed in section 3.1.2.1.1 (being humiliated or embarrassed). If a marketing company is aware of a person's embarrassing medical condition (if this kind of information has been used to market back to the individual) naturally one may develop a fear that others may also be aware of this fact, triggering the harm discussed in section 3.1.2.1.2. It is also a potential "disclosure" of personal information, depending on the medium used to market back to the individual, which will have an impact on the *risk of subjective harm*.

[1673] Some industry players had even raised that a requirement to declare to customers every use made of information about them, or provide the data subject with access to his record, might impose "costs out of all proportion to the possible dangers". See Lindop, *supra* note 96 at 140, para. 17.08. See also *ibid*. at 142, para. 17.14.

[1674] *Ibid*. at 143, para. 17.19. The authors of this report also had the concern that to match products and services to the individual needs of consumers and organizations, the precise personal characteristics of each individual had to be known. See *ibid*. at 142, para. 17.14.

[1675] *Ibid*. at 141, para. 17.11.

[1676] Online, with new collection tools, it may be easier to collect information about the interests of individuals. I discuss the concerns pertaining to the "collection" of personal information by behavioral marketers in section 1.2.4 which elaborate on this issue.

[1677] Section 3.2.2 entitled "Risk of Objective Harm: Criteria to Take Into Account" elaborates on the test to follow at the "use" level.

For example, suppose that a given person is afflicted with a stigmatizing medical condition and, from time to time, receives discounts (in the form of an e-mail or regular mail) for medication associated with the disease in question. Unless there is someone literally standing behind them at the exact moment that they open the mail or that someone else reads the message by mistake (or illegally), then there is actual no disclosure to speak of. Only the targeted individual will actually view the promotion. If the same advertisement promoting this medicine is sent by fax, there are more chances that another person, other than the individual targeted by the advertisement, views the promotion (depending on the amount of people accessing the same fax machine, etc.).[1678] Nevertheless, devices that are connected to the Internet (laptops, iPads etc.) are often used by more than one person; this should be taken into account when determining whether an online advertising message represents a potential "disclosure" of personal information and therefore, a *risk of subjective harm*.

The jury is still out on whether behavioral advertising practices are harmful to individuals. Some take the position that there is not much harm in these practices. Solove, for instance, raises the fact that direct marketers wish to observe behavior so they can tailor goods and advertisements to individual differences and that therefore, the ultimate goal of online marketers aims not at suppressing individuality but at studying it and exploiting it.[1679] Since online marketers generally are interested in aggregate data, some authors maintain that they do not care about the particulars of someone's private life. Furthermore, much personal information is amassed and processed by computers and therefore, online users are not being observed by other

---

[1678] As a matter of fact, since fax is not a very confidential method for transmitting personal information, the OPCC has issued various findings having to do with additional security measures to adopt when faxing personal information. See OPCC, *PIPEDA Case Summary #2003-251, A question of responsibility* (12 December 2003); OPCC, *PIPEDA Case Summary #2003-237, Individual accuses employer of disclosing personal information to co-workers* (20 November 2003); OPCC, *PIPEDA Case Summary #2003-226, Company's collection of medical information unnecessary; safeguards are inappropriate* (31 October 2003); OPCC, *PIPEDA Case Summary #2007-374, Bank faxes credit card account statement to fraudster* (23 March 2007); OPCC, *PIPEDA Case Summary #2006-332, Bank issues new guidelines and educates employees after customer information is faxed to the wrong individual* (12 April 2006); and OPCC, *PIPEDA Case Summary #2005-317, Fax from debt collector contained debtor's personal information* (24 October 2005). In Quebec, the CAI has published, on its website, in the section entitled: "Bulletins on Protecting Personal Information," a guide entitled "Using a fax machine" which also warns against sending personal information throiugh a fax machine. See CAI's guide entitled "Using a fax machine" online: <http://www.cai.gouv.qc.ca/index-en.html>.

[1679] Solove, "Privacy", *supra* note 1 at 1416-17.

humans, but by machines (which would make the online marketing practices less invasive and therefore, less harmful).[1680] Others, such as the PIAC, take the position that there may still be *harm* resulting from these practices.[1681]

Using the approach proposed, whether the information disclosed in the context of personalized online advertising is of an "intimate" nature, whether or not this information is already "available" and whether the information disclosed is "identifiable", are all criteria which should be taken into account when determining whether the online marketing activity is creating a *risk of harm*.

There is potentially a distinction to be made between the *risk of harm* triggered by an online advertisement sent to an individual who is registered on a given website as opposed to someone who is not. In the case of the former, there is less chance that the online marketer could be making a "disclosure" to someone other than that specific individual.[1682] There is more risk upon providing online advertising on random websites, based on a behavioral profile (which includes "intimate" data) linked to an IP address or a cookie which is linked to a computer or device connected on the Internet, since such a device may be used by more than one individual. The issue is not as relevant in an Internet café, since there is such a high volume of users and "intimate" information used to market back will not be identifiable to a specific past user.[1683] On the other hand, if the device is used by a handful of individuals, for example co-workers or family

---

[1680] *Ibid*. at 1418: "Being observed by an insect on the wall is not invasive for privacy; rather, privacy is threatened by being subject to *human* observation, which involves judgments that can affect one's life and reputation. Since marketers generally are interested in aggregate data, they do not care about snooping into particular people's private lives. Much personal information is amassed and processed by computers; we are being watched not by other humans, but by machines, which gather information, compute profiles, and generate lists for mailing, emailing, or calling. This impersonality makes the surveillance less invasive." Ryan Calo also raises that perhaps the harm resulting from the "disclosure" is less important if the data is only viewed by a machine instead of an individual or a human making a judgment. See Calo, "The Boundaries", *supra* note 443 at 25.

[1681] PIAC, *supra* note 448 at 6: "(…) delivery of better targeted advertisements. In other words, if consent does not work, little harm can result. However, we beg to differ, as our discussion of our survey results shows that Canadians are uncomfortable with the concept of such individualized targeting occurring at all and as our detailing of the potential risks of profiling and social sorting, discussed below, also make clear."

[1682] If this individual is registered on a website using his or her personal password, then chances are that this individual is the one behind the device once logged-in.

[1683] See section 2.1.2.2.2(b) entitled "Device Used by a Group: At What Point is it Identifiable?" and section 3.1.2.2.1(b)(ii) entitled "Group vs. Individual and Accuracy of Identification" which discusses the notion of "identifiability" of an individual if the data relates to a group.

members, there may be a potential disclosure made which could create a *risk of subjective harm*.

Marketing to individuals using information of an "intimate" nature has been creating concerns for quite some time. In 1978, the Lindop Report took issue with the fact that data of an "intimate" nature (such as "lists of pregnant women or those in affluent financial circumstances") could be transferred amongst organizations for marketing purposes.[1684] First, there is a type of harm (which is further discussed in section 3.1.2.1.2) that may be triggered when an individual is the subject of targeted marketing, thereby introducing the possibility that the advertiser is aware of certain "intimate" details of this person's private life. According to the Article 29 Working Party, in cases where marketers produce advertising that reveals sexual preferences or political activity, then offering/using interest categories that would reveal sensitive data[1685] (referring to information of "intimate" nature) should be discouraged and an opt-in type consent be obtained.[1686] The reasoning of the Article 29 Working Party implies that under the previous scenario (individuals receiving marketing revealing information of an "intimate" nature), the risk of *subjective harm* would be greater than if the behavioural advertising used non "intimate" information.[1687] An issue though is that by categorizing, one may be categorizing certain data or profile under categories which could be of "intimate" nature (ex: porn lovers) and this increases the potential for a disclosure which may be harmful.[1688]

[1684] Lindop, *supra* note 96 at 143, para. 17.20.

[1685] As defined in EC, *Directive 95/46/EC*, *supra* note 99 at art. 8.

[1686] Article 29 Data Protection Working Party, *Opinion 2/*2010, *supra* note 191 at 20-21.

[1687] See FTC, Preliminary Staff Report, *supra* note 372: "For example, one panelist noted that a consumer simply may not want information about his medical condition to be available to third-party marketers (*See 1st Roundtable, Remarks of Marc Rotenberg, Electronic Privacy Information Center*, at 301.) Another noted that the disclosure of a consumer's health or other sensitive information could lead to embarrassment, stigmatization, or simply needing to explain oneself (*See, e.g.*, *1st Roundtable, Remarks of Leslie Harris, Center for Democracy & Technology*, at 36-38.)."

[1688] Karas, *supra* note 362 at 23: "In September of 1995, Marketry, Inc., a list broker, started marketing a list of over 250,000 email addresses compiled from Internet newsgroup and web sites. The list was segmented into eleven interest categories, including pornography, computer, sports, education, news and religion. After this news was posted to a number of bulletin boards on the Internet and subsequent considerable adverse public reaction, the list was withdrawn."

Second, there is a potential "disclosure" of "intimate" information (and concurrently, a risk of subjective harm) if the marketing is delivered to a device (through a device's IP address or cookie) that is used by more than one individual. For example, if users of the same device often receive online advertising pertaining to medicine for a stigmatizing disease, they may begin to suspect that "one of them" is afflicted with the disease, therefore creating the risk of subjective harm detailed in section 3.1.2.1.2(a) for the individual in fact affected by that disease. At the same time, if the information shared amongst behavioural marketers was not of an "intimate" nature, but more trivial, such as serving ads for some type of trendy sports jackets,[1689] I maintain that the disclosure, in such case, would not create the *risk of harm* discussed in sections 3.1.2.1.1 and 3.1.2.1.2 and therefore, this data should not be governed by DPLs under the proposed approach.

Because, as detailed above, behavioural marketing can trigger the kind of subjective harm discussed in sections 3.1.2.1.1 or 3.1.2.1.2, behavioural marketers should not include information of an "intimate" nature in their profiles, unless they can prove that this information was already "available". For example, if an individual made general online searches about "relationship therapists", then it may be questionable if the device used should receive online advertising about "the best relationship therapist in your area". On the other hand, if the individual is registered on a website and has searched this specific website about relationship therapy, it would be more acceptable for the website to advertise about relationship therapy, once this individual returns and logs in on the website in question. Given that the individual did disclose an interest to a specific website about information of an "intimate" nature (relationship therapy) and upon this user log in (no possibility of disclosing this information to other users of the same device), it would not create any *risk of harm* discussed in section 3.1.2.1.1 or section 3.1.2.1.2 if the website uses this information to advertise back to this specific user. While this user is "identifiable", and the information is of an "intimate" nature, the

[1689] The "intimate" nature of the data is indeed relevant. Some suggest that customer profiles may not necessarily be sensitive data if they only include information which is not of "intimate" nature. See for example Karas, *supra* note 362 at 4: "Our consumer profiles are replete with purchases that are neither embarrassing nor unseemly. If you purchase a pair of Dockers, and the retailer discloses transaction to a third party, you may be disconcerted but perhaps not truly offended. The third party would know something about you, but that information is so impersonal that your privacy has not been invaded any more than if a passerby happened to see you wearing that pair of Dockers."

information was made "available" by this individual to this website. Basically, there is more than likely no harm from using this information to market back to the user, since once the user is registered (and logged in) on the site, chances of "disclosing" the interest of an "intimate" nature to other users of the same device is no longer a threat.[1690]

The fact that the individual is registered on a given website is relevant in the overall test. If the behavioral profile is only linked with a cookie or an IP address that can be traced back to a device used by one or more individuals, there is a potential "disclosure" triggered by the behavioral marketer serving marketing message using the data collected in connection to this device (vs. collected in connection with the relevant individual). It would also be a different scenario, if online websites shared "intimate" information with other websites (though affiliate marketing networks), who then used this information to contact or to market back to the user, therefore potentially triggering a *risk of harm* discussed in section 3.1.2.1.

3.1.2.3.2. Examples of Levels of Subjective Harm

I will discuss various examples which illustrate cases in which the risk of harm resulting from a disclosure of personal information would qualify as "high risk", "medium risk" and "low risk".

(a) High Risk of Harm: Launch of Buzz and AOL breach

The disclosure of personal information would create the highest risk of harm if the data is of an "intimate" nature, is not "available" (or has, to a certain extent, been kept confidential) and is otherwise highly "identifiable" to a unique individual.

To illustrate this thought, let's recall the privacy concerns that took place when Google released its "Buzz" service, a social-messaging system built into the Gmail service. A major concern was that the earliest versions of the service revealed a list of the

[1690] The situation would be different if the individual was not logged on the website since in that case, there would be a potential disclosure of information by this website marketing back to the device (using its cookie for example), since the marketer would not know if the individual behind the screen is the same individual that made the online search on his website (in the example discussed, looking for information about couple's therapy).

individuals the Gmail user e-mailed most frequently;[1691] which was found to be a privacy breach. This type of information could lead to various unpleasant scenarios: for instance a wife discovering that her husband emails and chats with an old flame or a boss discovering that his employee exchanges emails with executives at a competitor.[1692] Under the approach proposed, before launching a service such as Buzz, the organization would have had to first acknowledge the potential disclosure of the names or email addresses of the individuals with which a Gmail user communicates most frequently. The test proposed in this section would then have to be considered. The organization would have to determine if the information (the names or email addresses of the individuals with which a Gmail user communicates with the most frequently) is of an "intimate" nature, if this information already "available" publicly (the disclosure of this information was going to become public with the launch of the service), and if this information is "identifiable" to this Gmail user.

Since the relevant information in the Buzz scenario was most likely of an "intimate" nature[1693] and it was clearly linked with Gmail users (and therefore "identifiable"), unless Google could demonstrate and prove that this information (the fact that Gmail user X communicated with individual Y most frequently) was already public (the "availability" test), then it should not have disclosed this information upon the launching of the Buzz service. To make this disclosure by Google even worse under this Buzz scenario, the "disclosure" of personal information actually impacted not only the Gmail users, but also the individuals with which this Gmail user communicated with the most frequently.

Another example to illustrate the outcome of the approach is with the privacy breach which took place on August 4, 2006, when AOL Research published (publicly disclosed for research purposes) a compressed text file on one of its websites containing twenty million search keywords which had been punched into AOL's search engine for over

---

[1691] Robert McMillan, "Google Buzz Criticized for Disclosing Gmail Contacts" *IDG News* (10 February 2010), online: PC World <http://www.pcworld.com/article/189081/google_buzz_criticized_for_disclosing_gmail_contacts.html>.

[1692] Carlson, *supra* note 480.

[1693] See section 3.1.2.2.2(c)(viii) which elaborates on this issue and on the fact that personal communications are usually considered as "intimate" information.

650,000 anonymous AOL users over a 3-month period further discussed in sections 1.2.1.3 as well as discussed in section 2.1.2.1.2(b). Using the approach proposed, before disclosing this information, AOL Research would have had to analyze the information using the proposed test. So while not every single profile was "identifying", given the volume of the information made available (millions of search keywords punched for over 650,000 AOL users over a 3-month period), the "potential" to identify some of the users was present. Although it wasn't clear if the information was "identifiable", the fact that the information was clearly of an "intimate" nature,[1694] coupled with the fact that there was no evidence that this data was already "available" to the public, the notion of "identifiable" was to be interpreted more softly.[1695] This risk, evaluated using the proposed test, would have refrained AOL from disclosing this research data to the public.

This AOL example illustrates how the disclosure of information of an "intimate" nature, not widely "available", but which is not necessarily "identifiable" can still create a high risk of harm, or at least a medium risk of harm. The reason being that the notion of "identifiability" is never foolproof.[1696] When you have a certain volume of information, all it takes is for the information released (disclosed) to come in contact with one single piece of information to make this bundle of information "identifiable". To illustrate this thought, van den Hoven provides the following example that was initially used by Gavison:

> "Consider the famous anecdote about the priest who was asked, at a party, whether he had heard any exceptional stories during confessionals. 'In fact', the priest replied, 'my first confessor is a good example, since he confessed to murder'. A few minutes later, an elegant man joined the group, saw the priest, and greeted him warmly. When he

[1694] Paul Ohm suggests that search engine data are even more sensitive than health data. See Ohm, *supra* note 562 at 1775-76: "We reveal even more than health information to search engines, supplying them with our sensitive thoughts, ideas, and behavior, mixed in of course with torrents of the mundane and unthreatening." See also Cohen, "Examined Lives", *supra* note 459 at 1426.

[1695] See section 3.1.2.2.1 which elaborates on this issue.

[1696] See section 1.2.1.3 entitled "Easier Identification of Individuals" and section 1.2.3 entitled "New Identifying Methods" which discuss this issue.

> asked how he knew the priest, the man replied: "Why, I had the honour of being his first confessor'."[1697]

While the priest initially did not disclose *personal information* according to the standard legal definition found in most DPLs (since the information was not "identifiable" to an individual), the information disclosed coming in contact with another piece of information completely changed the picture. Using the approach proposed, the outcome may have been different. For instance, the fact that the data was of a very "intimate" nature and not widely "available", should have been enough for the priest to limit the disclosing of this confession in order to limit the risk of subjective harm triggered by disclosure, which was medium to high in this specific situation.

Information which is of a very "intimate" nature, and not "available", may still be potentially harmful upon being disclosed even if it is absolutely not "identifiable". For example, in *Northwestern Memorial Hospital* v. *Ashcroft*,[1698] Posner comments on the fact that a privacy breach may still occur even if a person cannot be identified by name on the Internet: "Imagine if nude pictures of a woman, uploaded to the Internet without her consent though without identifying her by name, were downloaded in a foreign country by people who will never meet her. She would still feel that her privacy had been invaded".[1699] Usually though, the *risk of harm* in such cases will be lesser than if the information was "identifiable" (in this case, if the woman was identified on the picture).

I discuss, in section 2.1.2.1.1(c), the case of DoubleClick which was looking to merge with Abacus Direct Corp., a direct-marketing company that maintained an extensive database of names, addresses, telephone numbers, retail purchasing habits and other personal information on approximately ninety percent of American households. It was these companies' intention to merge their two databases, to create extremely detailed consumer profiles on Internet users' consumer behaviour, online and offline.[1700] It was

---

[1697] Van den Hoven, "Information Technology", *supra* note 642 at 309.

[1698] *Ashcroft*, *supra* note 1416.

[1699] *Ibid*. at 929.

[1700] When DoubleClick and Abacus announced a merger one of the executives proudly states, "The goal is to have the most complete picture of the consumer you can." Quoted in Beth Givens, "Privacy Expectations in a High Tech World" (2000) 16 Computer & High Tech. L. J. 347 at 352. Consolidation of

initially surprising that such a merger was even possible (the database from Abacus being biographic information) given that Double Click was claiming to collect "anonymous" profile information.[1701] Authors suggest that DoubleClick was pretending not to collect information pertaining to "identifiable individuals" but was still collecting some type of "point of collection" (i.e. cookies) that enabled them to make a link between the data collected and specific individuals.[1702] This simply illustrates how the information collected by DoubleClick should have been considered as *personal information* from the start, especially if the profiles included information of an "intimate" nature that was not otherwise "available". Also, using the approach proposed, the merging of the two databases was redefining the situation since the erstwhile anonymous profiles were being merged with a database containing biographic information. If there was any doubt whether the DoubleClick profiles were *personal information*, there was no doubt that this information, once merged with the Abacus database, constituted *personal information*. Using the approach proposed, since the merging of the two databases would result in more comprehensive profiles involving data which is of an "intimate" nature, not necessarily already "available" and now (post-merger) definitely "identifiable", this kind of disclosure would definitely create a risk of subjective harm which would trigger the application of the relevant DPL.[1703]

(b) Medium Risk of Harm: Court Records Made Available Online

As I have already mentioned in section 3.1.2.2.3, the act of increasing the availability of data is an important factor in assessing privacy harm. For instance, intimate and identifiable information that is already in wide circulation presents only a medium risk of harm.

---

information databases may also happen through sales of consumer lists of defunct dot coms, a phenomenon more common in the current economic climate. See Richard A. Beckmann, "Comment: Privacy Policies and Empty Promises: Closing the 'Toysmart Loophole'" (2001) 62 U. Pitt. L. Rev. 765.

[1701] Conseil de l'Europe, *L'autodétermination informationnelle*, *supra* note 20 at 31.

[1702] *Ibid*.

[1703] This means, for instance, that the consent of the individuals would be necessary for this merger to take place, subject to the provisions of the applicable DPL and any "business transaction" exception, as the case may be.

Search engines make information available more easily "available". By "Googling" an individual's name, much can often be gleaned about this person.[1704] www.123people.fr groups and aggregates all kinds of information (such as pictures, email addresses, links, etc.) pertaining to the name of an individual searched and displays the data available online in a comprehensive manner. While in an ideal world, search engines would not be making information of a highly "intimate" nature more easily available, it is difficult to argue that there is a risk of subjective harm given the fact that information disclosed is already "available" through the same medium (i.e. the Internet).

The issue is a different one when disclosing public records online (including courts records), which were only previously accessible offline. While some may argue that if information is already made public offline, then it should be available online as well; others may raise privacy concerns due to the fact that the data will become increasingly available once online. Many administrative bodies charged with examining the issue of making public records available online have hesitated because of the increased accessibility associated with the Internet.[1705] Nissenbaum also mentions that the question of whether public records ought to be available online provokes similar questions about court records in general, and more particularly, whether some of the information contained in them and other public records should be reclassified as personal or confidential and deserving of greater protection.[1706]

First, these records may often contain information of a highly "intimate" nature.[1707] For example, an interested party accessing these records could ascertain a litigant's credit history, occupation, debt burden, and income. Second, the "availability" factor is also relevant. For instance, the U.S. federal courts, along with many state courts and

---

[1704] See section 1.2.5.3 entitled "Spatial Shift" which elaborates on search engines.

[1705] Nissenbaum, *supra* note 230 at 120-21. See also Solove, "A taxonomy", *supra* note 339 at 536.

[1706] Nissenbaum, *supra* note 230 at 131-32.

[1707] See section 3.1.2.2.2(c) entitled "Information Inherently Intimate" which elaborates on information which is of intimate nature. See also Natalie M. Gomez-Velez which suggests that providing Internet access to court records increases the availability of court records exponentially, including any sensitive information they contain. Gomez-Velez, *supra* note 341, discussed in Trudel, "Privacy Protection", *supra* note 164 at 327-28: "Providing Internet access to court records increases exponentially the availability of court records, including any sensitive information they contain. Examples of sensitive information that might be found in court records include: social security numbers, home addresses, names of minor children, financial account numbers and medical information."

agencies, are developing systems to place their records online and Solove argues that while these records are readily available at local courthouses or government offices, placing them online has given rise to an extensive debate over privacy.[1708] This constitutes a more impactful "increased availability" between where the information was in fact available (with a certain amount of work required to actually access it) vs. the information made available to everyone in the world, with almost no amount of work required.

The risk of harm relating to the disclosure of information becomes lower (perhaps medium to low) if it has to do with information of an "intimate" nature, which is not "identifiable" and already "available"; information which is not of an "intimate" nature, not "available" but "identifiable"; or information which is not of "intimate" nature, not "available" and also "not identifiable".

Location data is an example of the type of information which may or may not be "identifiable" (it may be or may not be accurate, although I already discuss in section 1.2.1.3 how, if the location data collected is very accurate and collected over a long period of time, it may well be "identifiable").[1709] This kind of information may also potentially be of "intimate" nature. For instance, it can reveal where one lives and spends his time, therefore providing information about his or her personal interests, affiliations. For example, if one was at a given meeting place at the time at which there is a political even taking place, others accessing the location data of this individual could assume that this individual is probably a member or affiliated to that political party.[1710] Location data is sensitive and in many cases, it is information is of "intimate" nature. On the "availability" issue, some are saying that since this data is already available, that it should not be protected or at least treated differently than if it was "intimate" information such as medical information.[1711] But when evaluating the risk of harm which may be triggered upon this kind of information being disclosed, the fact

---

[1708] Solove, "A taxonomy", *supra* note 339 at 536.

[1709] Gratton, "Personalization", *supra* note 16.

[1710] Gratton, *Internet and Wireless Privacy*, *supra* note 193 at 32-36.

[1711] Kirkpatrick, "Location Data", *supra* note 800: "treating location data like medical data sounds like a recipe for shrouding it in complete privacy by default. Not allowing information about our activities in public (...) to be public (...) would be a real blow to the location service ecosystem."

that it is accurate or collected over a long period of time (volume of information collected) would increased the potential to "identify" the individual behind the location profile.[1712] This information could end up revealing information of very "intimate" information, such as the fact that an individual to which the location information belongs went to a HIV clinic twice a week for the last few months. In such case, the risk would be greater than revealing limited information, on a much shorter period of time.[1713] This is why, the accuracy of the data, its volume and the period of time for which it is collected will all be useful elements to take into account when assessing this risk of harm since it will impact on the "identifiability" of the data (which could range from the high risk to the low risk depending on the scenario).[1714]

Another example to illustrate the risk of harm through the disclosure of information that is not always of an "intimate" nature (not "available" but "identifiable") could be the sale of a list of magazine subscribers to a third party. In the U.S., in the *Shibley* case,[1715] a magazine subscriber sued Tim Inc., a publisher, for doing just that, claiming that this practice constituted an invasion of privacy because it amounted to a sale of individual "personality profiles" since "the buyers of these lists are able to draw certain conclusions about the financial position, social habits, and general personality of the persons on the lists by virtue of the fact that they subscribe to certain publications."[1716] The Ohio court held that the disclosure of magazine subscription information did not imply a violation of privacy and it is fairly clear that their decision was based, in part, on the fact the information transferred was in their view not of an "intimate" nature.[1717]

I maintain that the *risk of harm*, in such cases, should always be a function of the "intimate" nature of the special interest of the magazine. In the event that the magazine

---

[1712] See section 1.2.1.3 entitled "Easier Identification of Individuals" which elaborates on how the greater volume of data available may allow the identification of individuals more easily.

[1713] See section 1.2.1.3 entitled "Easier Identification of Individuals", section 1.2.5.2 entitled "Temporal Shift", and section 1.2.5.3 entitled "Spatial Shift" which elaborate on this issue.

[1714] See section 1.2.5 entitled "Increased Availability of Data" which discusses the relevant criteria to determine the risk of harm resulting from an "increased accessibility".

[1715] *Shibley v. Time Inc.*, 45 Ohio App. 2d 69, 341 N.E. 2d 337, 74 Ohio Op. 2d 101, 82 A.L.R. 3d 765 (1975) [*Shibley*].

[1716] *Ibid*. at 339.

[1717] *Ibid*. at 339-40.

relates to health or some other special interest of "intimate" nature (ex: magazine targeting homosexuals) then the risk of harm would be much higher than if it was a "general news" type of magazine. The proposed approach is therefore consistent with PIPEDA on this matter, which suggests that any information can be sensitive, depending on the context. To illustrate this, PIPEDA which states that "the names and addresses of subscribers to a news magazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive."[1718] Thus, the disclosure of intimate information (such as the list of subscribers to a special interest magazine) implies a heightened *risk of harm* and requires a greater degree of protection.

(c) Low Risk of Harm: Note2be

The *risk of harm* relating to the disclosure of information becomes even lower if it has to do with information which may be "identifiable", but is not of an "intimate" nature, and is already "available" to a certain extent.

In France, in the Note2Be case law, the French court found that the processing of the name, workplace and rating by students of their teachers were found to be illicit and the website (similar to www.ratemyteacher.com or www.ratemyprofessor.com) was in part shut down.[1719] Using the approach suggested here, one could claim that the disclosure test would have concluded that there was no *risk of harm* in the disclosure at stake. While the data was highly "identifiable" (name of teacher, place of work), it was also already "available" (if not publicly available) and not of "intimate" nature.[1720] Under certain DPLs such as PIPEDA, "business contact information" (name of employee and their address of place of work) is even excluded from the definition of personal information.[1721] Some authors, such as Trudel and Gautrais, have also raised

[1718] PIPEDA, *supra* note 63 at Schedule 1 (s. 5), principle 4.3.4.

[1719] Trib. gr. inst. Paris, 3 March 2008, ord. réf., RG 08/51650. See also CNIL, *supra* note 413.

[1720] Unless we take the position that the notations provided by students were data of "intimate" nature.

[1721] PIPEDA, *supra* note 63 at section 2.

the fact that it was not clear in this Note2be case whether the information at stake should in fact have been qualifying as *personal information* given its low sensitivity.[1722]

Information which is not of "intimate" nature, is already "available" and is not "identifiable" is on the lowest section in the risk of subjective harm upon being disclosed. This kind of information should not regulated by DPLs or at least, the information should be able to circulate without having to obtain the relevant individual's prior consent.

***

There is information that, once disclosed, may be harmful not because of the fact that this data may create some type of embarrassment, but because of the way that it may be "used" by third parties. This may include financial information, which, if released (by banks or e-commerce websites), may be used to create harm such as fraud or identity theft. This could also include location data, which may be used by a stalker to physically harm another individual. In another U.S. example, an Internet site known as the "Nuremberg Files" posted information about doctors working in abortion clinics, including names, photos, Social Security numbers, home addresses, descriptions of their cars, and information about their families.[1723] The doctors sued and at trial, they testified as to how their lives became riddled with fear, how some wore bulletproof vests and wigs in public.[1724] This is a clear illustration how sometimes a disclosure may

[1722] Pierre Trudel and Vincent Gautrais are raising the fact that the French court never discussed whether the data at stake (name of teacher, name of school and notations) actually qualified as *personal information*. Gautrais & Trudel, *supra* note 1 at 119: "En premier lieu, il nous semble pertinent de s'interroger sur le fait de savoir si le nom, le prénom, l'établissement d'enseignement et éventuellement une notation qui pourrait y être associée, constituent des renseignements personnels. De par leur caractère public, de par leur faible sensibilité, la question nous semble devoir être posée. C'est d'ailleurs pour cela que la Loi fédérale sur la protection des renseignements personnels, a pris le soin d'exclure de la définition même de renseignements personnels, à l'article 2, ces données pour le moins banales."

[1723] Doctors who were killed had a black line drawn through their names. Names of wounded doctors were shaded in gray. *Planned Parenthood of the Columbia/Williamette, Inc. v. Am. Coalition of Life, Activists*, 244 F. 3d 1007 (9th Cir. 2001) [*Planned Parenthood*]. This case is discussed in Solove, "Privacy", *supra* note 1 at 1426.

[1724] They won the suit and the site was shut down, but the appellate court reversed on First Amendment grounds. See *Planned Parenthood*, *supra* note 1723 discussed in Solove, "Privacy", *supra* note 1 at 1426.

trigger a more objective kind of harm which mostly relates to the fear of this information being "used".[1725]

As Solove suggests: "Privacy (…) involves more than avoiding disclosure; it also involves the individual's ability to ensure that personal information is used for the purposes she desires."[1726] The risk of harm triggered by the "use" of information will be addressed in the next section.

[1725] See section 3.1.2.1.2(a) entitled "Fear of a Disclosure or that Information Disclosed will be Used" which elaborates on this issue.

[1726] Solove, "Conceptualizing", *supra* note 23 at 1108.

3.2. Objective Harm Associated with the Definition of Personal Information

The last data handling activity regulated by DPLs is the use of personal information.[1727] Reidenberg aptly observes:

> "(…) the creation of special protection is also understood as requiring attention not only to whether information identifies particular aspects of a person's life that are sensitive, but how data will actually be used. (…) The impact of bureaucratic use of personal information, whether merely personal or highly sensitive, depends on the means of processing, the kinds of databases linked together, and the ends to which information will be used."[1728]

Section 3.1 details how the type of harm that may arise from the collection or disclosure of information is usually of a subjective nature. I maintain that at the "use" level, the type of harm is usually of an objective nature.

There is a psychological or subjective component in the harm that may result from an individual having the concern that his or her personal information is being used by various organizations to take significant decisions that will have an impact on his or her life. For instance, Solove believes that the potential for secondary use generates fear and uncertainty over the manner in which information will be used in the future.[1729] According to him, this fear and uncertainty creates a sense of powerlessness and vulnerability; a dignitary harm.[1730] So while there may be a psychological component to the type of harm resulting from the use of data, I maintain that, in general, the type of harm resulting from the use of data is usually of an objective nature.

It is not clear if this objective harm (resulting from the use of personal information) necessarily qualifies as a privacy breach. Certain authors take the position that the

---

[1727] This particular activity (or the term "using") is not defined in the Canadian or French DPLs analyzed. In Europe, the activity of "processing" the information includes the "use" of personal information. As a matter of fact, EC, *Directive 95/46/EC*, *supra* note 99 at art. 2 defines "processing of personal data" as "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."

[1728] Reidenberg & Schwartz, *supra* note 203 at 9.

[1729] Solove, "A taxonomy", *supra* note 339 at 520.

[1730] *Ibid*.

harm resulting from the use of personal information can be associated with a "privacy harm". For example, Trudel and Benyekhlef have associated secondary uses of personal information with some type of intrusion, which would constitute a breach of privacy.[1731] Solove suggests that courts must abandon the notion that privacy is limited to concealing or withholding information, and must begin to recognize that uses of information (and not merely disclosures of secrets) can also threaten privacy.[1732] He states:

> "Privacy involves the ability to avoid the powerlessness of having others control information that can affect whether an individual gets a job, becomes licensed to practice in a profession, or obtains a critical loan. It involves the ability to avoid the collection and circulation of such powerful information in one's life without having any say in the process, without knowing who has what information, what purposes or motives those entities have, or what will be done with that information in the future. Privacy involves the power to refuse to be treated with bureaucratic indifference when one complains about errors or when one wants certain data expunged. It is not merely the collection of data that is the problem—it is our complete lack of control over the ways it is used or may be used in the future."[1733]

Solove, therefore, includes objective types of harm under the "privacy harm" category, and so does Calo.[1734]

Others take the position that the harm caused by the use of information has nothing to do with privacy. For instance, in his article entitled *Privacy and the Varieties of Moral Wrong-doing in an Information Age*, van den Hoven suggests that there are forms of wrongdoing or harm which have as their necessary condition that the wrong-doer make "use" of certain personal information about the victim. Nevertheless, the fact that it is information about individuals that is used to inflict the harm doesn't necessarily make it a "privacy issue".[1735] Since post modern criminals are known to use computerized

---

[1731] Trudel & Benyekhlef, *supra* note 367 at 10: " (…) celui qui s'aviserait de copier la liste des participants et l'utiliser à des fins différentes des finalités pour lesquelles elle est constituée commettra vraisemblablement une intrusion, portant ainsi atteinte au droit à la vie privée".

[1732] Solove, "Privacy", *supra* note 1 at 1457.

[1733] *Ibid*. at 1426-27.

[1734] Calo discusses both the subjective and objective types of harm under the "privacy harm" category. See generally, Calo, "The Boundaries", *supra* note 443.

[1735] Van den Hoven, "Moral Wrong-doing", *supra* note 272 at 34-35.

databases and the Internet to stage their crimes, van den Hoven argues, we must acknowledge a new vulnerability to what might be called "information based harms": "As you can grab someone's arm and twist it to hurt him, you can get someone's personal information and use it to his harm."[1736] Van den Hoven posits that it is strange that the defenders of privacy often point to the Second World War as a paradigmatic case of privacy violation:

> "They relate the sad history of the occupation by the Nazi's, who found an easily accessible and well organized citizen administration, from which they could hand-pick jews, gypsys, criminals, mentally handicapped, homosexuals, trace them and send them off to the extermination camps. This part of our national past has for a long time effectively prevented the introduction of identification cards, registration of religion and sexual preference. But it seems somewhat odd to say that the Nazi's invaded the privacy of the Dutch Jews. They murdered, tortured innocent human beings." [1737]

In section 2.2.2.1, a distinction was made between "privacy" and "data protection". I am not convinced that objective types of harm triggered by the use of personal information should be included under the more general "privacy harm" category. Whether or not the use of information leads to a veritable privacy harm, this kind of harm is clearly more objective in nature. Calo explains that while at the collection or disclosure levels, the corresponding harm may be subjective in nature,[1738] the consequence of a third party using data would be much more concrete and in many cases, would have financial implications. For example, when TJX was hit with a security breach, its customers were worried about a potentially costly identity theft.[1739] According to Calo, the objective category of privacy harm would be the unanticipated or forced use of personal information against a given person:

[1736] *Ibid*.

[1737] *Ibid*.

[1738] Calo, "The Boundaries", *supra* note 443 at 20: "Subjective privacy harms are injuries individuals experience from being observed. But why does the belief that one is being observed cause discomfort or apprehension? In some instances, the response seems to be reflexive or physical. The presence of another person, real or imagined, creates a state of 'psychological arousal' that can be harmful if excessive and unwanted."

[1739] See *TJX Companies Retail Sec. Breach Litigation*, 564 F. 3d 489 at 491 (1st Cir. 2009). In January 2007, TJX Companies, Inc. ('TJX'), a major operator of discount stores, revealed that its computer systems had been hacked and that credit or debit card data for millions of its customers had been stolen. This case is discussed in Calo, "The Boundaries", *supra* note 443 at 20.

> "The second category is "objective" in the sense of being external to the person harmed. This set of harms involves the forced or unanticipated use of information about a person against that person. Objective privacy harms can occur when personal information is used to justify an adverse action against a person, as when the government leverages data mining of sensitive personal information to block a citizen from air travel, or a neighbor forms a negative judgment from gossip. They can also occur when such information is used to commit a crime, such as identity theft or murder." [1740]

While individuals may suffer some type of subjective harm when their information is collected or disclosed,[1741] it is often the use of information that leads to a more tangible kind of harm. For example, if the criminal record of a bank employee is disclosed to his co-workers, this employee may feel embarrassed and humiliated and may even fear that this information may eventually be used against him (subjective harm resulting from the disclosure).[1742] Once the information is then used by the bank to dismiss the employee, the resulting harm will be objective in nature (in this case, a financial or economical harm). Whenever personal information is used by an organization to take a decision or make an assessment about an individual or influence the way in which that individual is treated or evaluated, this will usually trigger a potential objective harm.

Section 2.1.2 explains how the definition of *personal information* may be over-inclusive, under-inclusive, be the source of uncertainties or even be obsolete in certain situations. Section 2.1.1.2 elaborates on the "notice and choice" model, which may prove defective since privacy policies are often quite vague on the use which will eventually be made of the information.[1743] A way to ensure that information which was meant to

---

[1740] Calo, "The Boundaries", *supra* note 443 at 14 [footnotes omitted]

[1741] See section 3.1.1.1 entitled "Harm Resulting from the Collection (1960s – 1970s Concerns)" and section 3.1.2.1 entitled "Harm resulting from the Disclosure (1960s-1970s Concerns" which elaborate on those harms.

[1742] See section 3.1.2.1.1 entitled "Harm Directly Linked to Disclosure: Subjective (and Psychological)" which elaborates on this issue and more specifically, section 3.1.2.1.2(a) entitled "Fear of a Disclosure or that Information Disclosed will be Used" which elaborates on this issue.

[1743] For example, online service providers may claim to use the data collected for broad purposes such as improving their products and services or enhancing the customer's experience. The implication is that potential future uses of the information are too vast to enable individuals to make an adequate valuation. See section 2.1.1.2.1(a) entitled "Policies are Overly Vague" which elaborates on this issue.

be covered by DPLs is in fact protected, is to first determine the situations in which the use of information will create a *risk of harm*.[1744]

First, I will discuss in section 3.2.1 the kind of objective harms meant to be addressed by DPLs, in the context of regulating the use of information. Second (in section 3.2.2), I will elaborate on the proposed test to determine whether a given set of information "used" by an organization should be governed by DPLs. Instead of determining whether the data is "identifiable" to an individual, the first step in this test is to ascertain whether the use of the data may have a "negative impact" on the relevant individual (i.e. objective harm). If the use creates said negative impact, then the data should be governed by the relevant DPL (in which case the data "accuracy" and "relevancy" criteria would be relevant).[1745] Third, I will apply the proposed interpretation to practical business cases to illustrate with examples how the approach would actually work in practice (section 3.2.3).

3.2.1. Objective Harm Resulting from the Use of Information (1960s-1970s Concerns)

In this section, I will first elaborate on how the objective harm is somehow well illustrated with the Kafka Metaphor. I will then detail various types of objective harms which pertain to the use of individual.

3.2.1.1. Objective Harm and the Kafka Metaphor

Evidence from old documents dating back to the late 1960s and early 1970s, when the FIPs were in their infancy, illustrate the main concern pertaining to regulating the use of personal information: protecting individuals against objective harm.

Documents from the early 1970s produced in the context of the adoption of DPLs already raised the concern of having organizations use the information of individuals in a way which would be detrimental to them. In 1973, the *Report of the Secretary's Advisory Committee on Automated Personal Data Systems* (U.S.) mentioned that

---

[1744] Adressing this risk of harm being the ultimate purpose of DPLs. See section 2.2.2 entitled "Determining Risk of Harm as Purpose Behind the Protection of Personal Information" which elaborates on this issue (purpose behind DPLs).

[1745] See section 3.2.2.2 and section 3.2.2.3 which elaborate on this issue.

privacy was directly affected by the kind of "uses" made of personal information.[1746] In the late 1970s, in the U.K., while discussing the adoption of a DPL or some type of regulation incorporating the FIPs, the Lindop Committee was already suggesting that individuals should be able to know if their data was to be used as the basis of "an adverse decision against them",[1747] and that "outdated data" should be discarded especially when "used for making decisions which affect the data subject".[1748]

In recent years, certain Canadian DPLs have introduced notification obligations in the event of data security breaches if such breach is triggering a risk of significant harm. A definition of "significant harm" is included and in fact refers in part to the objective harm that may occur if the information is then "used" by third parties. More specifically, Bill C-12 refers to "bodily harm, (…) loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property."[1749] In Alberta, Information Sheet 11: *Notification of a Security Breach*, also provides for the same kind of definition of "significant harm" in cases in which the information disclosed is then used: "A significant harm is a material harm; it has non-trivial consequences or effects. Examples may include possible financial loss, identity theft, physical harm (…) or damage to one's professional or personal reputation."[1750]

I already discuss earlier how it is not always clear whether certain new types of data are covered under the definition of *personal information*.[1751] On the issue of data

---

[1746] U.S. Department of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *supra* note 57 at s. III.

[1747] Lindop, *supra* note 96 at 49, para. 5.50: "A point often made was that the data subject should be able to see such data as soon as they were (…) used as the basis for an adverse decision against him."

[1748] *Ibid*. at 51, para. 5.61: "The objective of discarding outdated data clearly applies principally to data used for making decisions which affect the data subject, and several witnesses told us that users should not be prevented from retaining personal records for statistical, research and archival purposes."

[1749] The key factors for identifying whether there is a real risk of significant harm are also spelled out in the Act; they are the "sensitivity of the personal information" involved (referring to a more subjective kind of harm) and "the probability that the personal information has been, is being or will be misused", which refers to a more objective kind of harm. See *Safeguarding Canadians' Personal Information Act*s, *supra* note 506 aimed to amend PIPEDA, re-introduced by the Government of Canada on September 29, 2011.

[1750] Service Alberta, *supra* note 1367 at 2-3.

[1751] See section 2.1.2.2 and more specifically, section 2.1.2.2.2 entitled "Identifying a Device or an Object" which elaborate on this issue.

protection raised by RFID tags, the Article 29 Working Party noted that: "data relates to an individual if (…) such information is used to determine or influence the way in which that person is treated or evaluated."[1752] This statement is in line with the approach that I propose. At the use level, I maintain that the test to determine if certain data should qualify as *personal* should hinge on whether the information is used to determine or influence the way in which that person is treated or evaluated, as further discussed in section 3.2.2.1.1.

Solove argues that the use of personal information in databases presents a different set of problems than does government surveillance[1753] and, therefore, the Big Brother metaphor fails to capture the most important dimension of the database problem:

> "We live today in a world largely controlled by public and private bureaucracies, affecting our communication, entertainment, health care, employment, education, transportation, and culture. These institutions structure our lives in the modern state, and our freedom is implicated in our relationships to them. Databases alter the way the bureaucratic process makes decisions and judgments affecting our lives; and they exacerbate and transform existing imbalances in power within our relationships with bureaucratic institutions. This is the central dimension of the database privacy problem, and it is best understood with the Kafka metaphor."[1754]

He uses the metaphor of Franz Kafka's *The Trial*, to illustrate the problem (or the harm) resulting from databases and the activity of "using" personal information.[1755] In *The Trial*, an unscrupulous bureaucracy uses personal information to take important decisions, while denying the relevant people the ability to participate in how their information is being used. Solove states that this problem is derived from information processing (which he defines as the storage, use and analysis of data) rather than

---

[1752] Article 29 Data Protection Working Party, *RFID technology*, *supra* note 196 at 8.

[1753] Daniel J. Solove, *The Digital Person: Technology and Privacy in the Information Age* (New York: NYU Press, 2004) at 6-9 [Solove, *The Digital Person*]. See also Daniel J. Solove, "I've Got Nothing to Hide' and Other Misunderstandings of Privacy" (2007) 44 San Diego Law Review 745 at 756.

[1754] Solove, "Privacy", *supra* note 1 at 1399.

[1755] *Ibid*. at 1429: "In sum, the privacy problem created by the use of databases stems from an often careless and unconcerned bureaucratic process—one that has little judgment or accountability—and is driven by ends other than the protection of people's dignity. We are not heading toward a world of Big Brother or one composed of Little Brothers, but toward a more mindless process—of bureaucratic indifference, arbitrary errors, and dehumanization—a world that is beginning to resemble Kafka's vision in *The Trial*."

simply information collection.[1756] According to him, this sort of information processing (or use of information) would affect power relationships between people and the institutions of the modern state. The individual would be frustrated by a "sense of helplessness" and "powerlessness". Social structure would also be affected by altering the kinds of relationships people have with the institutions that make important decisions about their lives.[1757]

3.2.1.2. Types of Objective Harm

A broad range of harms can be inflicted on data subjects emerging out of the use of their personal information. Van den Hoven and Vermaas believe that: "the first type of moral reason for data protection is concerned with the prevention of harm, more specifically harm that is done to persons by making use of personal information about them."[1758] The purpose behind regulating the "use" of data which is found in DPLs was in fact to limit the type of information-based harms which could emerge.

I maintain that instead of restriction all circulation of information, we should focus on regulating information which may be used in a harmful way towards individuals. I will examine below the objective harms that the "use" of personal information by organizations may trigger:

3.2.1.2.1. Financial Harm (Information-based)

A first type of objective harm is a financial or economic one. Van den Hoeven believes that the first type of moral reason for thinking about constraining the flow of personal information is concerned with the prevention of information-based harm, which includes financial harm such as theft or identity fraud.[1759] When discussing the type of harm that

---

[1756] See Solove, "A taxonomy", *supra* note 339 at 490-91.

[1757] Solove, "Privacy", *supra* note 1 at 1456.

[1758] Van Den Hoven & Vermaas, *supra* note 1036 at 285-86.

[1759] Van den Hoven, "Information Technology", *supra* note 642 at 311: "In an information society, there is a new vulnerability to harm done on the basis of personal data – theft, identity fraud, or straightforward harm on the basis of identifying information. Constraining the freedom to access information of persons who could cause, threaten to cause, or are likely to cause information-based harm can be justified on the basis of Mill's Harm Principle. Protecting identifying information, instead of leaving it in the open, diminishes epistemic freedom of all to know, but also diminishes the likelihood that some will come to harm, analogous to the way in which restricting access to firearms diminishes both freedom and the likelihood that people will get shot in the street. In information societies, identity-relevant information resembles guns

may result from the use of personal information, RAND Corporation (U.K., 2009) refers to an economic harm such as "financial damages suffered as a consequence of identity theft, loss of earnings."[1760] The Canadian breach notification guidelines and provisions discuss the fact that individuals should be notified in case of a security breach triggering a loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.[1761] The Alberta "Notification of a Security Breach" guide also suggests that: "a lost Social Insurance Number might lead to significant harm, since a SIN can be used to commit fraud."[1762]

Nissenbaum further summarizes the objective type of financial harm which may result from the use of personal information as follows:

> "Less palpable, but also serious, are harms like identity theft, which occurs with increasing frequency, apparently as a result of the ready availability of key identifying information like Social Security numbers, addresses, and phone numbers. Furthermore, various goods such as employment, life, and medical insurance, could be placed at risk if the flow of medical information were not restricted (…)."[1763]

One problem is identity theft and identity fraud, which brings a high risk of financial damage to potential victims.[1764] Criminals are known to have used databases and the Internet to obtain information on their victims in order to stage their crimes. Identity theft would be one of the fastest growing white collar crimes.[1765] Solove suggests that identity theft is enabled by the existence of "digital dossiers", extensive repositories of

---

and ammunition. Preventing information-based harm clearly provides us with a strong moral reason to limit the access to personal data."

[1760] Robinson et al., *supra* note 151 at 48.

[1761] See *Safeguarding Canadians' Personal Information Act*s, *supra* note 506, introduced in 2012, if enacted, would require organizations governed by Canada's private sector privacy legislation to notify the federal Privacy Commissioner of any material privacy breaches involving personal information. See also Service Alberta, *supra* note 1367 at 2-3.

[1762] *Ibid*.

[1763] Nissenbaum, *supra* note 230 at 147.

[1764] Van den Hoven, "Information Technology", *supra* note 642 at 311.

[1765] Jennifer Lee, "Fighting Back When Someone Steals Your Name", *The New York Times* (8 April 2001) at 8, § 3, discussed in Solove, "A taxonomy", *supra* note 339 at 515.

their personal information which are maintained by various organizations.[1766] Some report that the careless use of data by private-sector and public-sector organizations makes the crime of identity theft incredibly easy. For instance, organizations may use social security numbers as passwords. These can be readily obtained by identity thieves from public records, organizations' databases or personal accounts which are not properly secured.[1767]

Another issue comes from the fact that with web 2.0, individuals may be disclosing a lot of personal information on blogs or OSNs, which may be used by third parties and may lead to identity theft. Information found online may include someone's hometown, his or her birthday, high school, e-mail address and workplace. Information such as pet names or mother's maiden name, which may be the answer to a security question, may also be available online and easily accessible.[1768] Some are claiming that RFID systems used to complete transactions would be vulnerable to fraud and even identity theft, since unauthorized readers could scan tags, deduct money or even carry out other transactions to the detriment of the consumer.[1769]

The most important problem with "identity theft" may be the risk of financial damages. After the individual's file has been tapped into, the profile of the individual may include polluted information such as unpaid debts or information pertaining to the profile used to commit a crime. Victims of identity theft are therefore submerged into a "bureaucratic hell" where they must spend time to decontaminate their dossier.[1770] While their dossier

---

[1766] Solove, *The Digital Person*, *supra* note 1753 at 110.

[1767] *Ibid*. at 115-19. Solove notes that investigation and prosecution of identity theft cases is not a top priority for law enforcement agencies, and that victims are slow to realize that their identity has been stolen.

[1768] For instance, a pet's name may be tagged in pictures and someone's mother's maiden name may be available to anyone browsing the individual's profile and friends list and it might be relatively easy to guess the name.

[1769] Hariton, Lawford & Palihapitiya, *supra* note 197 at 20: "While many of the issues have already been raised in the context of credit card and bank debit card use, the use of RFID may involve many more transactions and hence broaden the scope of concern. As well, if small dollar amounts are involved, fraud may not be as readily noticed."

[1770] Janine Benner, Beth Givens & Ed Mierzwinski, "Nowhere to turn: victims speak out on identity theft" (1 May 2000) at pt. II, §§ 1, 4, online: Privacy Rights Clearinghouse <http://www.privacyrights.org/ar/idtheft2000.htm>, discussed in Solove, "A taxonomy", *supra* note 339 at 515.

remains defiled, victims may have difficulty getting employment, loans, or mortgages,[1771] and this may lead to economic or financial harm.

Theft is another type of economic harm which may take place upon the use of personal information by thieves (e.g. home address, whereabouts of the home owner). In its breach notification guidelines, PIPEDA illustrates how the sensitivity of data is dependant on the context and provides the following example: while the list of subscribers to a newspaper is not considered to be sensitive information, the list of subscribers that have requested a stop on their newspaper delivery for a certain period (i.e. they are out of town) would be considered sensitive information.[1772] With new types of wireless devices or smart phones (iPhones, etc.) and "check-in" features, it is now more possible than ever for individuals to disclose their current location in real time.[1773] The site www.pleaserobme.com[1774] was scanning Twitter streams for users who were saying that they were not at home, and then published that information on the website in order to raise awareness of the dangers of individuals publicly posting information about their location.[1775] This is an illustration on how personal information could be used by thieves to commit a burglary, therefore triggering an economic or financial harm for the victims.

When discussing the type of harm resulting from the use of personal information, RAND Corporation refers to an economic harm triggered by discrimination such as

---

[1771] Van den Hoven, "Information Technology", *supra* note 642 at 311; Solove, *The Digital Person*, *supra* note 1753 at 110; See also Solove, "A taxonomy", *supra* note 339 at 507.

[1772] OPCC, *Key Steps for Organizations in Responding to Privacy Breaches: Guidelines* (August 2007), at 2, online: <http://www.priv.gc.ca/information/guide/2007/gl_070801_02_e.asp>: "What is the context of the personal information involved? For example, a list of customers on a newspaper carrier's route may not be sensitive. However, the same information about customers who have requested service interruption while on vacation may be more sensitive."

[1773] Some may be reluctant to broadcast their location through Foursquare or other OSNs, because they worry that this might let a thief know that they are not at home. Riva Richmond, "Apple's Plans for iPhone Location Privacy" *The New York Times* (8 April 2010), online: The New York Times <http://gadgetwise.blogs.nytimes.com/2010/04/08/apples-plans-for-iphone-location-privacy/>: "But I don't much like the idea that someone might be tracking my every movement. And I'm reluctant to broadcast my location through Foursquare or other social networking services, because I worry that might let a thief know that I'm not at home — or tell a frienemy where the party is."

[1774] Online: Please rob me <http://www.pleaserobme.com>.

[1775] Preston Gralla, "Google CEO Schmidt: We can know everything about you" (18 February 2010), online: Computer World <http://blogs.computerworld.com/15614/google_ceo_schmidt_we_can_know_everything_about_you>.

"financial damages suffered as a consequence of (…) financial or economic discrimination."[1776] Financial harm may potentially be linked to, or result from, some type of discrimination; this theme will be explored in the following section.

3.2.1.2.2. Discrimination (Information Inequality)

A second type of objective harm has to do with discrimination. Van den Hoeven proposes a classification of four types of harm that may arise as a result of the compromise of privacy protections.[1777] The second type of harm which I will discuss is one that van den Hoeven refers to as "Information Inequality". According to him, this type of moral reason to justify constraints on our actions with identity-relevant information is concerned with *equality and fairness*.

As early as the 1970s, misuse of data and the resulting discrimination was of paramount importance; evidence of this can be found in the documents leading to the adoption of Convention 108.[1778] It is interesting to note that DPLs were also meant to address inequalities.[1779] The preamble of the U.S. *Department of Health, Education, and Welfare's report on computerized records* (1973) presents fairness or justice as a foundational value for regulating the collection, storage, and use of personal information in computerized databases.[1780] While DPLs don't prohibit discrimination *per*

[1776] Robinson et al., *supra* note 151 at 48.

[1777] Van den Hoven, "Information Technology", *supra* note 642 at 311. Information based harm; Information inequality, Information injustice, and Restriction of moral autonomy.

[1778] Resolutions (73) 22 and (74) 29 refer to electronic data processing that "may lead to unfair discrimination". See Council of Europe, *Explanatory Report: Resolution (73) 22*, *supra* note 56 at para. 19 and Council of Europe, *Resolution (74) 29*, *supra* note 13 at Principle 3 of Annex.

[1779] Nissenbaum, *supra* note 230 at 147-48: "There are a number of facets to this value. In the crucial 1973 U.S. Department of Health, Education, and Welfare's report on computerized records, the opening sentences presented fairness, or we might say justice, as a foundational value for regulating the collection, storage, and use of personal information in computerized databases. The Department's politically grounded argument will be familiar in the American contexts where entities, such as government and financial institutions, wield significant power over the fates of individual citizens and clients. Allowing these institutions free reign in collecting and using information further tips the balance of power in their favor. Responsive to the strong sentiment in favor of leveling the playing field, the widely influential Code of Fair Information Practices defined restrictions on gathering, storing, and using information about people in the name of fairness."

[1780] U.S. Department of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *supra* note 57 at s. IV.

se, they provide certain restrictions on the use of personal information, which may be useful in the context of addressing the concerns resulting from this kind of harm.[1781]

Information may be used to discriminate, remove a benefit or tarnish a reputation. An individual may be subject to some type of discrimination, which could lead him to being refused for a job, refused for credit, mortgage or a loan etc.[1782] Many have voiced their concerns about consumer profiling, as it is a tool used to facilitate the practice of discrimination.[1783] Classifying people in such a way that their chances of obtaining certain goods, services or employment are diminished may also illustrate this type of harm.[1784] Van den Hoeven suggests that: "accumulative information-based harm would refer to the releasing snippets of identity-relevant information at different occasions on the basis of which others may eventually form a rich and comprehensive picture of a person and inflict harm on him or her."[1785]

With the onslaught of new Internet technologies, online profiling activities are taking on a range of different forms. For instance, certain website providers are tailoring the content of their sites as a function of user profiles. Whether this practice is harmful to the user is debatable; in certain cases, it may actually prove to be beneficial.[1786] I will discuss certain online practices which may potentially be viewed as some type of discrimination (objective harm).

[1781] DPLs provide that individuals be informed of the information used in decisions affecting them and have the right to consent to this use, that the information used shall be relevant for the intended purpose, and that these individuals be able to verify that the information used is accurate. The idea is that if there is a "use" of information which may create a risk of objective harm to individuals, at least the use (decision or assessment) will have been taken based on data which is "accurate" and "relevant" for the intended use. These criteria ("accurate" and "relevant") are further discussed in sections 3.2.2.2 and 3.2.2.3.

[1782] Being black listed or refused certain services on the basis of a tarnished reputation can lead to a psychological harm. However, this harm will usually be also of an economic or financial nature, and therefore, this harm falls under the category of "objective" harms.

[1783] PIAC, *supra* note 448 at 10-11; See Conseil de l'Europe, *L'autodétermination informationnelle*, *supra* note 20 at 24: "Ainsi, la création, au sein de réseaux inter-entreprises ou inter-administrations, de bases de données permettant un profilage a priori des utilisateurs de services peuvent amener à les discriminer lors de la recherche d'un logement, de la recherche d'information, de la demande d'une couverture d'assurance ou de l'acquisition d'un ouvrage."

[1784] Van den Hoven, "Information Technology", *supra* note 642 at 312: "Being classified as Muslim in many Western countries implies a reduced chance of getting a job."

[1785] *Ibid*.

[1786] See section 1.2.4.1 entitled "New Business Models (Customization and Sponsored Services)" elaborates on new uses made of information by organizations active online.

(a) Adaptive Pricing

One discriminatory practice taking place online is known as "adaptive pricing" or "dynamic pricing". Some refer to this growing problem as first-degree price discrimination, a practice where organizations attempt to perfectly exploit the differences in price sensitivity between consumers.[1787] With consumer profiling, consumers can be sorted as individuals or groups by retailers and this makes it possible for the retailers to create a pricing scheme tailored to individual customers based on their purchase or online histories.[1788]

For example, a retailer could create a pricing scheme tailored to each customer by offering a different basket of services to distinctive groups of clients and display a price (higher or lower) which would be based on the profile of the potential buyer. Economically speaking, since a unique price for all customers would not maximize the retailer's profit (since certain customers may be willing to pay more than others) maximizing the profit would only be reached if each product is sold for the maximum price that the individual is willing to pay. I already discussed the case of Amazon which was suspected of using such practices, using cookies to identify the visiting consumers.[1789] In the offline space, retailers could profile a customer in real-time (based on an RFID read of objects carried and by cross-referencing to past buying patterns) and they may offer differential service based on the "value" of the customer to the retailer.

One could claim that certain privileged customers may actually benefit from this practice but some claim that: "Ironically, more loyal shoppers may end up paying more for products than other shoppers as retailers develop the ability to track product desire and ability to pay".[1790] As a matter of fact, it is not clear that the value that this creates for organizations is passed on to individuals, as suggested by Janet Gertz:

[1787] Anthony Danna & Oscar H. Gandy, Jr., "All That Glitters is Not Gold: Digging Beneath the Surface of Data Mining" (2002) 40 Journal of Business Ethics 373 at 381.

[1788] Tal Z. Zarsky, "Mine Your Own Business!: Making the Case for the Implications of Data Mining of Personal Information in the Forum of Public Opinion" (2002-03) 5 Yale J.L. & Tech. 1.

[1789] Conseil de l'Europe, *L'autodétermination informationnelle*, *supra* note 20 at 29.

[1790] Hariton, Lawford & Palihapitiya, *supra* note 197 at 20.

> "By profiling consumers, financial institutions can predict an individual's demand and price point sensitivity and thus can alter the balance of power in their price and value negotiations with that individual. Statistics indicate that the power shift facilitated by predictive profiling has proven highly profitable for the financial services industry. However, there is little evidence that indicates that any of these profits or cost savings are being passed on to consumers. For this reason, and because most consumers have no practical ability to negotiate price terms for the exchange of their data, many characterize the commercial exploitation of consumer transaction data as a classic example of a market failure."[1791]

CIO Insight Magazine published an article discussing pricing ceilings where price discrimination is described as a goal for the industry.[1792] In the U.K., the OFT has also expressed its concern over price discrimination, especially if consumers are left in the dark.[1793]

(b) Eliminating Customers

With consumer profiling, consumers can be identified by retailers as individuals or groups, allowing them to discriminate against customers and even eliminate or avoid certain individuals based on their purchases or online history.[1794] Chris Jay Hoofnagle ("Hoofnagle") and Kerry E. Smith ("Smith") warn that information flows can be used to eliminate certain customers.[1795] They point to an emerging movement called "Customer Relationship Management" that would systematically exclude customers if they are not profitable to the business. To illustrate this, the authors refer to the example of the president of a retail consulting firm who was urging storeowners to create disincentives for certain customers in order to eliminate them. The bottom 20% of the population is referred to as "bottom feeders," those who frequently complain and have low-levels of

---

[1791] Janet Dean Gertz, "The Purloined Personality: Consumer Profiling in Financial Services" (2002) 39 San Diego L. Rev. 943 at 964-65.

[1792] Amy Cortese, "Price Flexing: How the Web Adds New Twists", *CIO Insight* (1 March 2002).

[1793] OFT is conducting two market studies into websites using behavioural data to set customized pricing, where prices are individually tailored using information collected about the user's behaviour. Julia Kollewe, "Office of Fair Trading to probe use of personal data by online retailers", *The Guardian* (15 October 2009).

[1794] Zarsky, *supra* note 1788.

[1795] Hoofnagle & Smith, *supra* note 82 at 20-21. See also various examples showing how prices have been increased, at 13 to 17 inclusively.

customer loyalty.[1796] Professors Anthony Danna and Oscar Gandy ("Gandy") explain that information flows may be used more frequently in the future to create databases of undesired customers.[1797] While organizations may simply be trying to locate and retain loyal customers so that they can avoid the traditional means of successful sales (offering the best product or service at the lowest price), these practices may be assimilated with some type of discrimination which may be harmful for certain individuals.

(c) Profiling

With consumer profiling, retailers are in a position to offer a basket of select services to a clients based on their profile (created with their purchase or online histories).[1798] Some may argue that more efficient tailoring methods may be a positive thing for consumers while others are not so convinced. For example, Gandy has vividly conveyed how profiling and the widespread collection, aggregation, and mining of data increase social injustice and generate even further discrimination against traditionally disadvantaged ethnic groups.[1799] Hoofnagle and Smith claim that financial institutions may analyze and use information that they collect about their customers in order to target them for the purchase of products and services and that the data may potentially be used to deny consumers choice or to steer them towards choices not in their best interest.[1800]

For instance, in the financial services arena, personal information has been used to unload unwanted products to low priority consumers; these include minorities, the poor

---

[1796] Mickey Alam Khan, "Technology Creates Tough Environment for Retailers" (13 January 2003), online: DMNews <http://www.dmnews.com/cgi-bin/artprevbot.cgi?article_id=22682>, discussed in Hoofnagle & Smith, *supra* note 82 at 20-21. See various examples showing how prices have been increased, at 13 to 17 inclusively.

[1797] Danna & Gandy, *supra* note 1787 at 381, citing Frederick Newell, *loyalty.com: Customer Relationship Management in the New Era of Internet Marketing* (New York: McGraw-Hill, 2000); Don Peppers & Martha Rogers, *The One to One Future: Building Relationships One Customer at a Time* (New York: Currency, 1997), discussed in Hoofnagle & Smith, *supra* note 82 at 20-21.

[1798] Zarsky, *supra* note 1788.

[1799] See Gandy, *supra* note 1236; Oscar H. Gandy, Jr., "Coming to Terms with the Panoptic Sort" in David Lyon & Elia Zureik, eds., *Computers, surveillance, and privacy* (Minneapolis: University of Minnesota Press, 1996) 132; Oscar H. Gandy, Jr., "Exploring Identity and Identification" (2000) 14 Notre Dame J.L. Ethics & Pub. Pol'y 1085, all of which are discussed in Nissenbaum, *supra* note 230 at 150-51.

[1800] Hoofnagle & Smith, *supra* note 82 at 13.

and non-English speakers.[1801] To illustrate this statement, they provide the case of a sworn declaration of a former CitiFinancial employee confirming that branch managers targeted deceptive loan solicitations to borrowers in certain zip codes (belonging to less affluent areas) or that they attempted to sell extra insurance by identifying vulnerable borrowers based on their occupation, race, age and education level.[1802] In the Minnesota Attorney General investigation case, it was found that the elderly and those who spoke English as a second language were particularly vulnerable to preacquired account telemarketing fraud.[1803] The PIAC produced the following comments on this issue:

> "Consumer profiling could place low-income and vulnerable consumers at risk, as their profiles may lead them to be neglected, avoided or preyed upon. Facts about an individual, such as prior bankruptcy, may disqualify vulnerable consumers from economic transactions. Such profiling shifts the balance of power in business-to-consumer relationships. With consumer profiling, any semblance of equal footing between businesses and consumers is displaced as profiling allows for segregation based on social or economic criteria. Online consumer profiling is an efficient and effective system for monitoring, making it possible for the vendor or service provider to make subtle distinctions of rank.[1804]

Profiling methods can therefore result in harm to poorer sections of the population and vulnerable consumers, who might be targeted for useless services based upon their profile information.[1805] One way to avoid this unfair discrimination is to ensure that only personal information which is relevant for the intended use is actually used in the

---

[1801] *Ibid*. at 19: "The depositions conducted by the Commission in the CitiFinancial investigation demonstrated that information flows allowed employees to access personal financial information without authorization, and pack unneeded products to minorities, the poor, and non-English speakers."

[1802] *FTC v. Citigroup*, No. 1:01-CV-00606, Decl. of Gail Kubiniec, 10 (May 2001) at 14. One stated, "If someone appeared uneducated, inarticulate, or was a minority, or was particularly old or young, I would try to include all the coverages CitiFinancial offered. The more gullible the consumer appeared, the more coverages I would try to include in the loan."

[1803] See U.S., *Financial Privacy and Consumer Protection Hearing Before the Senate Comm. on Banking, Housing and Urban Affairs*, 107th Cong. (2002) (statement of Mike Hatch, Attorney General, State of Minnesota) who elaborates on how the Office's review of randomly selected sales of one preacquired account telemarketer revealed that 58% of customers whose accounts were charged were over 60 years old, discussed in Hoofnagle & Smith, *supra* note 82 at 19-20.

[1804] Lawrence Lessig argues that online consumer profiling brings us back to the past, where hierarchical social orders can now persist. See PIAC, *supra* note 448 at 10-11.

[1805] Lo, *supra* note 188 at 53.

decision-making process.[1806] But in certain situations this "relevancy" criteria is difficult to evaluate, such as with behavioral marketing practices.

(d) Behavioral Marketing

Online behavioural advertising involves tracking consumers' online activities over time in order to deliver targeted advertisements tailored to their inferred interests.[1807] The fact that information collected online may be used to target individuals is a reality with new Internet technologies, and some claim that this information may be used to discriminate against individuals. Janet Lo raises that: "Data mining enhances marketers' ability to discover hidden traits of their customers and possibly cause them additional distress, leading to seclusion of certain vulnerable consumers."[1808] A concern is that online behavioural targeted advertising based on data mining practices may push individuals to make certain consumer decisions by narrowing the options they receive, and offering persuasive arguments at the right time to lower the resistance of the consumer.[1809] The PIAC is concerned that this kind of practice may result in providing less choices or options to customers:

> "When the motives of the advertisements are not obvious and the system appears to know the consumers' thoughts and desires better and earlier than they know themselves, how will the consumer be aware of where these desires came from? Legal scholar Lawrence Lessig argues that it is possible that consumer profiles will begin to normalize the population from which the norm is drawn as observation affects the observed. In the broader societal context, thoughts and beliefs could be directed by pre-sorted information chosen by others in the case where there is not sufficient diversification in the media market. Such foundational concerns with possible societal ill-effect of consumer profiling and discrimination should lead the OPCC to carefully consider the privacy implications of current and future industry practices of online targeted behavioural advertising and consumer tracking."[1810]

[1806] See section 3.2.2.3 which elaborates on this issue.

[1807] Behavioural advertisers often use sophisticated algorithms to analyze the collected data, build detailed personal profiles of users, and assign them to various interest categories. Interest categories are used to present ads defined as relevant to users in those categories. See OPCC, *Online Behavioural*, *supra* note 275 at 1.

[1808] Lo, *supra* note 188 at 54.

[1809] Zarsky, *supra* note 1788 at 22.

[1810] PIAC, *supra* note 448 at 10-11 [footnotes omitted]

Jason Millar articulates the view that predictive data mining practices have the potential to violate our core privacy because they may expose an individual's beliefs, intentions and desires.[1811] Tal Z. Zarsky highlights the concern that data mining practices manipulate and threaten consumer and societal autonomy, and refers to this as the "autonomy trap."[1812]

3.2.1.2.3. Physical Harm

A third type of objective harm is a physical one. For example, individuals may become a victim of a crime against their person, in the event that their information (home or work address) are used by criminals such as stalkers and rapists.[1813] The harm in question can be severe, a perfect example is the murder of actress Rebecca Schaeffer in 1989. It was discovered that her assailant located her home address through the records of the Department of Motor Vehicles.[1814] In the U.S. case *Remsburg v. Docusearch*,[1815] a stalker killed a woman after obtaining her work address from a data broker. Criminals can sometimes use the Internet and on-line databases to track down their victims. Canadian breach notification provisions include, in the definition of "significant harm", "bodily harm"[1816] (PIPEDA) and "physical harm"[1817] (Alberta). The Alberta report pertaining to breach notifications also implies a physical type of harm when it states that:

> "Although an organization does not need to consider the point of view of each affected individual, the organization needs to consider the general

---

[1811] Jason Millar, "Core Privacy: A Problem for Predictive Data Mining" in Ian Kerr, Valerie Steeves & Carole Lucock, eds., *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society* (New York: Oxford University Press, 2009) 103 at 119, online: <http://www.idtrail.org/content/view/799>.

[1812] Zarsky, *supra* note 1788 at 38.

[1813] Robinson et al., *supra* note 151 at 48. See also Van den Hoven, "Information Technology", *supra* note 642 at 311: "Stalkers and rapists have used the Internet and online databases to track down their victims. They could not have done what they did without access to electronic resources and without accessing some of the details of their victim's lives."

[1814] See *Margan v. Niles*, 250 F. Supp. 2d 63 at 68-69 (N.D.N.Y. 2003).

[1815] *Remsburg*, *supra* note 1379.

[1816] *Safeguarding Canadians' Personal Information Act*s, *supra* note 506 aimed to amend PIPEDA was re-introduced by the Government of Canada on September 29, 2011. This bill proposes amendments related to, among other things, breach notification, business transactions and disclosures to law enforcement.

[1817] Service Alberta, *supra* note 1367 at 2-3.

> circumstances. For example, if a women's shelter loses its client list, the possible harm might be much more significant than the possible harm if a fitness club loses its membership list."[1818]

The FTC, in its recent 2012 Report, states that:

> "a consumer can use a mobile application on her cell phone to "check in" at a restaurant for the purpose of finding and connecting with friends who are nearby. The same consumer might not expect the application provider to retain a history of restaurants she visited over time. If the application provider were to share that information with third parties, it could reveal a predictive pattern of the consumer's movements thereby exposing the consumer to a risk of harm such as stalking."[1819]

These types of uses (physical harms), together with fraud and identity theft, are of a criminal nature, and they are governed by criminal laws (therefore, they are to a certain extent outside the scope of this thesis). As we have seen, when certain objective harms resulting from the use of personal information are found to be very significant for individuals, they are often governed by laws, other than DPLs, which address these harms specifically. Still, acknowledging that certain disclosures may be harmful because criminals may use the information is relevant when assessing the risk of objective harm (or in assessing if there is a risk upon disclosing this information).

3.2.2. Risk of Objective Harm: Criteria to Take Into Account

Canadian and French DPLs usually stipulate that obtaining consent is a necessary precondition for the "use" of personal information.[1820] Certain DPLs, such as the Alberta and the B.C. DPLs, provide that the consent is deemed or presumed in certain situations.[1821] As already mentioned, in France, an organization would be able to use

---

[1818] Service Alberta, *supra* note 1367 at 2-3.

[1819] Cf. *U.S. v. Jones*, 565 U.S. 132 S. Ct. 945 at 955 (2012) (Sotomayor, J., concurring) (noting that "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations"), discussed in FTC, *Recommendations* 2012, *supra* note 381 at 33.

[1820] PIPEDA, *supra* note 63 at Schedule 1 (s. 5), principles 4.3 and 4.5; Quebec DPL, *supra* note 110 at ss. 13-14; Alberta DPL, *supra* note 114 at Part 2, Division 2, s. 7 (1) (c); B.C. DPL, *supra* note 115 at Part 3, ss. 6 (1) (a), (b), (c) and 6 (2) (a), (b), (c); *Loi informatique et liberté*, *supra* note 131 at c. II, s. 1, art. 7 (5).

[1821] One example of such a situation would be if personal information is provided voluntarily for the intended purpose (i.e. the "use") and if it is reasonable that a person would voluntarily provide that

the personal information without having obtained the prior consent of the individual if the use is legitimate and the organization takes into account the fundamental rights of the individual.[1822] The Directive 95/46/EC also has a consent requirement prior to use, with certain specific exceptions.[1823]

Section 3.1.2.2 details the relevant criteria in establishing the risk of subjective harm that may emerge when information is "disclosed", which is the fact that the information is "identifiable", of an "intimate" nature, and whether previously "available" (and the extent of such availability). In light of the objective harm, whether financial, discriminatory, or physical, linked to the use of personal information, there are two central outcomes that I will elaborate on.

First, I maintain that the only relevant criteria when assessing whether the use of certain information should be governed by DPLs is whether the use of the information will create an objective harm to the individual concerned (instead of whether the individual is "identifiable"). Once it is determined that the use of information triggers an objective harm, then whether the information used is "accurate", and whether it is "relevant" to the intended use will be important. These criteria are discussed below under sections 3.2.2.2 and 3.2.2.3 respectively.

Second, I maintain that the relevant criteria when establishing the *risk of harm* generated by the use of data (objective harm) are quite different than those relevant in the context of disclosure (subjective harm). The criteria of "identifiability", "intimate" nature and "availability" of the data, pivotal when assessing the risk of harm at the "disclosure" level, are not relevant to assess whether there is an objective harm. The picture is flipped when we are assessing the risk of harm at the "disclosure" level. In the event that the data is "disclosed", the criteria of "relevancy" and data "quality"

information. Alberta DPL, *supra* note 114 at Part 2, Division 2, s. 8 (2) and (3); B.C. DPL, *supra* note 115 at Part 3, s. 8 (1) (a) and (b).

[1822] *Loi informatique et liberté*, *supra* note 131 at c. II, s. 1, art. 7 (5).

[1823] EC, *Directive 95/46/EC*, *supra* note 99 at art. 7 (a), (b), (c), (d), (e), and (f).

(which are important to take into account in the presence of an objective harm) are much less important to assess the risk of subjective harm.[1824]

The notion of "identifiability" is quite relevant when assessing the risk of subjective harm triggered by the disclosure of information. For instance, an individual may not be embarrassed or humiliated by the disclosure of "intimate" information, if this information is not "identifying".[1825] Whether the information is "identifying," at the "use" level, is much less relevant, since the ultimate test is whether the information used may have a negative impact (objective harm) on the individual, regardless of whether the individual is identifiable by name, as further discussed in section 3.2.2.1.

The "intimate" nature of the data used will usually not be very relevant when assessing the risk of objective harm. While certain individuals may feel "uncomfortable" with the idea that certain data of an intimate nature may be used to take a decision which may have an impact on them, if the data is "relevant" for the purpose used, and is of "quality" in light of such purpose, individuals may have a hard time arguing that a certain use is harmful to them. An applicant for a position with a pharmaceutical company, for example, may be required to submit personal health records in order to demonstrate the lack of prior addiction to narcotics. This information will be a definitive factor in the hiring process, potentially triggering an objective harm for the individual as detailed under sections 3.2.1.2.1 and 3.2.1.2.2, if the individual is not hired. A health record may be viewed by some as information of an "intimate" nature, but I argue that this criterion is not relevant when assessing the risk of objective harm and that the test (to assess if there is an objective harm) should not take it into account. Instead of evaluating whether the information is of an "intimate" nature, I maintain that the test should focus on whether the data used (health record) is "relevant" and "accurate" for the purpose of assessing the applicant's candidacy.

The "availability" of the information is relevant when assessing the risk of harm at the disclosure level, however it, is not relevant when assessing the risk of harm at the

---

[1824] See section 3.1.2.2 entitled "Risk of Subjective Harm: Revisiting the Sensitivity Criteria" and section 3.2.2 entitled "Risk of Objective Harm: Criteria to Take Into Account" which elaborates on this issue.

[1825] See section 3.1.2.2.1 which elaborates on this issue.

"use" level. According to certain DPLs, personal information that is already publicly available or made available by the individual may be used without the individual's prior consent.[1826] In this Information Age, and with new technology and tools on the Internet, there is a considerable amount of information already at our fingertips.[1827] I will illustrate my views using the example of an individual applying for a position with a bank. The potential employer may want to verify certain information pertaining to the applicant's credentials with information available online. The bank may access an old resume made available online on LinkedIn which may not pass the "accuracy" test,[1828] because it may not be up-to-date. The bank may also access certain compromising pictures of the applicant through Facebook, but this employer may have a hard time actually using these pictures unless they pass the "relevancy" test.[1829] Bottom line, it is not because the data is publicly available, that it can be used unconditionally. The data has to be relevant and accurate for the purposes of using the data, in order to comply with the second step of the proposed test.[1830]

Certain DPLs also have "reasonableness" or "legitimacy" tests.[1831] Clearly, when a certain "use" of personal information by an organization creates no risk of objective harm, then it is more easily considered as being either "reasonable" or "legitimate". In the following section, I discuss the sole criteria which may be useful in assessing whether a use of personal information may trigger an objective harm.

3.2.2.1. Identifiability Replaced by Negative Impact (Objective Harm)

Information usually has to be able to "identify" an individual to qualify as *personal* under DPLs. I argue that this criterion of "identifiability" is much less relevant when assessing if there is an objective harm upon information being used, and that this metric

---

[1826] See section 3.1.2.2.3(a)(i) entitled "Publicly Available Information" which elaborates on this issue.

[1827] See section 1.2.1 entitled "Increase in Volume of Information" which elaborates on this issue.

[1828] See section 3.2.2.2 entitled "Accuracy of Information Used" which elaborates on this issue.

[1829] See section 3.2.2.3 which elaborates on this issue. See also Eloïse Gratton, "Can Quebec Employers Search OSNs for Employee-related Information?" (2009) PrivacyScan [Gratton, "Quebec Employers"].

[1830] See section 3.2.2.2 and section 3.2.2.3 which discuss the second steps of the test to be used when assessing the risk of objective harm.

[1831] See section 2.2.1.3.2(a)(i) entitled "Reasonableness or Legitimacy Tests" which elaborates on this issue.

("identifiable") should instead be replaced by the following: whether the information used may have a "negative impact" (objective harm) on the individual.

I maintain that the first part of the test, in order to determine whether a certain piece of information "used" should be regulated by DPLs, would be to establish whether the use of the data has an impact on an individual. As a matter of fact, information may in certain cases be "used" by organizations for various purposes which may have no impact whatsoever on an individual, a very indirect and limited impact, or even a positive one. I argue that in such cases, the information should not be governed by DPLs.

This is especially relevant in light of the fact that personal information is valuable for various organizations since it provides knowledge over a whole range of issues: population health, interests, hobbies, trends, etc. Personal information may therefore be valuable to the government, to organizations and even to society at large.[1832] Section 2.1.1.1.2 also details how new types of data (such as online search queries) provide a wealth of information.[1833] According to Ron A Dolin, as long as the search data is stored securely, the privacy issues should be of no concern.[1834]

Current DPLs already partially address the usefulness of personal information by including exceptions for uses of information for historical, statistical or scientific purposes.[1835] This notion of usefulness is not a new one. As early as 1972, when DPLs were in their infancy, it was clear that a great deal of personal information would be useful to provide statistics to assist planning and other research. Since researchers (or

---

[1832] See section 2.1.1.1.1 entitled "Ignoring the Importance of Information Flow For the Society" and section 2.1.1.1.2 entitled "Ignoring Legitimate Reasons for Collecting, Using and Disclosing Information" which elaborate on this issue. See also Van den Hoven, "Moral Wrong-doing", *supra* note 272 at 33: "The communitarian arguments to make more information on persons available and to relativize privacy claims are often clear, straightforward and convincing. They refer to benefits to the community of having knowledge about its members freely available."

[1833] For example, several queries about foreclosures or bankruptcies may indicate pending economic problems and allow to detect a signal early enough to prevent a national or international economic crisis.

[1834] Dolin, *supra* note 371 at 144: "This is similar to our treatment of census data, even though that data collection is compulsory, while for search queries it is voluntary. The trade-off we make here in the name of privacy is the loss of the vast potential usefulness of the data. If they can be kept intact safely, however, the apparent dichotomy goes away."

[1835] See for example B.C. DPL, *supra* note 115 at Part 6, s. 21 (1) (c); See also EC, *Directive 95/46/EC*, *supra* note 99 at art. 13 (2).

information gatherers in general) rarely needed to know the identity of their data subjects, the anonymization of data was seen as a natural solution.[1836] Now that it is less and less clear at what point data is in fact anonymized,[1837] I argue that we should focus on protecting information that may trigger a risk of harm upon being used or disclosed.

3.2.2.1.1. Purpose behind Regulating the Use of Data: Negative Impact

The original goal behind DPLs regulating the use of personal information was to avoid the kind of objective harm discussed in section 3.2.1. I maintain that this translates into DPLs regulating information being "used", only if it is used in such a way which will create a "negative impact" on the individual (therefore triggering an objective harm to the individual).[1838]

According to older as well as more recent documents (including DPLs), the central concern behind regulating the use of information has to do with the awareness of potentially negative impacts on the data subjects (objective harm). A number of provisions or principles lead us to this conclusion.

DPLs were to apply to information "used" in such a way which would have an impact on the individuals. For instance, the Lindop Report (U.K. 1978) mentioned that: "The objective of discarding outdated data clearly applies principally to data used for making decisions which affect the data subject."[1839] Many recent DPLs provide that the information should be accurate, especially if it will be used in such as way which will create a negative impact on the individual. For example, PIPEDA provides that

---

[1836] *Report of the Committee on Privacy*, *supra* note 3 at 183, para. 594: "A great deal of personal information is acquired to provide statistics to assist planning and other research, or is acquired for some other purpose and subsequently adapted to a form suitable for such ends. Planners and researchers, however, rarely need to know identities of individuals. Therefore: "4. In computerised systems handling information for statistical purposes, adequate provision should be made in their design and programs for separating identities from the rest of the data."

[1837] See section 2.1.2.2.1(c) entitled "At what point is data anonymized?" which elaborates on this issue.

[1838] Such as a financial or physical harm, or some type of discrimination. See section 3.2.1.2 entitled "Types of Objective Harm" which elaborate on this issue.

[1839] Lindop, *supra* note 96 at 51, para. 5.61: "The objective of discarding outdated data clearly applies principally to data used for making decisions which affect the data subject, and several witnesses told us that users should not be prevented from retaining personal records for statistical, research and archival purposes."

organizations should avoid that "inappropriate information (…) be used to make a decision about the individual."[1840] Article 38 of the C.c.Q. states that any person may examine and cause the rectification of a file kept on him by another person "with a view to making a decision in his regard or to informing a third person."[1841] The Quebec DPL includes special provisions for money lending organizations. Such organizations must, upon request, divulge the content of any credit report consulted for the purpose of "making a decision concerning the person".[1842] Under the B.C. DPL, an organization must make a reasonable effort to ensure that personal information collected by or on behalf of an organization is accurate and complete, "if the personal information is likely to be used by the organization to make a decision that affects the individual to whom the personal information relates."[1843] The French DPL, in line with the Directive 95/46/EC on the subject matter, has a similar provision: any individual is entitled to interrogate the data controller of his personal data in order to obtain information allowing him to know and to object to the reasoning involved in the automatic processing, "in the case of a decision taken based on automatic processing and producing legal effects in relation to the data subject".[1844] This obligation has an additional layer of complexity (also in line with the Directive 95/46/EC),[1845] as it provides that no decision having a legal effect on an individual may be taken solely on the grounds of automatic processing of data.[1846] These provisions were clearly meant to ensure that when personal information is used in assessments or decisions that may have a negative impact on an individual (what I refer to as an objective harm), the data in question should at least be accurate. It is interesting to note that under the Directive 95/46/EC, the decision has to either produce "legal effects" for, or "significantly affects", an individual.[1847] This means that there is an argument to be made that perhaps an

---

[1840] PIPEDA, *supra* note 63 at Schedule 1 (s. 5), principle 4.6.1.

[1841] Art. 38 C.c.Q.

[1842] Quebec DPL, *supra* note 110 at s. 19.

[1843] B.C. DPL, *supra* note 115 at Part 9, s. 33 (a).

[1844] *Loi informatique et liberté*, *supra* note 131 at c. V, s. 1, (II), art. 39 (5); EC, *Directive 95/46/EC*, *supra* note 99 at art. 12 (a).

[1845] *Ibid*. at art. 15 (1) and (2).

[1846] *Loi informatique et liberté*, *supra* note 131 at c. II, s. 2, art. 10.

[1847] EC, *Directive 95/46/EC*, *supra* note 99 at art. 15.

organization using personal information which triggers a non significant impact for an individual should not be regulated in all instances by DPLs and a positive impact, even less.

It is not always clear whether new types of data are covered under the definition of *personal information*, as discussed in sections 3.1.2.2.1(a)(ii) and 3.1.2.2.1(b). The Article 29 Working Party commented on this very issue as it relates to RFID tags, noting that data relates to an individual, "if such information is used to determine or influence the way in which that person is treated or evaluated."[1848] This further confirms that information (including new types of data) should only be covered by DPLs if their use creates an impact on individuals.

The Lindop Report (U.K., 1978) mentioned that personal information be verified by the relevant individual before being "used" for "any purpose likely to affect the data subject",[1849] and also suggested that:

> "A point often made was that the data subject should be able to see such data as soon as they were disclosed to a third party or used as the basis for an adverse decision against him.[1850]

As far as DPLs are concerned, protecting against the use (or misuse) of personal information has everything to with protecting against the risk of objective harm (see section 3.2.1). Clearly, however, this risk only becomes a factor when the information is used *to the detriment* of the data subject in question. The parliamentary debates leading to the adoption of the Quebec DPL in 1993 confirm that this particular DPL was initially to focus on regulating uses which would have a "negative" impact on individuals.[1851] The "negative" criterion was eventually abandoned in the final wording of the law, since there was a concern that organizations would argue that certain

---

[1848] Article 29 Data Protection Working Party, *RFID technology*, *supra* note 196 at 8.

[1849] Lindop, *supra* note 96 at 269, para. 30.05: "Accordingly, we believe that such information should, in general, not be used for any purpose likely to affect the data subject unless it has been verified by him, or corroborated by other information from some independent source. This is, of course, one of the arguments for 'subject access' to information."

[1850] *Ibid*. at 49, para. 5.50.

[1851] See *Les travaux parlementaires*, 34th législature, 2nd session, Commission permanente de la culture, cahier no 13 (March 1, 1993), at 23.

"uses" were not negative, they were only potentially so.[1852] In Europe, it is interesting to note that the 2002 Proposals for Amendment to Directive 95/46/EC suggested redefining the scope of the provision pertaining to the use of the information in terms of acts of data processing that include "any kind of discriminatory practice".[1853]

The purpose of DPLs regulating the activity of using personal information was not to address situations or uses having a positive impact for the individual, as illustrated by van den Hoven:

> "They do not mind if their library search data are used to provide them with better *library* services, but they do mind if these data are used to criticize their taste and character. They would also object to these informational cross-contamination when they would benefit from them, as when the librarian would advise them a book on low-fat meals on the basis of knowledge of their medical records and cholesterol values, or when a doctor asks questions on the basis of the information that one has borrowed a book from the public library about AIDS."[1854]

Certain DPLs even authorize the use of personal information by organizations, without obtaining prior consent, if such use is in the interest of the individuals concerned. For instance, the public sector Quebec DPL (An Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information)[1855] states that a public body may use personal information for a new purpose without the consent of the individual if the information is clearly used for the benefit of the person to whom it relates.[1856] Under the Alberta DPL, an organization may use personal information without prior consent, if "a reasonable person would consider that the use of the information is clearly in the interests of the individual" (and consent of the individual cannot be obtained in a timely way), or "the individual would not reasonably be expected to withhold consent."[1857] The B.C. DPL has a similar requirement.[1858] In

---

[1852] Therefore, the word "negative" was removed to avoid any uncertainty pertaining to this issue. See *ibid*.

[1853] *2002 Proposals for Amendment*, *supra* note 794.

[1854] Van den Hoven, "Information Technology", *supra* note 642 at 314.

[1855] R.S.Q., c. A-2.1.

[1856] See section of the public sector Quebec DPL: 65.1 (2) that: "a public body may, however, use such information for another purpose with the consent of the person to whom it relates, or without that consent, but only (…) (2) if the information is clearly used for the benefit of the person to whom it relates".

[1857] Alberta DPL, *supra* note 114 at Part 2, Division 4, s. 17 (a).

Europe, personal data may be processed (or used) if it is deemed necessary for the performance of a contract to which the data subject is party or in order to protect the vital interests of the data subject.[1859]

In Europe, the Article 29 Working Party notes that ultimately, the appropriate legal ground foreseen by Article 7 of the Directive 95/46/EC to legitimize a given data processing will depend on the specific circumstances of such processing. They give the example of a situation in which consent may be necessary to legitimize a certain processing of personal data versus a situation which does not require such consent. For example, they suggest that a supermarket that wishes to tag loyalty cards and link it with information gathered through RFID technology will need the individual's consent to do so. On the other hand, a hospital that uses RFID in surgical instruments to eliminate the risk of leaving an item inside of a patient at the conclusion of an operation may not need the patient's consent insofar as this processing might be legitimized in the vital interests of the data subject.[1860] This example can be used to better illustrate my point: that consent would not be required if the data will be used for a purpose which will have a positive impact for the individual.

The fact that information can be used with no impact for individuals is also addressed in certain documents or DPLs. For example, the Lindop Report (U.K. 1978) mentioned that: "several witnesses told us that users should not be prevented from retaining personal records for statistical, research and archival purposes (…)."[1861] While Canadian and European DPLs usually require that data be collected, used, and/or retained only for specified purposes, there are exceptions which are provided for processing or using data for historical, statistical or scientific purposes, provided that certain appropriate safeguards are complied with.[1862] For example, the Directive 95/46/EC states that:

[1858] B.C. DPL, *supra* note 115 at Part 5, s. 15 (1) (a).

[1859] EC, *Directive 95/46/EC*, *supra* note 99 at art. 7 (a), (b), (c), (d), (e), and (f).

[1860] See Article 29 Data Protection Working Party, *RFID technology*, *supra* note 196 at 10.

[1861] Lindop, *supra* note 96 at 51, para. 5.61.

[1862] See for example, Quebec DPL, *supra* note 110 at ss. 18, 21; Alberta DPL, *supra* note 114 at s. 15; B.C. DPL, *supra* note 115 at Part 6, s. 21 (1) (c); EC, *Directive 95/46/EC*, *supra* note 99 at art. 13 (2).

> "Subject to adequate legal safeguards, in particular that the data are not used for taking measures or decisions regarding any particular individual, Member States may, where there is clearly no risk of breaching the privacy of the data subject, restrict by a legislative measure the rights provided for in Article 12 when data are processed solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics." [1863]

Certain uses are therefore authorized under DPLs, in specific situations in which there is no harm resulting from such uses, because the information is not used for taking measures or decisions regarding any particular individual. This further illustrates that if the information is protected against the risk of harm at the "disclosure" level ("subject to adequate legal safeguards"), and will not be used to create a risk of objective harm to individuals ("not used for taking measures or decisions regarding any particular individual"), then there is no harm in having this information used for scientific research. These findings fully support the argument that only information used to impact an individual negatively (objective harm) should be governed by DPLs.

3.2.2.1.2. The Notion of "Identifying" is Not Relevant at the Use Level

The various definitions of *personal information* in Europe, Canada or France are all very similar.[1864] In section 3.1.2.2.1, I maintain that the notion of "identifiability" should be interpreted taking into account the *risk of subjective harm* taking place at the "disclosure" level. As information becomes more sensitive (in the sense that it is of "intimate" nature and more elusive i.e. less "available"), it becomes more likely that the information would qualify as *personal information*.[1865]

With the advent of certain new technologies, decisions can be made that will exert a palpable impact on the owner of an online profile, without even needing to identify the individual behind the profile (identifying meaning by face, name or address). Therefore, at the "use" level, the metric of whether data "identifies" the individual should be replaced by whether the use of the information may create an objective harm on the

---

[1863] EC, *Directive 95/46/EC*, *supra* note 99 at art. 13 (2).

[1864] See section 1.1.3 entitled "Definition of Personal Information: Origin and Background" which elaborates on this issue.

[1865] See section 3.1.2.2.1 which elaborates on this issue.

individual. Section 2.1.2.3.1 already explains how this notion of identity may be obsolete in certain situations. I argue that this "identifiable" criteria becomes obsolete when the information is used creating a negative impact (objective harm) for the individual concerned.

Certain authors including Solove and the Comité consultatif suggest that the interpretation of the notion of *personal information* should reflect this, therefore, in line with what I propose here.[1866] My approach is also in line with van den Hoven's views, who believes that the referential reading of "personal data", "identity" and "identifiability" of the European DPLs may lead to unduly harsh constraints on the use of *personal data* and that as a result, attributively used descriptions could go unprotected.[1867] According to him, one way to ensure that information that should be protected actually is (and therefore avoiding an under-inclusive interpretation of the definition of *personal information*, see section 2.1.2.1.2) would be to focus on "Identity Relevant Information". This argument is very telling in the context of the "use" of information to the point where I maintain that the notion of "identity" should perhaps not even be taken into account when evaluating a piece of data or data sets that are being "used". More specifically, van den Hoven suggests that given the prominence and importance of identity management technology, RFID technology, profiling and data mining, and genetic profiling, we need to have a new look at the dominant referential interpretation of *personal data*.[1868] Instead of defining the object of protection in terms of referentially

---

[1866] According to Solove, the digital person in digital space is having a greater and greater impact on the flesh-and-blood individual in realspace. Solove, "A taxonomy", *supra* note 339 at 508: "Elsewhere, I have discussed the multitude of ways that the compilation of an individual's data–-what I call the 'digital person'––is being used to make important decisions about an individual. The digital person in digital space increasingly is affecting the flesh-and-blood individual in realspace."; See Conseil de l'Europe, *L'autodétermination informationnelle*, *supra* note 20 at 34. This Comité consultatif discusses how it is now possible to characterise an individual taking into account certain socioeconomic, psychological and philosophical or other in order to apply certain decisions to the point of contact of a certain individual (could be the computer of the individual) without requiring this person's identity (for instance, his name).

[1867] Van den Hoven, "Information Technology", *supra* note 642 at 310: "The referential reading of 'personal data', 'identity' and 'identifiability' of the EU data-protection laws leads to an unduly narrow construal or moral constraints on the use of personal data. As a result, attributively used descriptions could go unprotected. This seems a major weakness of data-protection regimes, because we know that large amounts of data are used attributively in marketing and homeland security investigations, for example, and are the stepping stones to find out about people. One could have a file on an owner of a blue Ford, and add a long list of descriptions, all used attributively, but one piece of information added to the rich and anonymous file could suddenly make the data set uniquely referring."

[1868] *Ibid*.

used descriptions, he articulates the view that we need to define the object of protection in terms of the broader notion of "identity relevant information":

> "The owner of a blue Ford living in a postal code area 2345' could have more than one individual satisfying the description, and the user of these descriptions may not have a particular individual in mind; he just thinks about the owner of a blue Ford 'whoever he is'. 'The owner of a blue Ford', however, could also be used referentially, when we have a particular person in mind or in attendance. 'The man sipping his whisky' (pointing out to the person at a party) is used referentially, and is about the person the speaker mistakenly thought was drinking whisky, even when it turns out he is having apple juice instead of whisky, and there is, strictly speaking, no one over there sipping his whisky."[1869]

Following the proposed approach, data would fall under the definition of *personal information*, regardless of whether or not it is identifying, if it could potentially trigger an objective harm for an individual upon being used; for instance, if the use has a focus on a specific individual. The following example illustrates my point:

> "One may open a mental or another type of file on a person under the label 'the murderer of Kennedy', in the same way crime investigators do, in the hope to find out more information about this person who ever he is, or turns out to be. These initially nondescript identifications may eventually lead to a physical encounter (i.e., arrest or interrogation) later. The history of a particular criminal investigation is at the same time the history of filling the file with identity-relevant information".[1870]

In the above situation, since the information collected under "the murderer of Kennedy" is done in the hopes of eventually being able to arrest or file criminal charges against the right person (use this information in such a way which may trigger a negative impact to the individual concerned), it should be treated and considered as *personal information.*[1871] The Article 29 Working Party notes that behavioural advertising methods often entail the processing of *personal data*.[1872] According to this Article 29

[1869] *Ibid*. at 309-10.

[1870] *Ibid*. at 310.

[1871] This means that some of the obligations provided by DPLs should apply to this data, such as ensuring that the data is "accurate" before using it, and also "relevant" for the intended use. These criterias are further discussed in section 3.2.2.2 and section 3.2.2.3.

[1872] As this term is defined by Article 2 of Directive 95/46/EC and interpreted by the Article 29 Working Party. See interpretation of the concept of personal data in the Article 29 Data Protection Working Party, *Opinion 4/2007*, *supra* note 100.

Working Party, this is due to two reasons which both imply a "use" which will negatively impact the individual regardless of whether the identity (name and face) behind the profile is in fact known:

> "*i)* behavioural advertising normally involves the collection of IP addresses and the processing of unique identifiers (through the cookie). The use of such devices with a unique identifier allows the tracking of users of a specific computer even when dynamic IP addresses are used. In other words, such devices enable data subjects to be 'singled out', even if their real names are not known. *ii)* Furthermore, the information collected in the context of behavioural advertising *relates to*, (*i.e*. is about) a person's characteristics or behaviour and it is used to influence that particular person."[1873]

According to the Article 29 Working Party, as long as the individual behind the profile is "singled out", and this person's characteristics or behavior are used to "influence that person" (what I call a "negative impact" or an objective harm), then the information should qualify as *personal information*. Schwartz and Solove, in a recent article, point out the distinction between "identified" and "identifiable" individual applied in the context of behavioral marketing and also discuss the fact that if an individual can reasonably be capable of being "singled out" from others, then we should consider that the information at stake qualifies as *personal information*.[1874] The proposed framework would ensure that organizations taking decisions with regards to profile information (in certain cases, using new types of data), regardless of whether these profile are "identifiable" or not, would have to comply with DPLs, if these decisions may trigger an objective harm for the individuals involved.[1875]

Organizations may be using information relating to a small group of individuals, for example, individuals that are using the same device. One issue that requires more

---

[1873] Article 29 Data Protection Working Party, *Opinion 2/*2010, *supra* note 191 at 9 [footnotes omitted].

[1874] Schwartz & Solove, *supra* note 529 at 1887-88: "The necessary analysis in PII 2.0 should be contextual. *Identified* information is present when a person's identity has been ascertained, or when there is a substantial risk of identification of a specific individual. In contrast, *identifiable* information exists when such a specific identification, while possible, is not significantly probable. Put differently, the question becomes whether the gathering of information pursuant to behavioral marketing, in a specific application, makes an individual reasonably capable of being 'singled out' from others and linked to her identity. In such cases, the law should treat this information as identified. In other cases, the information that is processed may only be identifiable."

[1875] Such as the kind of objective harm detailed in section 3.2.1.2 entitled "Types of Objective Harm" (discrimination, financial or physical harm).

attention is when a small group of individuals are sharing the same device. Does the negative impact have to be linked to a *unique* individual?[1876] I maintain that the extent of the objective harm should be taken into account when evaluating the data. More specifically, the more impactful or negative the risk of objective harm for the individual upon the information being used, the less important the notion of "identifying" (or having the device link to) a "unique" individual versus a small group of individuals should actually be.[1877]

DPLs include various obligations for organizations handling *personal information* including limits on data collection.[1878] Considering new types of data (such as IP addresses or information collected from cookies) as *personal information* brings the situation where certain information will be governed by DPLs, and this implies certain obligations for organizations handling this information which may be challenging.[1879] At the same time, not to consider these new types of data as *personal information* may be harmful in that this information may be eventually be processed, and "used", as discussed above.[1880]

In the event that the use of personal information has no impact on an individual or exerts a positive one (i.e. is beneficial), I maintain that organizations would not need to ensure compliance with DPLs on the notice and choice aspects. Nevertheless, they

---

[1876] See section 2.1.2.2.2(b) entitled "Device Used by a Group: At What Point is it Identifiable?" which elaborates on this issue.

[1877] For example, if insurance services are being refused to an online profile, the fact that this profile is linked to a device that may be used by more than one individual should not be taken into account and the profile information used should qualify as *personal information* since the use is triggering a negative impact (objective harm) on one individual behind the profile.

[1878] For instance, these include limits on the disclosure of personal information and on intended uses; on obligations to use only accurate information and provide access rights; on obligations to ensure that the information handled is held securely, etc. See section 2.2.1.3.2(a)(ii) entitled "Subjectivity in Type of Notices Provided and Method of Obtaining Consents", section 2.2.1.3.2(a)(iii) entitled "Subjectivity Pertaining to Collection, Use and Disclosure Activities", section 2.2.1.3.2(a)(iv) entitled "Subjectivity in Security Measures to Adopt and Retention Obligations", and section 2.2.1.3.2(a)(v) entitled "Subjectivity in Access Rights and Data Quality" which elaborate on these obligations.

[1879] For instance, it may be difficult for the organization collecting the data to grant access to the individual to which the information belongs if this information has not even been processed. Also, how is it possible for an organization to disclose its privacy policy and obtain consent from someone without actually identifying this individual? See section 2.1.2.1.1(d) entitled "Consequences of Over–Inclusiveness" which elaborates on this issue.

[1880] See section 3.2.1.2 entitled "Types of Objective Harm" which elaborates on the kind of objective harm which may take place upon the information being used.

would need to ensure that the data is stored securely in order to avoid any subjective harm resulting from disclosures, as the case may be (see section 3.1.2.1).[1881] On the other hand, in the event that the use of personal information has a negative impact on the individual, then the information used should qualify as *personal information* and full notice, access, and correction rights (data accuracy, see section 3.2.2.2), should be granted to the affected individuals.[1882]

3.2.2.1.3. Limits to DPLs Addressing Discrimination

The purpose behind DPLs regulating the use of personal information was in part to ensure that only data which is "accurate" and "relevant" for the intended use is considered. But we have to realize that DPLs were not meant to regulate all uses of *personal information* which may be harmful to individuals.

In certain situations, a group of individuals may be discriminated against by a given organization using their personal information. For example, an insurer may wish to refuse all clients living in a certain geographical area. Although, in this case, there would be an objective harm resulting from the use of personal information, the underlying issue may be outside the scope of DPLs, since a group of individuals are discriminated against (instead of a unique individual).[1883]

Certain industries will use personal information in harmful ways towards individuals and discriminate, and this is normal and acceptable to society to a certain extent. For

---

[1881] The security measures would be necessary in the event that the disclosure creates a risk of subjective harm, and taking into account the extent of this harm. See Schwartz & Solove, *supra* note 529 at 1881: "Data security for identifiable information, as for identified information, should be commensurate with the nature of the information and the likely risks of disclosure."

[1882] While I realize that this may be challenging for organizations that wish to apply impactful decisions on profiles, I believe that the approach proposed would comply with the purpose behind regulating the activity of "using" personal information in DPLs.

[1883] See for example Schwartz & Solove, *supra* note 529 at 1869: "Privacy rights should attach when data pertains to particular people. The disclosure that there are nine million people living in New York City does not create a privacy harm for any specific New Yorker. To be sure, certain types of aggregate data can be used in ways to harm people. For example, banks might draw on a statistical indication that a certain demographic group has a much higher default rate to deny loans to members of this group or to charge them higher rates. In addition, actuarial data by insurance companies affects coverage and rate decisions. These decisions can cause harm to people, and these harms do involve information. Nonetheless, this category of harm is far broader than the category of information privacy harms. As a policy matter, these issues raise questions that predominately sound in civil rights, discrimination, and insurance law. At least as far as the analysis of the aggregate data is concerned, the critical issues are not those of information privacy law."

example banks will refuse to give credit (loan, mortgage, etc.) to those who don't have a good financial track record. Employers will refuse to hire individuals who don't have the requisite credentials for a given job, etc. Ron A. Dolin explains how discrimination is, to a certain extent, necessary to ensure the viability of our financial system:

> "Imagine the case of a person with a criminal record where a potential employer wants to know about it. A more common case is where a credit agency has (accurate) information about a person's bad credit. Perhaps the person would like that information deleted. We certainly cannot argue that we keep the information around to benefit him, but rather to protect lenders in an attempt to maintain an efficient financial system. We often allow someone to correct mistakes, say in credit information and criminal records. But we do not always allow even that – say in the case of non-public personal notes. Even for public writings, someone would only have cause to correct mistakes in cases of defamation, but not have the right to delete or alter personal observations by others that are factually correct (e.g., journalism)."[1884]

DPLs apply to general data handling activities unless laws have been adopted to regulate certain situations specifically. Where DPLs have been found not to properly regulate a certain situation, laws specific to that situation have usually been adopted. DPLs or other laws in certain jurisdictions will, for instance, limit the ability of certain employers to make inquiries about employee disabilities or gather information which is not directly linked to the employee's or applicant's employment position and many jurisdictions also prohibit employers from questioning employees or applicants about certain matters or discriminating against individuals unless the information used is in connection with the employment.[1885]

In other cases, laws other than DPLs are regulating certain uses of *personal information* because while the use of *personal information* may not be that harmful (the risk of objective harm is on the low side), there are enough issues or concerns for society to restrict these uses. An example is with unsolicited email marketing, which is being regulated by specific anti-spam laws.[1886] While the objective harm resulting from

---

[1884] Dolin, *supra* note 371 at 161.

[1885] See section 3.2.2.3.2(b) entitled "Evaluating Individuals" which elaborates on this issue.

[1886] In Europe, spam is regulated by the EC, *Directive 2002/58/EC*, *supra* note 860; In the U.S., *The CAN-Spam Act of 2003*, 15 U.S.C. § 7701 [*Can-Spam Act*], regulates spam. In Canada, spam will be regulated by the CASL which will be coming in force in 2012. See Industry Canada, "Electronic Commerce in

unsolicited commercial email marketing is potentially present, it is not necessarily straight forward.[1887] Still, these practices have been found to be problematic that they have been regulated by other means than DPLs.[1888] These examples simply illustrate that there are certain limits to the effectiveness of DPLs in addressing the risk of objective harm triggered by organizations using personal information.

***

DPLs were meant to ensure that individuals, if discriminated against (objective kind of harm discussed in section 3.2.1.2.2), for instance when being refused employment, insurance coverage, or a loan or credit, that this discrimination (or the financial harm which they sustain) be based on data meeting the "relevancy" and "accuracy" criteria; meaning data which is up to date and accurate. This issue is discussed next.

3.2.2.2. Accuracy of Information Used

Nowadays, there is a lot of personal information already in circulation.[1889] Organizations may wish to use this information for various purposes without always considering whether the information is accurate. Jeffrey Rosen aptly observes:

> "Privacy protects us from being misdefined and judged out of context in a world of short attention spans, a world in which information can easily

---

Canada: Government of Canada Introduces Anti-Spam Legislation (CASL)", online: <http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/gv00521.html> [Industry Canada, "Electronic Commerce in Canada"].

[1887] For instance, they may not trigger discrimination or physical harm although they may trigger a financial harm. See Eloïse Gratton, "Dealing with Unsolicited Commercial Emails: A Global Perspective" (2004) Journal of Internet Law 3, at 4 [Gratton, "Unsolicited Commercial Emails"]: "A recent survey also revealed that consumers feel that spam is costing them time and money. The time-consuming process of deleting the unsolicited e-mails is added to the time taken to download spam. Furthermore, Internet users that have e-mail wireless devices that bill them based on the amount of data they download actually pay to receive spam. Certain users have limits on the amount of e-mail their ESP will hold. Spam can often mean a full mailbox, with the result of having desirable e-mails getting rejected. There are many other costs that ISPs and other businesses have to bear due to spam such as: bandwidth and network costs, downtime attributable to spam overload, clogging of computer servers of ISPs, and productivity cost to businesses caused by time taken by employees to open, read, and respond to such messages."

[1888] *Ibid*.; Eloïse Gratton, Bruce McWilliam & Cindy Wan, *Canadian Legal Requirements for Electronic Marketing: International Privacy Guide*, vol. 2 (Thomson Reuters, 2010).

[1889] See section 1.2.1 entitled "Increase in Volume of Information" which elaborates on this issue.

> be confused with knowledge. True knowledge of another person is the culmination of a slow process of mutual revelation."[1890]

DPLs usually provide for a data quality principle under which personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes of its ultimate use.[1891] Longstanding privacy principles, such as the FIPs and the OECD Guidelines, also contain provisions for ensuring the accuracy of records.[1892] One way to ensure the accuracy of the data is for organizations to disclose to the individuals concerned the particular parcels of information that will be used and to allow them to review this data. This principle, known as the "access" principle, is found in most DPLs and grants people the right to access their information, to request that it be corrected or amended if not accurate and up-to-date.[1893] Even inaccurate information may qualify as *personal information,* and this is in fact the purpose behind providing individuals with an access right to their information.[1894]

This data accuracy principle is directly linked with the use of personal information.[1895] The parliamentary debates leading to the adoption of the Quebec DPL in 1993, made reference to the fact that the notion of "accurate" data was only relevant when the information was in fact going to be "used".[1896] As we have already seen, the risk of

---

[1890] Jeffrey Rosen, *The unwanted gaze: the destruction of privacy in America* (Random House, 2000), discussed in Solove, "Privacy", *supra* note 1 at 1424.

[1891] PIPEDA, *supra* note 63 at Schedule 1 (s. 5), principle 4.6; Quebec DPL, *supra* note 110 at s. 11; Alberta DPL, *supra* note 114 at Part 3, Division 2, s. 33; B.C. DPL, *supra* note 115 at Part 9, s. 33 (a); *Loi informatique et liberté*, *supra* note 131 at c. II, s. 1, art. 6 (4); EC, *Directive 95/46/EC*, *supra* note 99 at art. 6 (1) (d).

[1892] OECD, *Guidelines*, *supra* note 11.

[1893] PIPEDA, *supra* note 63 at Schedule 1 (s. 5), principle 4.9; Quebec DPL, *supra* note 110 at s. 27; See also arts. 38, 40 C.c.Q.; Alberta DPL, *supra* note 114 at Part 3, Division 1, s. 24 (1.1), s. 25 (1) to (3); B.C. DPL, *supra* note 115 at Part 7, s. 23 (1) and s. 24 (1) (a), (b); *Loi informatique et liberté*, *supra* note 131 at c. V, s. 1, (II), art. 40; EC, *Directive 95/46/EC*, *supra* note 99 at art. 12 (b).

[1894] Article 29 Data Protection Working Party, *Opinion 4/2007*, *supra* note 100 at 6: "For information to be 'personal data', it is not necessary that it be true or proven. In fact, data protection rules already envisage the possibility that information is incorrect and provide for a right of the data subject to access that information and to challenge it through appropriate remedies."

[1895] According to Chris Hoofnagle, "accuracy allows for better business decisionmaking". See Hoofnagle & Smith, *supra* note 82 at 3.

[1896] See *Les travaux parlementaires*, 34th législature, 2nd session, Commission permanente de la culture, cahier no 32 (June 8, 1993), at 18-19.

harm at the use level is objective in nature,[1897] and that *harm* only emerges when the use of the personal information will exert a negative impact on the individual.[1898] Therefore, where there is a risk of exerting such a negative impact on an individual, the information in question should at least be accurate and up-to-date (the information should also be relevant, as discussed in section 3.2.2.3).

Early discussions leading to the creation of the data quality principle also seem to suggest that it has its place in the regulation of information use. For instance, the drafting of Resolution (73) 2 (leading to the adoption of Convention 108) took place at a time when there was a great deal of concern owing to the sharp rise in computers and electronic databases.[1899] Decisions could now be based on information stored electronically, which could easily not be up-to-date.[1900] To cite another example, emerging from the Lindop Report (U.K., 1978) was the sentiment that an individual should be able to see his or her data as soon as they were disclosed to a third party or used as the basis for an adverse decision against him or her.[1901] Moreover, the report also suggested that the objective of discarding outdated data clearly applies principally to "data used for making decisions which affect the data subject".[1902]

The data "accuracy" protection principle, which means that the data shall be "of quality" or accurate, is only relevant when evaluating the type of harm which will take place at the "use" level; for instance in the event that data is being "used" for a purpose or a decision which will have a negative impact on the individual.[1903] Although the quality of the data (whether the information is true or accurate) may be relevant in certain very specific cases, this criterion is much less important when evaluating the *risk of harm* to

---

[1897] See section 3.2.1 entitled "Objective Harm Resulting from the Use of Information (1960s-1970s Concerns)" which elaborates on this issue.

[1898] See section 3.2.2.1.1 entitled "Purpose behind Regulating the Use of Data: Negative Impact" which elaborates on this issue.

[1899] See Council of Europe, *Explanatory Report: Resolution (73) 22*, *supra* note 56 at para. 18.

[1900] See *ibid*.: "Computerised information can give a semblance of special reliability. Mistakes may cause serious damage, because of the intensive use that can be made of the data."

[1901] Lindop, *supra* note 96 at 49, para. 5.50.

[1902] *Ibid*. at 51, para. 5.61.

[1903] See section 3.2.2.1.1 entitled "Purpose behind Regulating the Use of Data: Negative Impact" which elaborates on this issue.

the individual that may arise upon "disclosure".[1904] For instance, the fact that one's sexual orientation is disclosed on the Internet may cause embarrassment (subjective harm) to this individual, whether or not this information is actually true. A picture "PhotoShopped" showing an individual naked, whether or not the body showed belongs to the individual in question, may nonetheless create the subjective harm discussed in section 3.1.2.1.1 (embarrassment) to the individual. Another example if with the U.S. case law *Paul v. Davis*,[1905] in which the police had distributed flyers with names and photographs to various stores erroneously listing the plaintiff as an active shoplifter. The plaintiff almost lost his job and was embarrassed and afraid to enter stores.[1906] The disclosure did cause subjective harm to the plaintiff in this case ("humiliation and embarrassment"), even if the data disclosed was not accurate. Solove, in his privacy taxonomy, discusses the harm of "disclosure" (of true facts) differently than the harm of "distortion" (disclosure of untrue facts), but still suggests that distortion results in some type of harm to individuals which is of similar nature.[1907]

At the "use" level, the fact that the information used is "accurate" will be an important element to consider in determining the *risk of harm*, together with whether the information used is "relevant" for the use intended.

I will first elaborate on the fact that the type of use made of the information and the risk of objective harm that it may trigger for the individual affected is directly linked with the

---

[1904] Whether the personal information disclosed is of "quality" is not necessarily important when evaluating the type of subjective which may be triggered by the disclosure of personal information in the sense that it is the disclosure of information which is of "intimate" nature which will be subject to the type of harm discussed under section 3.1.2.1.1 entitled "Harm Directly Linked to Disclosure: Subjective (and Psychological)" whether or not the information is true.

[1905] 424 U.S. 693 (1976).

[1906] Solove, "Privacy", *supra* note 1 at 1426.

[1907] Solove, "A taxonomy", *supra* note 339 at 547: "Why are these harms of inaccuracy understood as privacy injuries? Why does the law protect against these harms? Why should people have a right to be judged accurately? I refer to these harms as 'distortion.' Distortion is the manipulation of the way a person is perceived and judged by others, and involves the victim being inaccurately exposed to the public. I include distortion in the taxonomy of privacy because of its significant similarity to other privacy disruptions. Distortion, like disclosure, involves the spreading of information that affects the way society views a person. Both distortion and disclosure can result in embarrassment, humiliation, stigma, and reputational harm. They both involve the ability to control information about oneself and to have some limited dominion over the way one is viewed by society. Distortion differs from disclosure, however, because with distortion, the information revealed is false and misleading."

level of accuracy required. I will then discuss the criteria pertaining to the data which may impact positively or negatively on the accuracy of the data.

3.2.2.2.1. Degree of Accuracy Subject to Use

Section 3.2.2.2 already discusses how the data accuracy principle is directly linked with information "used" to make a decision which will have an impact on the individual.[1908] For example, PIPEDA provides that information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that "inappropriate information may be used to make a decision about the individual."[1909] Article 38 of the C.c.Q. states that any person may examine and cause the rectification of a file kept on him by another person "with a view to making a decision in his regard or to informing a third person."[1910] Under the B.C. DPL, an organization must make a reasonable effort to ensure that personal information is accurate and complete, "if the personal information is likely to be used by the organization to make a decision that affects the individual to whom the personal information relates."[1911] In line with the Directive 95/46/EC on the subject matter, the French DPL has a similar principle (accuracy is important when evaluating an individual), which provides that any individual is entitled to interrogate the data controller of his personal data in order to obtain information allowing him or her to know and to object to the logic involved in the automatic processing, "in the case of a decision taken based on automatic processing and producing legal effects in relation to the data subject".[1912]

(a) The Higher the Risk of Harm, the More important the Accuracy

Personal information which is accurate may not be deleted or amended at the request of an individual simply because it may be harmful for the individual.[1913] However, the

---

[1908] Also when the information is disclosed to parties which will "use" it.

[1909] PIPEDA, *supra* note 63 at Schedule 1 (s. 5), principle 4.6.1.

[1910] Art. 38 C.c.Q.

[1911] B.C. DPL, *supra* note 115 at Part 9, s. 33 (a).

[1912] *Loi informatique et liberté*, *supra* note 131 at c. V, s. 1, (II), art. 39 (5)**;** EC, *Directive 95/46/EC*, *supra* note 99 at art. 12 (a).

[1913] For example, in Quebec, although information contained in someone's credit report may cause him "harm", this is not a ground for rectification, when information is otherwise accurate. *X. v. Équifax Canada*,

extent to which personal information shall be accurate, complete, and up-to-date will depend upon the "use" made of the information and therefore, on the extent of the objective harm which this use may trigger.[1914] The more important this objective harm, the more crucial it is that the information used to make a decision be, in fact, accurate.[1915] On this issue, the FTC in its recent 2012 Report states that :

> "The preliminary staff report called on companies to take reasonable steps to ensure the accuracy of the data they collect and maintain, particularly if such data could cause significant harm or be used to deny consumers services." [1916]

The U.K. Information Commissioner recently published a data protection strategy which emphasizes the need to make judgments about the seriousness of the risks of individual harm due to inaccurate, insufficient or outdated information.[1917] Thus it is easy to understand that certain industries are being specifically targeted with the data "accuracy" principle since their use of information will more likely create a high risk of objective harm to individuals. For example, under the Quebec DPL, businesses involved in the lending of money have special and additional obligations.[1918] If the information is to be used in such a way that there will be little or no observable impact

---

[1995] C.A.I. 286; *Hallis v. Équifax Canada*, [1996] C.A.I. 107; *Ravinsky v. Équifax Canada*, [2003] C.A.I. 46 [*Ravinsky*].

[1914] This issue was already raised thirty years ago. See Lindop, *supra* note 96 at 269, para. 30.07: "All this can be done where computers are used for information handling. However, there are so many different kinds of personal information, and so many different purposes for which they can be used, that it would be foolish to attempt to lay down any rigid rules for all these cases. We do not therefore believe that any special provision needs to be written into the statute." See PIPEDA, *supra* note 63 at Schedule 1 (s. 5), principle 4.6.1: "The extent to which personal information shall be accurate, complete, and up-to-date will depend upon the use of the information, taking into account the interests of the individual. (…)"

[1915] As the risk of harm increases, so too must the need for accurate information. See Lindop, *supra* note 96 at 271-72, para. 31.09: "For much published information, therefore, caution will be necessary before it can safely be used in ways which may affect the data subject. To take just on extreme and unlikely example, the DPA might think it necessary to prescribe very high standards of compliance with the statutory principles for a system designed to collect only adverse information about UK residents – even if it was to be taken exclusively from sources published during the last 50 years – if the user's sole purpose was the sale of that information, at a profit, to those who wished to use it against the data subjects concerned."

[1916] FTC, *Recommendations* 2012, *supra* note 381 at 29 [footnotes omitted].

[1917] ICO, *Data Protection Strategy*, *supra* note 986 at 7: "The principal risk which our activities must address is the risk that individuals will suffer harm because personal information about them is: inaccurate, insufficient or out of date."

[1918] They must communicate to individuals, on request, the content of any credit report or recommendation consulted for the purpose of "making a decision concerning the person". See Quebec DPL, *supra* note 110 at s. 19.

for the individual (or a positive impact) then the level of accuracy is much less important.

Let us consider location information for instance. The degree of accuracy associated with this kind of information varies greatly and may depend on the location tracking technology used. Certain authors have even questioned whether location data should qualify as "accurate" data under DPLs.[1919] Location information may be used in a context where a high level of accuracy is not required. In the event that the location information used is not very accurate, but that it is used strictly to manage taxis (i.e. no impact on individuals) then this use may not be problematic from a privacy (or harm) standpoint. On the other hand, if the location information is used to evaluate the performance of employees (taxi drivers for example), then this information would have to be *more* accurate since it creates a concrete risk of objective harm (potentially being dismissed from their employment) for the individuals concerned.

Location information would have to be extremely accurate if it is to be used in a criminal investigation. The suspect would have to be identified with pinpoint accuracy, in order to avoid leaving open the possibility of false inferences regarding an individual who raises some suspicion.[1920] An illustration of inaccurate information used for a harmful purpose would be the mistaken detention of U.S. lawyer Brandon Mayfield, who was imprisoned for two weeks by the U.S. Federal Bureau of Investigation in June 2004 following a match between his fingerprints with those found in the Madrid terrorist bombing.[1921] Another example is *PIPEDA Case Summary #2002-53*,[1922] in which a bank was found liable for having disclosed inaccurate personal information to the

---

[1919] See Gratton, *Internet and Wireless Privacy*, *supra* note 193 at 297-98.

[1920] Bennett notes problems with the application of the general PIPEDA principles to location-based services, such as the degree of accuracy required of location-based services records, which are presently not able to exactly pinpoint an individual – leaving open the possibility of false inferences regarding an individual who simply passes near a 'sensitive' area. Bennett & Crowe, *supra* note 1574 at 36-37, discussed in Hariton, Lawford & Palihapitiya, *supra* note 197 at 30.

[1921] Henry Schuster & Terry Frieden, "Lawyer wrongly arrested in bombings: 'We lived in 1984'" (29 November 2006), online: CNN Justice <http://articles.cnn.com/2006-11-29/justice/mayfield.suit_1_train-bombings-brandon-mayfield-madrid?_s=PM:LAW>.

[1922] OPCC, *PIPEDA Case Summary #2002-53, Bank accused of providing police with surveillance photos of the wrong person* (28 June 2002) [OPCC, *PIPEDA Case Summary #2002-53*].

police about a woman.[1923] Two photographs of her taken from a surveillance videotape were later featured in a newspaper article mistakenly identifying her as a crime suspect.[1924] Since the information used was to have an extremely negative impact (objective harm) on the individual, then the degree of accuracy was, concurrently, extremely important.

"Accuracy" may sometimes translate into "completeness". Even highly accurate information could be misleading if taken out of context or left incomplete. For example, the fact that an individual was charged with a criminal offense would be inaccurate if it does not also mention that the individual was acquitted for the offense.[1925] Solove has raised his concerns with the fact that the compiling and using data about the so-called "digital person" is increasingly having an effect on the flesh-and-blood individual in real space. Since profiles are often "incomplete", this phenomenon is highly problematic:

> "Although making decisions based on aggregated data is efficient, it also creates problems. Data compilations are often both telling and incomplete. They reveal facets of our lives, but the data is often reductive and disconnected from the original context in which it was gathered. This leads to distortion."[1926]

Another interesting point was raised in the recent FTC 2012 Report: "Providing enhanced accuracy standards for marketing data would raise additional privacy and data security concerns, as additional information may need to be added to marketing databases to increase accuracy."[1927] Since the objective harm in connection with the practices of marketing may be viewed as being on the low side, it may not make any

---

[1923] In *PIPEDA Case Summary #2002-53*, the OPCC had to consider how accurate the information should have been, and how diligent the bank should have been about verifying the accuracy of the information before disclosing it to the police. The OPCC determined that since the purpose of the information disclosure was the solving of a crime, accuracy was crucial to the fulfilment of the purpose, and therefore the bank should have made sure that the information it disclosed was as accurate as possible.

[1924] Considering its failure to have done so, the OPCC found that the bank had been clearly in contravention of Principle 4.6 of PIPEDA (accuracy principle).

[1925] Lindop, *supra* note 96 at 47, para. 5.43.

[1926] Solove, "A taxonomy", *supra* note 339. See also Solove, *The Digital Person*, *supra* note 1753 at 1-10, 507.

[1927] FTC, *Recommendations* 2012, *supra* note 381 at 29 [footnotes omitted]. See also Comment of Experian, cmt. #00398, at 11 (arguing against enhanced standards for accuracy, access, and correction for marketing data); see also Comment of Yahoo! Inc., cmt. #00444, at 6-7. Cf. Comment of Yahoo! Inc, cmt. #00444, at 7 (arguing that it would be costly, time consuming, and contrary to privacy objectives to verify the accuracy of user registration information such as gender, age or hometown).

sense to impose an accuracy obligation to these marketers. The FTC rightfully recommended that organizations using data for marketing purposes need not take special measures to ensure the accuracy of the information they maintain but that using data to make decisions about consumers' eligibility for benefits should take much more robust measures to ensure accuracy.[1928]

The risk of objective harm resulting from the intended use of information needs to be assessed and the degree of accuracy of the information must be consistent with this risk. The extent of the responsibility that this entails for the organization is discussed next.

(b) Responsibility of Organization to Ensure Accuracy

Some contributors to the Lindop Report (U.K. 1978) went as far as to claim that organizations should be legally responsible for accuracy, and that good faith should not be a defence for inaccuracy if the data had either not been checked by the individual concerned, or had been used without the individual's knowledge.[1929] Others took a different position, one under which an organization could not be held responsible if the individual concerned, or a third party, had deliberately or inadvertently supplied inaccurate information and that the organization's responsibility should, therefore, be limited to ensuring that the data received were correctly recorded and that the supplier of the data was reliable.[1930]

Organizations usually have the obligation to ensure that the information that they "use" is accurate, based on the information that they already have on hand and based on

---

[1928] FTC, *Recommendations* 2012, *supra* note 381 at 30 [footnotes omitted]: "The Commission agrees that the best approach to improving the accuracy of the consumer data companies collect and maintain is a flexible one, scaled to the intended use and sensitivity of the information. Thus, for example, companies using data for marketing purposes need not take special measures to ensure the accuracy of the information they maintain. Companies using data to make decisions about consumers' eligibility for benefits should take much more robust measures to ensure accuracy, including allowing consumers access to the data and the opportunity to correct erroneous information."

[1929] Lindop, *supra* note 96 at 46, para. 5.38: "This objective was accepted by some of our witnesses. Esso, for instance, pointed out that accuracy was in the interest of the user as well as that of the data subject. The British Psychological Society went so far as to say that the user should be legally responsible for accuracy, and that good faith should not be a defence for inaccuracy if the data had not been checked by the subject or had been used without his knowledge."

[1930] *Ibid*. at 46, para. 5.39.

what is reasonable.[1931] In *PIPEDA Case Summary #2005-295*,[1932] a satellite equipment seller who had debited the ex owner of a business' personal bank account was found to have contravened the "data quality" obligations as dictated by the OPCC. On two occasions, the new owner of the complainant's former business had contacted the company and therefore, the customer service representative should have seized the opportunity (when the new owner indicated that he did not know about the preauthorized plan) to confirm the preauthorized debit information.

There are examples of "data accuracy" breaches in Canada. In *PIPEDA Case Summary #2007-381*,[1933] the OPCC concluded that a bank ought to have noticed that the information provided by a fraudster who opened a store credit card account was inaccurate (year of birth provided), and therefore was at fault for consequently transferring the information of the inaccurate debt (incurred by the fraudster) to a collection agency. In *PIPEDA Case Summary #2005-299*,[1934] a bank, which had already been advised that a customer's mail had been stolen (which contained convenience cheques), was at fault for authorizing a third party to fraudulently cash a cheque in his customer's name since this would not have happened should there have been accurate information in the account (i.e. the fact that the mail which contained convenience cheques was stolen). In *PIPEDA Case Summary #2006-344*,[1935] a bank branch was found at fault when it opened a safety deposit box in error, as this was caused by the fact that information mentioned on a customer's signature card it held was inaccurate. In *PIPEDA Case Summary #2004-275*,[1936] a bank was at fault for

---

[1931] For example, in Quebec, the Quebec DPL provides that individuals are granted with the right to access their file held by an organization and to ask for its rectification when the information contained is inaccurate, incomplete or equivocal, through the C.c.Q. When a rectification is requested, the burden lies on the organization to prove that the information is accurate, complete and unequivocal, unless the information was communicated directly by the individual concerned or with his or her consent. Arts. 38, 40 C.c.Q.; Quebec DPL, *supra* note 110 at ss. 27, 28, 53.

[1932] OPCC, *PIPEDA Case Summary #2005-295, Customer concerned about mysterious debits from bank account* (14 March 2005).

[1933] OPCC, *PIPEDA Case Summary #2007-381, Bank improves safeguards after individiual's personal information used fraudulently to open credit card account* (15 March 2007).

[1934] OPCC, *PIPEDA Case Summary #2005-299, Thief cashes convenience cheque on cancelled credit card account* (31 March 2005).

[1935] OPCC, *PIPEDA Case Summary #2006-344, Couple's safety box opened in error* (17 July 2006).

[1936] OPCC, *PIPEDA Case Summary #2004-275, A bank provides inaccurate information to credit agencies* (24 August 2004) [OPCC, *PIPEDA Case Summary #2004-275*].

cancelling an individual's credit card with the consequence that a credit agency reports showed a debt owing for this amount indicating "bad debt", when the payment in connection with the debt had already been paid by cheque (which the bank had cashed). In *PIPEDA Case Summary #2009-012*,[1937] after a fraudster used forged identification of an individual to open a bank account, the bank was held not to be acting in breach of PIPEDA since it had followed the requirements for personal information collection when opening new customer accounts, as stipulated by the *Bank Act*.

In France, the CNIL has taken the position that an organization which did not update its marketing database containing individuals' contact information intended to be used for telemarketing purposes, acted in breach of the French DPL's accuracy obligation.[1938] The CNIL has also taken the position that the registration by an organization at a national database detailing the defaults of individuals with regards to the payment of loans or debts (the fichier FICP)[1939] of an incident which took place in 1988 was illegal when made in 2004 (sixteen years after the incident) as it was at that point no longer "accurate" information.[1940]

Certain organizations (such as credit agencies, schools, etc.) that are in the business of rating individuals and disclosing the information, need to take extra precautions as the information disclosed could result in significant harm to data subjects if it were to fall in the hands of third parties. In the event that the information used by an organization is subjective, it may be more difficult to determine at what point that information will qualify as being accurate. This issue is discussed next.

[1937] OPCC, *PIPEDA Case Summary #2009-012: Bank not responsible after new account was opened using stolen identity* (24 August 2009).

[1938] Délibération n°2008-470 du 27 novembre 2008 de la formation restreinte prononçant une sanction pécuniaire à l'encontre de la société ISOTHERM.

[1939] Fichier national des Incidents de remboursement des Crédits aux particuliers (FICP)

[1940] *Délibération n°2006-245 du 23 novembre 2006 prononçant une sanction pécuniaire à l'encontre de la Caisse régionale de crédit agricole mutuel de centre France* [*Délibération n°2006-245*].

(c) Subjective vs. Objective Information

The Article 29 Working Party suggests that personal data includes information regarding private and family life, preferred types of activity, working relations or the economic or social behaviour of the individual.[1941] Personal information would therefore include information about individuals, regardless of their position or capacity (as consumer, patient, employee, customer, etc.) and it would include "objective" information (such as a person's name, address, etc.) as well as more "subjective" information (such as an opinion about this person's health, work assessment, psychological evaluation, etc.).[1942]

With regards to the information being accurate, it is usually more difficult to correct "subjective" information, because the accuracy of subjective information is itself assessed subjectively. Under the Quebec DPL, requests for modifications made by individuals may be refused by the organization if the information that the individual wants deleted or modified represents a subjective opinion.[1943] When the information is a subjective opinion (ex: a doctor's report stating that "this individual is depressed"), the individual's only right is to deposit his or her personal comments in the file (i.e. "I do not think that I am depressed") in accordance with article 40 of the C.c.Q.[1944]

In the Report of Finding pertaining to a complaint made under PIPEDA against the U.S. company Accusearch Inc. (doing business as "Abika.com")[1945] a complainant alleged that Abika.com was compiling and disclosing inaccurate personal information through

---

[1941] Article 29 Data Protection Working Party, *Opinion 4/2007*, *supra* note 100 at 6-7.

[1942] See for example *ibid*. at 6: "From the point of view of the nature of the information, the concept of personal data includes any sort of statements about a person. It covers 'objective' information, such as the presence of a certain substance in one's blood. It also includes 'subjective' information, opinions or assessments."

[1943] *S.R. c. Côté*, [2009] C.A.I. 172; *M. C. c. Champoux*, [2008] C.A.I. 587; *M. B. c. Anapharm inc*., [2006] C.A.I. 484; *Bilodeau c. Dr Benoit Goulet*, [2004] C.A.I. 366; *Chamberlain c. Association québécoise d'aide aux personnes souffrant d'anorexie nerveuse et de boulimie*, [2003] C.A.I. 544; *Ravinsky*, *supra* note 1913; *Benoit c. Dr Maurice Leduc*, [1995] C.A.I. 270. The same principle applies under the Quebec public sector DPL. See *J.B. c. Commission de la santé et de la sécurité du travail,* [2009] C.A.I. 43 ; *M.C. c. Champoux,* [2008] C.A.I. 230.

[1944] Art. 40 C.c.Q.

[1945] OPCC, *Report of Findings, Complaint under PIPEDA against Accusearch Inc., doing business as Abika.com* (31 July 2009) [OPCC, *Accusearch*].

its "psychological profile" service.[1946] The OPCC took the position that the complaint relating to "accuracy" was not well-founded since it contained subjective facts and therefore, facts which were not verifiable:

> "I am of the view that Principle 4.6 was intended primarily to address matters of objective, verifiable fact. The positions of the respondent and the original complainant in this regard are rather matters of differing opinion, unverified and practically unverifiable in the circumstances. I consider many of the statements in the psychological profile at issue to be highly questionable, and I would not be at all surprised if the profile proved to be partly or largely inaccurate or even fabricated. (…) Despite my suspicions, and despite my disapproval of the company's non-consensual collections, uses, and disclosures of personal information, I have no objective factual basis upon which to find that Abika has compiled and disclosed inaccurate information about the original complainant." [1947]

This case simply illustrates the kind of challenges that one may have with regards to consumer profiles. In France, the Paris Appeal Court took the position that the personal information of teachers and notations collected by the French website Note2be.com were illegal, in part because there was no warranty as to their "accuracy".[1948] Consequently, organizations should be extremely cautious before making decisions based on subjective information found online, if this information may trigger an objective harm for the individual. For instance, many websites allow individuals or customers to "rate" professionals such as doctors[1949] or teachers.[1950] Schools and hospitals should not base their decisions to employ a teacher, or a doctor based on information found online on these sites; without taking reasonable measures to verify the accuracy of the information.[1951]

[1946] As the basis for her complaint, the original complainant provided the OPCC with a copy of a psychological profile of herself that she had requested and obtained from Abika for a fee of $100 which, according to the complainant, was "laughably inaccurate in a number of respects, and often bore no similarity to the person being searched".

[1947] OPCC, *Accusearch*, *supra* note 1945.

[1948] CA Paris, RG 08/04727, *supra* note 413.

[1949] See online : <http://www.ratemymd.com>; <http://www.ratemymd.ca>.

[1950] See online : <http://www.ratemyteachers.com>; <http://www.ratemyprofessors.com>; <http://www.note2be.com/>.

[1951] This could include, for instance, allowing the professionals to comment the notations or ratings received, etc.

3.2.2.2.2. Origin of Data

In certain situations, more information can mean more accurate information, which can then be used to provide services. With more and more personal information being made publicly available, some organizations may also be using this data to increase the value or accuracy of the data that they already hold. Some organizations, such as ChoicePoint, base their business model on the aggregation and selling of personal information by acquiring information from public records.[1952] This means that the more information they collect, the more accurate it is likely to be. At the same time, I maintain that one of the most important criteria, useful in assessing whether the information used is accurate, has to do with the origin of the data; this will often have a direct impact on the quality of the information.

(a) Individual Provided the Information for the Purpose (Highest Quality)

The fact that an individual provided his or her personal information for a specific purpose may usually imply that this information is of high "quality". As a matter of fact, the Lindop Report (U.K., 1978) already discussed the fact that information supplied by third parties (instead of by individuals themselves) tends to be less accurate:

> "As a general rule, information about a data subject supplied by others will tend to be less reliable than that which he supplies himself. Such information will tend to reflect, at least in part, the perceptions of the informant, which may not themselves be known to the collector of the information; it may be deliberately distorted by the informant, again without the knowledge of the collector; and it may very easily be incomplete, since often it will be the data subject alone who knows the full story."[1953]

Therefore, it is not hard to understand why certain DPLs favour collection of personal information *directly* from individuals.[1954] Other DPLs provide certain additional

---

[1952] Lo, *supra* note 188 at 52.

[1953] Lindop, *supra* note 96 at 268, para. 30.02.

[1954] See section 3.1.1.2.1(a) entitled "Knowledge and Transparency" which elaborates on this issue. See also for example section 6 of the Quebec DPL, which requires that personal information be collected from the person concerned, unless the latter consents to collection from third persons or an exception is applicable.

obligations in cases where the information will be supplied by third parties.[1955] The Lindop Report even suggested that information be verified by the individual before being "used" for any purpose likely to affect the individual.[1956] This Report also discussed the fact that there will always be certain situations in which information provided by third parties will tend to be more accurate than if provided by individuals,[1957] as discussed below.

(b) Information Provided by Third Party (Medium Quality)

Perhaps because personal information provided by third parties will generally tend to be less accurate, many DPLs have a requirement that organizations that disclose personal information to third parties ensure that this information be accurate. For instance, PIPEDA provides that "personal information (….) disclosed to third parties, should generally be accurate and up-to-date (…)."[1958] The B.C. DPL provides that:

> "an organization must make a reasonable effort to ensure that personal information collected by or on behalf of the organization is accurate and complete, if the personal information (…) is likely to be disclosed by the organization to another organization."[1959]

The purpose of this requirement has to do with ensuring that information is accurate when disclosed since it may be "used" by these other organizations. Section 24 (2) of the B.C. DPL states that once information is corrected by an organization, it shall "send the corrected personal information to each organization to which the personal information was disclosed by the organization during the year before the date the

---

[1955] See section 3.2.2.2.2(b) entitled "Information Provided by Third Party (Medium Quality)" which elaborates on this issue.

[1956] Lindop, *supra* note 96 at 269, para. 30.05: "Accordingly, we believe that such information should, in general, not be used for any purpose likely to affect the data subject unless it has been verified by him, or corroborated by other information from some independent source. This is, of course, one of the arguments for 'subject access' to information." See also *ibid*. at 47, para. 5.40 and at 268, para. 30.04.

[1957] *Ibid*. at 268, para. 30.03: "On the other hand, there will also be some cases where 'third party information' will be more reliable than any that the data subject can himself supply. One obvious example is the clinical observations and diagnosis of a physician, which are more likely to be right than those of the patient; another is the balance shown on a bank statement, which is more likely to be correct than that calculated by the customer from his own records."

[1958] PIPEDA, *supra* note 63 at Schedule 1 (s. 5), principle 4.6.3.

[1959] B.C. DPL, *supra* note 115 at Part 9, s. 33 (b).

correction was made." [1960] Under article 40 of the C.c.Q., a notice of the rectification shall be given without delay to every person having received the information "in the preceding six months" and, where applicable, to the person who provided that information.[1961] The Lindop Report (U.K. 1978) suggested that when information is provided by third parties, there should be a note indicating it, so that organizations wishing to use it will be aware of the potential lack of accuracy.[1962]

As discussed above, in Quebec, section 6 of the Quebec DPL requires that personal information be collected from the person concerned, unless the latter consents to collection from third parties (or an exception applies). There are cases where additional information could be sought from third parties. Except where exceptions apply, the person concerned must be informed and consent must be obtained.[1963] The process of obtaining personal information from a third party is a double-edged sword. Not only does the organization seeking to obtain the information have to make sure that it is authorized to get the information from the third party, but the third party must also make sure that it is authorized to communicate the information to the receiving party.[1964] The exceptions that allow for the collection of personal information from third parties must be interpreted restrictively.[1965] For example, the CAI took the position that when conducting an inquiry on an insurance claim, insurance companies may collect information from the third party in order to ensure the accuracy of the information.[1966] In credit reference situations, a financial institution may also contact third parties such as credit offices to check the accuracy of information in certain situations (such as trying to locate a client).[1967] In France, I have already discussed the fact that the Paris Appeal

---

[1960] *Ibid*. at Part 7, s. 24 (2) (a), (b).

[1961] Art. 40 C.c.Q.

[1962] Lindop, *supra* note 96 at 269, para. 30.06.

[1963] See Quebec case law on this issue: *X. v. Agence de recouvrement Réjean Aubé*, A.I.E. 96AC-75 (Inquiry Report).

[1964] In Quebec, generally, before communicating such information, the third party must be authorized under sections 13, 14 and 15 of the Quebec DPL, as confirmed by certain case law on the subject matter. See *X. v. Services aux marchands détaillants ltée*, A.I.E. 96AC-101 (Inquiry Report) ; *X. v. Banque nationale du Canada*, A.I.E. 96AC-103 (Inquiry Report).

[1965] *X. and Banque Royale du Canada*, A.I.E. 95AC-72 (Inquiry Report).

[1966] *Duchesne v. Great-West (La), compagnie d'assurance-vie*, [1995] C.A.I. 493.

[1967] *Tremblay v. Caisse populaire Desjardins de St-Thomas*, [2000] C.A.I. 154 [*Tremblay*].

Court took the position that the personal information of teachers and notations collected by the French website Note2be.com were illegal, in part because there was no warranty as to their "accuracy" (this information being provided by third parties and not the teachers themselves).[1968]

Certain organizations will logically be the ones making the personal information available. As discussed previously, in such cases, they are the ones that need to ensure the accuracy of data. Third parties will specifically rely on this information in order to take decisions which may ultimately be harmful for individuals; as illustrated by Nissenbaum with the example of schools rating students:

> "Consider teachers in the setting of primary and secondary education in the United States—they collect and aggregate information about students in order to assign grades. Over time, these grades are further aggregated to yield grade point averages and are combined with other information to form a student dossier, which, in some form, may be submitted to colleges or employers to which students have applied for admission or employment. A school might be judged remiss if it failed to notice that the performance of particular students had changed significantly in one way or another, if it failed to "mine" its data for other categories of change that reflected on students' and the school's performance."[1969]

Organizations such as credit agencies are in the business of disclosing financial information that is then used by third parties to make significant decisions which may be harmful to individuals (grant credit, a loan, etc.). Therefore, such organizations have to ensure that the information disclosed is accurate. For example, in *Nammo v. Transunion of Canada Inc.,*[1970] the federal court (Canada) awarded damages to the plaintiff which had lost a business opportunity because he was denied a loan (objective harm), a decision based on an inaccurate credit report provided by credit agency Transunion. In the case of *Boulerice* v. *Acrofax inc.*,[1971] the Quebec court took the position that a credit bureau was at fault for not maintaining up to date and accurate information about the plaintiff, although the plaintiff had made numerous demands to

---

[1968] CA Paris, RG 08/04727, *supra* note 413.

[1969] Nissenbaum, *supra* note 230 at 154-55.

[1970] *Nammo*, *supra* note 1084.

[1971] *Boulerice c. Acrofax inc.*, [2001] R.L. 621 (C.Q.).

rectify his file, since a credit bureau is a party usually providing third parties with information which third parties will rely on.[1972]

The OPCC has also rendered decisions in which it confirms the fact that in situations in which an organization is disclosing information to a third party, knowing that the third party will use it to take a decision that may have a negative impact (objective harm) for the individual concerned, this disclosing organization has to ensure that the information disclosed is in fact accurate.[1973] In France, as I have already discussed, the CNIL has taken the position that the registration by an organization at a national database detailing the defaults of individuals with regards to the payment of loans or debts (the fichier FICP)[1974] of an incident which took place in 1988 was illegal when made in 2004 (sixteen years after the incident) as it was at that point inaccurate (outdated) information.[1975]

(c) Information Widely Available (Medium to Low Quality)

In the 1970s, the Lindop Report warned of the possible inaccuracy and incompleteness of published data; notably due to data storage issues (while "published" data may be very accurate, it may also be potentially incomplete because of pressures of space).[1976] The concerns are different nowadays as the Internet has practically eliminated the storage problems. With web 2.0, there is a lot of information in circulation which may be inaccurate or incomplete which is "published" or at least made available for anyone to see. The accuracy of online information will often be dependent on the source. For example, information found in an article of an online newspaper is likely more accurate than information found on a blog or an OSN. While a lot of information is now available online (such as in OSNs), the information available may be incomplete and should not be taken out of context. In Quebec, the case of Nathalie Blanchard is worthy of consideration. Blanchard was on disability leave from her job because she was

---

[1972] The court awarded $800 in general damages and $1,500 in punitive damages.

[1973] OPCC, *PIPEDA Case Summary #2004-275*, *supra* note 1936; OPCC, *PIPEDA Case Summary #2002-53*, *supra* note 1922.

[1974] Fichier national des Incidents de remboursement des Crédits aux particuliers (FICP).

[1975] *Délibération n°2006-245*, *supra* note 1940.

[1976] Lindop, *supra* note 96 at 271, para. 31.08.

suffering from depression. Once her employer and insurer found online pictures of her having a good time on a sunny vacation, her disability benefits were promptly terminated.[1977] She claimed that these pictures were taken out of context and argued that the insurer's decision should not have been based on this inaccurate or incomplete information.[1978]

Research commissioned by Microsoft in December 2009 found that 79 percent of United States hiring managers and job recruiters reviewed online information about job applicants and most of those surveyed consider what they find online to impact their selection criteria.[1979] In fact, 70 percent of United States hiring managers in the study said that they had rejected candidates based on what they found online. Another recent survey completed by Ponemon Institute discovered that 35 percent of hiring managers perform online background checks and 23 percent research job candidates on OSN sites; one third of whom are eventually rejected.[1980] A potential employer may wish to access applicants' credentials on websites such as LinkedIn or Facebook. If the data found online is relevant for the purpose of assessing the applicant's suitability for the job,[1981] it may be used only if employers have taken reasonable measures to ensure that the information is accurate and up-to-date. If the information found online is

---

[1977] CBC News, "Depressed woman loses benefits over Facebook photos" (21 November 2009), online: CBC News <http://www.cbc.ca/news/canada/montreal/story/2009/11/19/quebec-facebook-sick-leave-benefits.html>.

[1978] An out of court settlement took place between the Nathalie Blamnchard and her employee IBM in January 2012. See Pascal Faucher, "Facebook : IBM règle son litige avec une employée" *Cyberpresse* (10 January 2012), online : Cyberpresse <http://technaute.cyberpresse.ca/nouvelles/internet/201201/10/01-4484477-facebook-ibm-regle-son-litige-avec-une-employee.php>.

[1979] Lyle Hanna, "Reputations Online, One in seven central Kentucky employers use social networking sites to screen candidates" (15 April 2010), online: Lex Weekly <http://www.lexweekly.com/Articles-c-2010-04-15-92201.113117_Reputations_Online.html>. See also the 2009 study which showed that 45 percent of employers surveyed used OSNs to evaluate potential employees. *See* Jenna Wortham, "More Employers Use Social Networks to Check Out Applicants", *The New York Times* (20 August 2009). A more recent study commissioned by Microsoft found that 70 percent of human resource professionals surveyed have turned down a potential job application based solely on online reputation information. See CrossTab, Inc., *Online Reputation in a Connected World* (Jan. 2010) [CrossTab, *Online Reputation*].

[1980] Hanna, *supra* note 1979.

[1981] See section 3.2.2.3 which elaborates on this "relevancy" criteria.

subjective, employers should allow the individual to explain or give his or her version of the facts.[1982]

As already discussed in section 3.1.2.2.3(b)(i), the CNIL recently announced that it had found *Pages Jaunes* guilty of violating several provisions of the French DPL, including its "accuracy" obligations.[1983] At issue was *Pages Jaunes'* web crawler function (which has since been discontinued). The web crawler captured information contained in Facebook, Twitter and LinkedIn profiles and would also display information from social media sites relating to name of the individual searches.[1984] Aside from the lack of consent issue, the CNIL found that *Pages Jaunes* had breached its obligation to use only accurate and updated data. The profile data that was presented by *Pages Jaunes* were, in many cases, outdated by four to twelve months. The risk of objective harm in this case was, as far as I am concerned, on the low side since Pages Jaunes was not using the information but instead potentially disclosing data already available.[1985] Therefore it is my opinion that *Pages Jaunes* should not have been found to be in breach of its accuracy obligations.

(d) Information Provided for a Different Purpose (Low Quality)

When personal information is used for a purpose other than that which it was collected for, this can be problematic. For instance, Solove suggests that secondary use creates problems; when removed from the original context in which it was collected, "data can more readily be misunderstood".[1986] This is especially true with online information which can be misinterpreted triggering the situation in which inaccurate information

---

[1982] Similar to the kind of rights which individuals have in Quebec under article 40 of the C.c.Q. when files about them contain subjective information. They can't modify the information but at least, they can include their personal comments in the file. See section 3.2.2.2.1(c) which elaborates on this issue.

[1983] The CNIL did not fine *Pages Jaunes*, but published a detailed warning, listing each privacy violation that the CNIL had identified during its investigation of *Pages Jaunes's* activities. See CNIL, "Carton rouge", *supra* note 1636.

[1984] The information may include photos, the name of employer, the schools attended, the individuals' geographic location, profession, etc.

[1985] Pages Jaunes was making data already available potentially more easily available, and therefore, this activity was more of a "disclosure" activity than a "use". See section 3.1.2.2 entitled "Risk of Subjective Harm: Revisiting the Sensitivity Criteria" which elaborates on the risk of subjective harm that may take place in these situations. The test to use in determining whether the information qualified as *personal information* was therefore whether there is a risk of subjective harm (instead of objective harm).

[1986] Solove, "A taxonomy", *supra* note 339 at 520.

may be used by organizations in decisions that negatively impact individuals (therefore triggering an objective harm).

In an interview with BBC News, a PIAC representative illustrated a scenario in which an insurance company could raise a client's premiums by 5% upon discovering that this individual had researched a particular type of cancer online.[1987] This kind of assumption could trigger a use of inaccurate information. According to Wong, for instance, there is a flaw with this assumption, as it is not always possible to draw an inference of an individual's interest or situation based on the mere fact that he or she has visited a particular website or has researched certain information.[1988]

The Article 29 Working Party has warned that profile data collected for behavioural advertising could potentially be used for purposes other than advertising, such as the development of new services whose nature is as yet undecided.[1989] The Article 29 Working Party suggests that if ad network providers want to use information gathered for behavioural advertisement for secondary purposes, they need additional legal grounds, such as obtaining consent of the individuals affected.[1990] Philippa Lawson summarizes the concerns regarding accuracy and transparency of consumer profiles, in the context of profile information being "used" when taking various decisions which will have an impact on individuals:

> "Research also suggests that the information in consumer profiles is often riddled with errors. Yet important decisions are made on the basis of this information by employers, insurance companies, governments and others. Such decision [*sic*] are made without the individual's knowledge and thus without any opportunity for them to explain, to

---

[1987] PIAC, *supra* note 448 at 8: "It is relatively incontestable that information on an individual's medical conditions is sensitive and that such information may be used against the individual, not to mention that the mere existence of the internet activity mentioned above may lead to erroneous conclusions by the insurance company (the individual may have been researching his/her friend's condition or performing research for any other number of reasons)."

[1988] Wong & Garrie, *supra* note 187 at 581.

[1989] However, they maintain that this new use would be conditioned to the compliance of Article 6(1)(b) setting forth the "purpose limitation principle", which prohibits the processing of personal data which is not compatible with the purposes that legitimized the initial collection. In other words, incompatible secondary uses of the information collected and stored for behavioural advertising would contradict art 6(b) of EC, *Directive 95/46/EC*, *supra* note 99. See Article 29 Data Protection Working Party, *Opinion 2/*2010, *supra* note 191 at 20.

[1990] *Ibid*. at 21.

> correct inaccurate information, or to expose decision-making based on prejudice or misinterpretation."[1991]

I maintain that in order to determine if a secondary use is harmful, the test should first be whether this new use creates an impact for the individual and if so, whether this impact is negative (i.e. objective harm) for the individual in question. Only in such cases should the data used have to qualify under the "accuracy" criterion.

3.2.2.2.3. Type of Technology Used or Analysis Made (Computer vs. Human)

In certain instances, the quality of data will depend on the technology used to collect the data. For instance, this is the situation with location information, which may be collected using different technologies, which each may impact on the accuracy of the data collected.[1992]

Part of the assessment in evaluating whether information used is of "accuracy" has to do with who is doing the processing and analyzing or evaluating the information at stake. The Lindop Report (U.K., 1978), already raised its concern in having computer evaluate information, making judgment calls and coding value judgments:

> "Second, we received a number of submissions on the principle that "care should be taken in coding value judgments". (…) Our witnesses pointed out to us other kinds of data about which special care needs to be taken; for instance, when dealing not only with value judgments but also with other subjective or unverifiable data. Such data were said to require special care because they are by their nature less reliable, because they are liable to be misinterpreted by a third party, and because they often contain serious or damaging implications for the data subject. (…) Our evidence showed that it is still unusual for computers to be used for other than purely factual data, but there is no doubt that there are a number of fields (e.g. medicine, criminal intelligence, consumer credit and personnel management) where the

---

[1991] Philippa Lawson, "Techniques of Consumer Surveillance and Approaches to their Regulation in Canada and the USA" (March 2005) at 7, online: <http://www.idtrail.org/index2.php?option=com_content&do_pdf=1&id=110>. Lawson cites the testimony of Marc Rotenberg, President, EPIC, before a committee of the USA House of Representatives, in a hearing on "Protecting Consumer's Data: Policy Issues Raised by ChoicePoint" (15 March 2005) at 2-3, online: <http://www.epic.org/privacy/choicepoint/testimony3.15.05.pdf>.

[1992] Gratton, *Internet and Wireless Privacy*, *supra* note 193 at 29-32.

> handling of subjective or evaluative data is beginning to be carried on automatically, and that this trend will probably continue.(…)"[1993]

According to this Lindop Report, the coding of subjective judgments often entails the loss of shades of meaning and emphasis: "For example, a numeral indicating "fair" in evaluating an employee's performance is capable of wide interpretation. In such cases it would be preferable to refer the interrogator of the computer to a more detailed report."[1994] It was suggested that the data be divided into three categories: fact, unverified factual assertion, and subjective judgment (or assessment or opinion). Where appropriate, the author of unverified or subjective data should not be computerized at all, because the computer gave such data a spurious authenticity.[1995]

H. Jeff Smith articulates the view that decisions that were formerly based on judgment and human factors are instead often decided according to prescribed formulas and that in today's world, this response is often characterized by the reliance on a rigid, unyielding process in which computerized information is given great weight.[1996] He maintains that facts that actually require substantial evaluation could instead be reduced to discrete entries in preassigned categories. Danièle Bourcier, in an article entitled "L'acte de juger est-il modélisable? De la logique à la justice", discusses the types of challenges that poses the use of automatic processing for taking decisions which may be impactful for individuals.[1997] She also elaborates in another article on the fact that individuals should be informed of the reasoning behind a decision affecting them in order to be in a position to challenge the decision.[1998] Solove has warned that

---

[1993] Lindop, *supra* note 96 at 47-48, para. 5.44.

[1994] *Report of the Committee on Privacy*, *supra* note 3 at 184, para. 600.

[1995] Lindop, *supra* note 96 at 47-48, para. 5.44.

[1996] H. Jeff Smith, *Managing privacy: information technology and corporate America* (Chapel Hill: University of North Carolina Press, 1994) discussed in Solove, "A taxonomy", *supra* note 339 at 508.

[1997] Danièle Bourcier, "L'acte de juger est-il modélisable? De la logique à la justice" (2011) 54 Arch. phil. Droit 37.

[1998] Danièle Bourcier, "Données sensibles et risque informatique: de l'intimité menacée à l'identité virtuelle", CURAPP – Questions sensibles, PUF (1998) at 51-53.

similar concerns can arise even with more objective information, since information in databases often fails to capture the texture of our lives.[1999]

Others raise the fact that computers analyzing great amounts of data for criminal purposes may end up identifying and flagging the wrong individuals as "criminals".[2000] For instance, government agencies may be using powerful data mining methods to trace networks of targets like criminals and terrorists, but the danger is that they may mistake good guys for bad guys.

Calo refers to Danielle Keats Citron's work in which the author identifies a series of instances where machines have used information in surprising ways, with very troubling consequences. For instance, consider the possibility that an airline traveler could be added to a "No Fly List" due to faulty data matching techniques.[2001] Calo goes on to argue that "human beings" need not physically review personal information for that information to form the basis of an adverse action:

> "There does not have to be a human observer who gathers and misuses information. Machines are perfectly competent to comb through private information and use it to make automatic decisions that affect us in tangible and negative ways. (…) In the past, computer systems helped humans apply rules to individual cases. Now, automated systems have become the primary decision makers. These systems often take human decision making out of the process of terminating individuals' Medicaid, food stamp, and other welfare benefits. (…) Computer programs identify parents believed to owe child support and instruct state agencies to file collection proceedings against those individuals. Voters are purged from

[1999] Solove, "Privacy", *supra* note 1 at 1425-26*:* "(…). Rather than provide a nuanced portrait of our personalities, they capture the stereotypes and the brute facts of what we do without the reasons. For example, a record of an arrest without the story or reason is misleading. The arrest could have been for civil disobedience in the 1960s—but it is still recorded as an arrest with some vague label, such as disorderly conduct, slapped onto it. It appears no differently from the arrest of a vandal. In short, we are reconstituted in databases as a digital persona composed of data. The privacy problem stems paradoxically from the pervasiveness of this data—the fact that it encompasses much of our lives—as well as from its limitations— how it fails to capture us, how it distorts who we are."

[2000] Maclean, *supra* note 154; See for example, Schuster & Frieden, *supra* note 1921.

[2001] Calo, "The Boundaries", *supra* note 443 at 25-26: "We do not know the exact source of the information these systems rely upon, but there is every indication that it includes personal information not supplied by citizens for this purpose."

> the rolls without notice, and small business are deemed ineligible for federal contracts."[2002]

Another issue is that the type of individual or organization providing the data will be relevant in assessing its quality. An expert in his or her field is not the same as a random individual and this will often have an impact on the quality of the data.[2003] Out of the parliamentary debates that took place before the adoption of the Quebec DPL in 1993, came the idea that data used needed to be of "quality" and must be evaluated by competent people.[2004]

The French DPL (in line with the relevant Directive 95/46/EC) contains a legal mechanism that empowers people to defend themselves when their interests are affected as a result of automatic data processing.[2005] Furthermore, the French DPL also stipulates that no decision having a legal effect on an individual may be taken solely on the grounds of automatic processing of data (also in line with the Directive 95/46/EC).[2006] These types of provisions were clearly meant to ensure that when personal information may be used in assessments or decisions that may have a negative impact on the individuals concerned, the data shall be accurate. These provisions illustrate a contemporary concern, shared by many, that information used may not be accurate if analyzed by automatic processing and computers.

3.2.2.3. Relevancy of Information Used

I maintain that once we have established that the information will be used in a such a way as to trigger an objective harm on the individual concerned, then the information should be regulated by DPLs. Therefore, we need to ensure that the information used is "accurate" (section 3.2.2.2 details this "data quality" criteria) and also that the

---

[2002] Danielle Keats Citron, "Technological Due Process" (2008) 85 Wash. U. L. Rev. 1249 at 1252, discussed in Calo, "The Boundaries", *supra* note 443 at 24.

[2003] Lindop, *supra* note 96 at 269, para. 30.08.

[2004] See *Les travaux parlementaires*, 34th législature, 2nd session, Commission permanente de la culture, cahier no 13 (March 1,1993), at 26.

[2005] *Loi informatique et liberté*, *supra* note 131 at c. V, s. 1, (II), art. 39 (5)**;** EC, *Directive 95/46/EC*, *supra* note 99 at art. 12 (a).

[2006] *Loi informatique et liberté*, *supra* note 131 at c. II, s. 2, art. 10. See also EC, *Directive 95/46/EC*, *supra* note 99 at art. 15 (1) and (2).

information is "relevant" for the intended use. In 1973, the fact that only relevant information should be used to discriminate individuals was already being discussed.[2007] It was found, for instance, that "race" and "sex" were already no longer asked on many application forms, because of their acknowledged influence on some types of decision making about individuals.[2008] In Europe, Resolution 73 (2), leading to the adoption of Convention 108, suggested that:

> "An example of information which may lead to unfair discrimination is that about his state of health, or his past criminal record. The text of this principle makes a distinction between the keeping and the release of this kind of information. Even though in general it is not allowed to record such information, there may be exceptions to this rule, for example in the case of a counseling agency for alcoholics, or of a political party. In such cases the dissemination of the information is not allowed, however."[2009]

The Lindop Report (U.K., 1978) also suggested that the requirement that information be "relevant" for the intended use was a very important one.[2010] Almost thirty years later, in the context of U.K. regulators looking at the "*preventing harm*" principle as a valid way forward, the U.K. Information Commissioner emphasized the need to make judgments about the seriousness of the risks of individual harm (that individuals will suffer) because personal information held about them is "excessive or irrelevant".[2011]

The current section will explore various themes, including the interpretations of "relevant" or "necessary" found in case law and how, with the advent of new

---

[2007] U.S. Department of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *supra* note 57 at s. IV.

[2008] *Ibid*.: "There is also reason to believe that failure to separate information collected for statistical-reporting or research from data used in entitlement decisions may cause such decisions to be made unfairly. 'Race' and 'sex' are no longer asked on many application forms because of their acknowledged influence on some types of decision making about individuals."

[2009] See Council of Europe, *Explanatory Report: Resolution (73) 22*, *supra* note 56 at para. 19.

[2010] Lindop, *supra* note 96 at 47, para. 5.42.

[2011] ICO, *Data Protection Strategy*, *supra* note 986 at 7: "The principal risk which our activities must address is the risk that individuals will suffer harm because personal information about them is (…) excessive or irrelevant."

technologies and an increase in the volume of information readily available,[2012] the "relevancy" criterion is crucial and more important than ever.

3.2.2.3.1. DPLs regulating the Relevancy or Necessity of Data

Canadian and French DPLs stipulate that information "used" should be *relevant* or *necessary* for the purpose intended, as discussed below. Some DPLs focus on the word "relevant", while others, on the word "necessary". The parliamentary debates leading to the adoption of the Quebec DPL in 1993 illustrate that the draft DPL emphasized the "relevance" of data. In the end, the Quebec legislator decided to use the word "necessary" instead of "relevant", as it was found to be less subjective and more stringent.[2013]

I already discuss, in section 3.1.1.1.1(b), the fact that individuals will react negatively to a collection which seems to be irrelevant for the organization collecting it (what I call an "excessive" collection). This concern was already present in the early 1970s and we can note that the Report of the Secretary's Advisory Committee on Automated Personal Data Systems raised this very issue:

> "The personal data that organizations collect for administrative purposes should be limited, ideally, to data that are demonstrably relevant to decision making about individuals."[2014]

Section 3.1.1.2.1(b) already elaborates on how current Canadian and French DPLs prohibit the collection of information in exchange for services or products, and the collection of information which is not "necessary" for the purpose of collection. Section

---

[2012] See section 1.2.1 entitled "Increase in Volume of Information" which elaborates on this issue.

[2013] See *Les travaux parlementaires*, 34th législature, 2nd session, Commission permanente de la culture, cahier no 11 (February 23, 1993), at 21 and 22; *Les travaux parlementaires*, 34th législature, 2nd session, Commission permanente de la culture, cahier no 13 (March 1, 1993), at 23; *Les travaux parlementaires*, 34th législature, 2nd session, Commission permanente de la culture, cahier no 15 (March 3, 1993), at 4, 5, 26 and 41; and *Les travaux parlementaires*, 34th législature, 2nd session, Commission permanente de la culture, cahier no 23 (May 13, 1993), at 6.

[2014] U.S. Department of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *supra* note 57 at s. IV: "A substantial amount of personal data, however, appear to be collected because at some point someone thought they might be 'useful to have,' and found they could be easily and cheaply obtained on an application form, or some other record of an administrative transaction. (….) We found that decisions to collect personal data are being made without careful consideration of whether they will in fact serve the purposes for which they are supposedly being collected."

1.2.4.1 elaborates on the fact that on the web, many of the services, information, and entertainment are sponsored, and that therefore, these kinds of provisions make much less sense in light of the emergence of these new types of online business models. Section 2.1.1.2 elaborates on the fact that individuals living in our modern society often have often no other choice but to provide their personal information to gain employment, procure insurance, obtain credit, to benefit from various public-sector and private-sector services. It is therefore arguable whether they have the *full control* over their personal information.

DPLs have certain subjectivity surrounding what kinds of "uses" are acceptable, once the data is in the hands of organizations. In Canada, article 5 (3) states that an organization may use personal information "only for purposes that a reasonable person would consider are appropriate in the circumstances".[2015] In Quebec, the C.c.Q., section 37, also provides similar relevancy requirements.[2016] The Quebec DPL provides that an organization may only use personal information for purposes which are "relevant" to the object of the file, unless with the individual's consent.[2017] This provision has been given a *stricto sensu* application and it is the organization's responsibility to ensure that personal information about an individual contained in a file is only used in accordance with the object of the file.[2018] Under the Alberta and B.C.

[2015] Principle 4.4.1 of PIPEDA states that: "Organizations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is *necessary* to fulfil the purposes identified." These two provisions (article 5 (3) of PIPEDA and principle 4.4.1. of PIPEDA) are often used "together" when the OPCC has to evaluate whether certain information collected is "necessary" for the intended use. See for example OPCC, *PIPEDA Report of Findings #2011-001, Report of Findings: Google Inc. WiFi Data Collection*; OPCC, *PIPEDA Case Summary #2009-014, Fraud detection not an acceptable reason to collect driver's licence numbers for store memberships* (29 May 2009) [OPCC, *PIPEDA Case Summary #2009-014*]; OPCC, *PIPEDA Case Summary #2009-008*, *supra* note 288.

[2016] Art. 37 C.c.Q.

[2017] Or if it is expressly authorized to do so under an exception in the Quebec DPL. Quebec DPL, *supra* note 110 at s. 13.

[2018] *X. v. Le Groupe Jean Coutu (P.J.C.)*, [1995] C.A.I. 128 [*Groupe Jean Coutu*]; *Laval (Ville) c. X.*, 2003 CanLII 44085 (C.Q.) [*Laval*]. Should an organization err and inappropriately use the personal information, it may be held liable for damages. See *Roy v. Société sylvicole d'Arthabaska-Drummond*, J.E. 2005-279 (C.Q.).

DPLs, an organization may use personal information only for purposes that a "reasonable person would consider appropriate in the circumstances".[2019]

In France, there is a similar requirement of legitimacy and the processing of personal data can only take place if the data is collected and processed in a loyal and licit manner,[2020] in line with Directive 95/46/EC on this issue.[2021] Organizations therefore can make a subjective assessment as to whether a certain piece of information is *relevant* or *necessary*, *appropriate* or *reasonable* in the circumstances.

Case law rendered on relevance or necessity of data, may assist in determining what kind of uses are considered as being acceptable by courts, and therefore, are "reasonable", "licit", or "appropriate".

3.2.2.3.2. When is Information Necessary or Relevant?

In the Information Age, organizations have more access than ever to various types of information.[2022] They may be collecting new types of data and sometimes, they may be collecting information using new types of collection tools.[2023] These organizations may wish to use the information collected or available for various purposes.[2024] It is not always clear if the information to be used may qualify as "necessary" or "relevant" under the DPLs requirements.

Case law rendered under the legal provisions found in Canadian and French DPLs under which only "relevant" or "necessary" information may be collected and used can assist, to a certain extent, in determining the situations in which certain information may be deemed "relevant" or "necessary" for a particular use. The establishment of an objective criterion to define the meaning of "necessary" under the Quebec DPL still

---

[2019] Alberta DPL, *supra* note 114 at Part 2, Division 1, s. 5 (1) and (5) and s. 2; B.C. DPL, *supra* note 115 at Part 5, s. 14 (a) and Part 2, s. 4 (1).

[2020] *Loi informatique et liberté*, *supra* note 131 at c. II, s. 1, art. 6 (1) and (2).

[2021] EC, *Directive 95/46/EC*, *supra* note 99 at arts. 6-7.

[2022] See section 1.2 entitled "Technological Background Affecting Personal Information" which elaborates on this issue.

[2023] See section 1.2.2 entitled "New Types of Information and Collection Tools" which elaborates on this issue.

[2024] See section 1.2.4 which elaborates on these new uses.

appears to be unsettled law. At times, the CAI and the Quebec courts have adopted a very restrictive approach under which "necessary" means "absolutely indispensable".[2025] At other times, the CAI and the Quebec courts have preferred to adopt a more contextual approach, which illustrates the difficulty encountered in establishing a specific criterion to be applied to the definition of "necessity/necessary."[2026] Finally, in a recent decision rendered by the Court of Quebec,[2027] a new method to determine and apply the "necessity" criterion was developed which proposes a test similar to the one developed in *R*. v. *Oakes*[2028] under which the information is deemed necessary when it is collected for a legitimate and important objective, and the invasion of privacy is proportionately less important to those objectives.[2029] It has generally been acknowledged that the burden lies with the

[2025] As a matter of fact, some CAI decisions apply the very narrow definition of "necessity" set out in Louis Philippe Pigeon, *Rédaction et interprétation des lois*, 1st ed., coll. "Études juridiques" (Québec: *Éditeur officiel*, 1978) at 15, where former Justice Louis-Philippe Pigeon underscores that "necessary" means "absolutely indispensable" (in French: "absolument indispensable/nécessité ineluctable"). According to these decisions, this strict definition must be adopted in order to accomplish the goals of DPLs. According to this approach, absent any reasonable basis to doubt its truthfulness, an indication that an employee is sick justifies his absence, without having to provide a medical diagnosis. *Syndicat des employées et employés professionnels et de bureau, section locale 57 and Caisse populaire St-Stanislas de Montréal*, D.T.E. 99T-59 (T.A.) [*section locale 57*]. See *Ordre des comptables*, *supra* note 1302 at 6; See also *Aventure Électronique*, *supra* note 1302 at 7-8: "[TRANSLATION] In law, the word 'necessary' has a very rigorous and rigid meaning. It denotes exclusively what is absolutely indispensable. In everyday language, we have a tendency to use the word 'necessary' to denote what is simply convenient or useful. However, in law, 'necessary' means something that is absolutely indispensable, that one cannot do without. In short, an inescapable necessity."

[2026] As per this second approach, the CAI and the Quebec courts have examined the factual context in which the question of "necessity" arises. Most of these decisions where rendered under the Quebec public sector DPL, which bears a similar requirement that public bodies not collect personal information that is not necessary for the carrying out of the mandate of the body or the implementation of a program under its management. Section 64 of the Quebec public sector DPL. The Superior Court also ruled that the decisions and interpretations rendered under the Quebec public sector DPL apply for the purpose of the interpretation of the Quebec DPL [*La Personnelle vie, Corporation d'Assurance v. Cour du Québec*, [1997] C.A.I. 466 (S.C.)]. See Karl Delawaide and Antoine Aylwin, "Leçons tirées de dix ans d'expérience : la *Loi sur la protection des renseignements personnels dans le secteur privé* du Québec" (2005) 233 Développements récents en droit de l'accès à l'information, at 13.

[2027] *Laval*, *supra* note 2018.

[2028] [1986] 1 S.C.R. 103.

[2029] The Quebec court has therefore preferred a balanced approach in order to protect the fundamental rights of privacy, when required. The determination of what is necessary information must be evaluated in light of the particular circumstances of each case. See *A. v. C.*, *supra* note 1302 at para. 63. See also Judge Filion of the Court of Quebec at para. 64: "[TRANSLATION] it is not a question of determining what is necessary as such, but rather one must look, in the context of the protection of personal information, and each situation, what is necessary to accomplish each particular goal".

person who claims that a piece of information is necessary.[2030] In France, the CNIL has issued various guidelines to be followed by organizations when evaluating employees.[2031] The CNIL usually adopts a strict position when determining whether certain information is "relevant", as detailed below.

(a) Internal Purposes

Organizations may be collecting information, in some cases for internal purposes. These may include the purposes of ensuring the quality of their services, for security and fraud detection purposes and for legal compliance. These types of uses are usually considered as "necessary" under the DPLs, according to the applicable case law.

(i) Quality of Services

Online service providers, such as search engines, collect and process vast amounts of user data including log files of search engine use. Various technical means are employed in this capacity, namely cookies. They claim to collect some of this data for internal purposes, such as to improve their services and the quality of their search services.[2032] Personal information used for ensuring the quality of the services provided is usually viewed as necessary. For instance, Canadian case law rendered on the notion of information "necessity" suggests that it is reasonable for an organization to collect and use: information through Deep Packet Inspection (DPI) technology, in order to ensure adequate bandwidth and quality of Internet service (ISP);[2033] information in exchange for an online service sponsored by advertising (Facebook);[2034] or information to track the location of the company's vehicles, for purposes of managing its assets.[2035]

[2030] *Groupe Jean Coutu*, *supra* note 2018; *Tremblay*, *supra* note 1967; *Julien*, *supra* note 1302 ; *A. v. C.*, *supra* note 1302.

[2031] CNIL, *Guide pour les employeurs et les salariés* (CNIL, 2010), online : <http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL_GuideTravail.pdf> [CNIL, *Guide 2010*].

[2032] Varian, *supra* note 387. Google claims that it needs users data for fighting webspam. Web spam is junk that the user sees in search results when websites successfully cheat their way into higher positions in search results or otherwise violate search engine quality guidelines. See Cutts, *supra* note 388.

[2033] OPCC, *PIPEDA Case Summary #2009-010, Assistant Commissioner recommends Bell Canada inform customers about Deep Packet Inspection* (13 August 2009).

[2034] OPCC, *PIPEDA Case Summary #2009-008*, *supra* note 288.

[2035] OPCC, *PIPEDA Case Summary #2006-351*, *supra* note 214.

At the same time, it is not clear if the collection and use of information for the development of new services would also be considered as legal (relevant or necessary information). In France, the CNIL took the position in Délibération n°2010-113 of April 22, 2010, that it was illegal for an organization to collect information about its clients (in this case, comments about its clients, students and their families) which had no connection with the services provided.[2036] This kind of reasoning may limit what organizations may collect in order to improve their products and services if the information collected is not relevant for the products or services already provided. This being said, I further elaborate in section 3.2.3.2.3 on how I am of the view that organizations should be able to use information to develop new services, if there is no harm in doing so, meaning if the information collected and used creates no risk of harm for individuals.

(ii) Security and Fraud Detection Purposes

Certain online service providers such as search engines also claim to collect and use personal information to keep their services secure and their users safe from *malware* or *phishing* attacks,[2037] or to detect and prevent advertising "click fraud".[2038] Personal information used in fraud detection or for security purposes is usually viewed as necessary. For example, in Canada, the OPCC has taken the position that it was reasonable for an organization to collect and therefore use the following information for such purposes: driver's license numbers for store memberships;[2039] driver's license or passport from an individual requesting a change to the administration e-mail address for a website domain name, as domain name hijacking is of concern to the industry (domain name registrar);[2040] personal information gathered through a telephone

---

[2036] *Délibération n°2010-113 du 22 avril 2010 de la formation restreinte portant avertissement à l'encontre de la société AIS 2 exerçant sous l'enseigne ACADOMIA Respecter* [*Délibération n°2010-113*].

[2037] Provos, *supra* note 389.

[2038] In some cases, search engines even argue that if such collection is not "necessary", it is at least not harmful to individuals. See Article 29 Data Protection Working Party, *Opinion 1/2008*, *supra* note 207 at 15-16.

[2039] OPCC, *PIPEDA Case Summary #2009-014*, *supra* note 2015.

[2040] OPCC, *PIPEDA Case Summary #2006-363, Registrar collects personal information to combat domain name hijacking* (14 December 2006).

connection for preventing piracy (satellite TV provider);[2041] and the location of the company's vehicles to protect its assets.[2042] Recently, in the Alberta Court of Appeal case *Leon's Furniture Limited v. Alberta (Information and Privacy Commissioner)*,[2043] Leon's locations in Alberta were found to be well within their rights to request from customers their driver's licenses and license plate numbers. This information was used at the loading dock to ensure that the right person comes to collect furniture therefore preventing fraudsters from driving off with someone else's goods.[2044] In France, the collection of the location data of employees, in part for security purposes, is legal (as this information is relevant for security purposes), although employees have to be informed of this collection.[2045] At the same time, the Tribunal de Grande Instance from Paris has taken the position that it was illegal for an employer to collect the digital fingerprints of employees in order to operate a system used to manage the employees' presence and their payment for the reason that the security usefulness was not properly demonstrated by the employer.[2046]

(iii) Legal Requirement or Compliance

Organizations from the private sector may wish to use IP addresses to ensure legal compliance in certain cases, such as to enforce Intellectual Property rights on the Internet.[2047] For example, one commonly used surveillance method of the Canadian

---

[2041] OPCC, *PIPEDA Case Summary #2004-276, The privacy implications of pay per view and piracy prevention measures* (2 September 2004).

[2042] OPCC, *PIPEDA Case Summary #2006-351*, *supra* note 214.

[2043] *Leon's Furniture Limited v. Alberta (Information and Privacy Commissioner)*, 2011 ABCA 94 (CanLII).

[2044] Alberta's OPC said that the practice violated the Alberta DPL, but Leon's successfully challenged this in court. The Supreme Court of Canada recently refused to hear an appeal of that decision, so the appellate court's analysis stands, even though it was a split 2-1 decision.

[2045] See CA Dijon, 14 September 2010, online: http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=2999 and see also the recommendations of the CNIL on the issue of videosurveillance which must be complied with. See CNIL, "La vidéosurveillance sur les lieux de travail", online : <http://www.cnil.fr/la-cnil/actu-cnil/article/article/la-videosurveillance-sur-les-lieux-de-travail/>.

[2046] Trib. gr. inst. Paris, 19 April 2005, *Comité d'entreprise Effia Services, Fédération des syndicats Sud Rail c. Effia services*, No. 05-00382.

[2047] Certain lobby groups and governments have moved toward requiring ISPs to terminate subscribers' accounts if they engage in file sharing activities on three occasions. See: EDRI, "French minister: copyright above privacy" (3 November 2005), online: <http://www.edri.org/edrigram/number3.22/copyright>; Michael Geist, "Quebecor Opens Door to Canadian Three Strikes Policy" (26 February 2006), online: Michael Geist <http://www.michaelgeist.ca/content/view/3706/125/>; Michael Geist, "'Three Strikes and You're Out'

and American music recording industries is known as "web bots"[2048] that are employed to locate alleged wrongdoers and collect evidence of illegal activities.[2049] Certain U.S. online gambling laws prohibit organizations from taking bets from U.S. citizens. Therefore, online gambling websites often use IP addresses that disclose the user's location for legal compliance, in order to block users from the U.S.[2050]

Personal information, used for legal compliance, is usually viewed as necessary. For example, in Canada, the OPCC has taken the position that it was reasonable for an organization to collect and therefore use the following information for legal compliance purposes: the customer's citizenship card (bank);[2051] personal information of employees who access the airport's restricted area (airport);[2052] and Social Insurance Number when a customer opens a savings account (bank).[2053] Other types of collection were found unnecessary because it was the wrong party collecting otherwise necessary information,[2054] or because it was collected preventively, in the event that the law changes in the future and requires certain additional data collections.[2055]

Policy Strikes Out" (21 April 2008), online: Michael Geist <http://www.michaelgeist.ca/content/view/2851/135/>.

[2048] Web bots are software programs that continually crawl from one server to another in cyberspace, compiling lists of sites having particular characteristics. They are launched in peer-to-peer networks to automatically scan user hard drives for titles of unauthorized copyrighted materials. See Katyal, *supra* note 1044 at 341.

[2049] When the web bots finds what appears to be infringing material, they match the user's IP address to its ISP and send a copyright violation notice to the ISP. IP addresses may also be used to provide online advertisers with correct billing information showing that genuine users are clicking on online ads since Internet "click fraud" can be traced by showing that the same IP address is jumping repeatedly to the same ad. See *ibid*. at 311.

[2050] IP addresses can also be used to block certain online users which may come from foreign jurisdictions, for instance if these jurisdictions do not have adequate DPLs or if certain users come from a jurisdiction in which the web services offered are illegal. See Eloïse Gratton, "Aiding-and Abetting Liability Exposure of Affiliate Program Service Providers Under the New U.S. Internet Gambling Law" (2007) 10:12 Journal of Internet Law.

[2051] OPCC, *PIPEDA Case Summary #2004-286, Bank customers required to declare citizenship* (21 December 2004).

[2052] OPCC, *PIPEDA Case Summary #2003-255, Airport authority's collection and retention practices questioned* (24 December 2003).

[2053] This was done to comply with the *Income Tax Act*, banks which require them to collect the SIN of individuals who open a personal, interest-bearing account, in order to supply CCRA with reports of income on deposits OPCC, *PIPEDA Case Summary #2003-209, Individual alleged that bank request for SIN was unnecessary* (5 August 2003).

[2054] It was found unnecessary for an international trucking company to collect the application for the Customs Self-Assessment Program and return it to the CCRA (although it was acceptable to collect this

(b) Evaluating Individuals

It has been reported that many employers are screening OSNs for data about employees or applicants.[2056] Certain lenders were also recently reported using OSNs, such as Facebook and Twitter, to gather information about current or potential borrowers.[2057] Any information found on an OSN or on the web could be used to make a decision which could be harmful for the individual, as this information may be used to decide whether to offer or refuse employment, grant a loan or credit, evaluate an insurance claim, provide insurance services, etc. Whether the data used is "relevant" or "necessary" for the intended purpose is therefore, more than ever, an important issue, as well as a tricky one since the relevancy of this information may not be straight forward:

> "Employers tempted to search OSNs without such consent should keep in mind that (…) it is debatable whether employers would be found to have collected information "necessary" for the employee's file or, as the case may be, to be using the information for purposes that are relevant to such file in compliance with the Quebec legal framework. In the event that the profile of the employee reveals information which employers may not like, they may actually have a hard time "using" the profile information to justify, for example, not hiring a potential employee. Quebec courts are usually reluctant to allow an employer to discriminate against an employee using information which is not related to the job for which an individual is applying for (such as a criminal record). It may therefore be a challenge for an employer to demonstrate that an employee who enjoys a good night out on a day off would necessarily be a "bad employee". Ever heard the expression "Work hard, play hard"?"[2058]

---

information, it was not for the employer to collect this information itself), OPCC, *PIPEDA Case Summary #2001-10, Trucking company collects personal information intended for Canada Customs* (17 August 2001).

[2055] A bank should not collect birth dates simply because they believe that revised regulations may one day compel all banks to collect dates of birth from customers. OPCC, *PIPEDA Case Summary #2002-45, Bank accused of misrepresenting purposes in collecting date of birth* (11 April 2002); OPCC, *PIPEDA Case Summary #2002-46, Bank accused of inappropriately demanding birthdates from account applicants* (26 April 2002).

[2056] Hanna, *supra* note 1979.

[2057] Tim Grant, "Lenders using Facebook, Twitter to gather borrower information" *Pittsburgh Post-Gazette* (28 May 2010), online: post-gazette.com <http://www.post-gazette.com/pg/10148/1061287-28.stm>.

[2058] See Gratton, "Quebec Employers", *supra* note 1829.

Many of the decisions rendered in Canada, Quebec and France (which may be useful in order to determine what kind of information is "relevant" or "necessary") are in connection with evaluating the health condition of an individual, this individual's financial situation (credit) or his or her suitability for employment.

(i) Health Condition

Employers or insurers may wish to access and use medical or health information of their employees or clients. Medical files are normally kept private; nevertheless, their consultation may become necessary in certain specific situations. Many U.S. states prohibit employers from questioning employees or applicants about certain health matters.[2059] In Canada, the OPCC has taken the position that it was necessary, in order to assess the medical condition of an individual, to collect (and therefore use) the following: based on substantial evidence after having tried less privacy-invasive ways, for an employer to videotape an employee (to assess if he is misrepresenting his state of health);[2060] for an employer to ask the employee's physician to release medical information about his illness to its occupational health staff, while on extended sick leave;[2061] and for an employer to collect health information of an employee to determine if he could be accommodated in another position for medical reasons.[2062] The OPCC has also taken the position that it was unnecessary for an adjuster to

[2059] For example, Solove discusses the fact that Wisconsin forbids employers from requiring employees or applicants to undergo HIV testing (Wis. Stat. Ann. § 103.15(2) (West 2002)); Massachusetts prohibits employers from asking about arrests not leading to conviction, misdemeanor convictions, or any prior commitment to mental health treatment facilities (Mass. Gen. Laws Ann. ch. 151B, § 4(9), (9A) (LexisNexis 1999)); and several U.S. states restrict employers from requiring employees or applicants to undergo genetic testing (*See, e.g.*, Cal. Gov't Code § 12940(o) (West 2005); Conn. Gen. Stat. Ann. § 46a-60(11)(A) (West 2004); Del. Code Ann. tit. 19, § 711(e) (Supp. 2004); N.Y. Exec. Law § 296.19(a)(1) (McKinney 2004)). See Solove, "A taxonomy", *supra* note 339 at 502.

[2060] OPCC, *PIPEDA Case Summary #2004-269, Employer hires private investigator to conduct video surveillance on employee* (23 April 2004).

[2061] OPCC, *PIPEDA Case Summary #2003-118, Employer's effort to collect personal medical information deemed appropriate; no evidence of inappropriate disclosure* (17 February 2003); OPCC, *PIPEDA Case Summary #2003-119, Employer's policy and practices regarding the collection of personal medical information deemed appropriate* (17 February 2003).

[2062] *Ibid*.

collect medical information dating back five years relating to a car accident in which the claimant had been injured.[2063]

In both Canada and Quebec, any indication that an employee is sick justifies his or her absence, without having to provide a medical diagnosis.[2064] The CAI or the Quebec courts or arbitrators have taken the position that the following information was necessary (or relevant) to allow an employer to dismiss (or to refuse to hire) an employee: the fact that a monitor at a summer camp is epileptic;[2065] the fact that an employee working at a factory had back problems;[2066] and the fact that an employee working as a steelworker had asthma.[2067] The Superior Court of Quebec has taken the position that when a potential new employer is verifying work references, an ex-employer should not be disclosing medical information "unnecessary" to assess the suitability for the applicant's job.[2068] In France, the CNIL confirms that in general, employees' health information shall not be collected by employers,[2069] and more specifically, that the health situation of employees, their height and weight, as well as their vision score are also not to be requested by employers (unless this information is specifically linked to, and relevant for, the employment).[2070] In other words, if

---

[2063] OPCC, *PIPEDA Case Summary #2006-362, Insurance adjuster readjusts its collection practices* (14 December 2006).

[2064] OPCC, *PIPEDA Case Summary #2004-281, Organization uses biometrics for authentication purposes* (3 September 2004); OPCC, *PIPEDA Case Summary #2003-257, Employees objected to corporation's requirement for medical diagnosis on sick leave certificates* (Fall 2003); OPCC, *PIPEDA Case Summary #2003-191, Company's collection and disclosure of employee sick leave information* (11 July 2003); OPCC, *PIPEDA Case Summary #2003-233, An individual challenged the requirement to provide the medical diagnosis on her doctor's certificate for sick leave* (3 October 2003); *Section locale 57*, *supra* note 2025. Moreover, in filling a part of an insurance coverage claim, an employer does not need to know, unless an employer is in charge of managing disability claims, the exact diagnosis of an employee absent from his employment. The physician's statement of the employee's disability (and applicable period) should be sufficient. *X. and Synergic International 1991*, [1995] C.A.I. 361.

[2065] *Larochelle c. Association des personnes handicapées de Lévis*, D.T.E. 2006T-359 (C.Q.).

[2066] *Fraternité nationale des forestiers et travailleurs d'usines et Groupe Bocenor, usine de Ste-Marie*, D.T.E. 2005T-545 (T.A.).

[2067] *Métallurgistes unis d'Amérique, section locale 696 et Waterville TG*, D.T.E. 2002T-1078 (T.A.).

[2068] *St-Amant c. Meubles Morigeau ltée*, [2006] R.J.Q. 1434 (C.S.)

[2069] CNIL, *Guide* 2010, *supra* note 2031 at 3: "Seules doivent être traitées les informations pertinentes et nécessaires au regard des objectifs poursuivis. *Par exemple : le recueil d'informations sur l'entourage familial, l'état de santé ou encore le numéro de sécurité sociale d'un candidat à un recrutement n'est pas pertinent. L'enregistrement de la situation familiale précise d'un salarié ne peut se justifier que pour l'attribution d'avantages sociaux particuliers au salarié ou à sa famille.*"

[2070] *Ibid*.

employers wish to use employees' (or potential employees') medical information, they must ensure that it is relevant for assessing suitability for the job in question. This issue of assessing suitability for employment is further discussed in section (iii) below.

(ii) Financial Situation

Organizations such as service providers, insurers, employers, landlords and banks may wish to obtain information pertaining to the financial situation of their potential clients or employees. The OPCC has taken the position that it was necessary, in order to assess the financial situation of an individual, to collect (and therefore use) the following information: for a bank to request information on additional credit on a rental property owned and Notices of Assessment (Revenue Agency) for the last two years from an individual wishing to secure a line of credit;[2071] for a telecommunications company to require two pieces of identification for a credit check from an applicant for a residential phone line;[2072] for a bank to request from an applicant for a credit card, her vehicle's model year, the number of kilometers on it, its current value, and her property and school taxes;[2073] for a telecom company to require two pieces of identification for running a credit check before initiating a telephone service.[2074] The OPCC found that an insurance adjusters' consent form was overly broad (collecting credit history, financial information, medical information, driver's record, and employment information) and therefore, he was collecting information which was irrelevant for the purpose of processing the insured's claim for theft of jewelry and money.[2075]

[2071] OPCC, *PIPEDA Case Summary #2003-169, Individual objects to bank's requirements to provide Notice of Assessment for income verification purposes* (24 April 2003).

[2072] OPCC, *PIPEDA Case Summary #2003-217, A telecommunications company requires two pieces of identification from a subscriber* (5 August 2003).

[2073] OPCC, *PIPEDA Case Summary #2003-223, Bank accused of collecting too much information from credit card applicant* (16 September 2003).

[2074] OPCC, *PIPEDA Case Summary #2002-94, Individual objects to request for information as condition of supply of service* (2 December 2002). It was also acceptable to refuse to provide telephone service upon an applican't refusal to provide her social insurance number since the complainant was provided with a choice of identification that she could provide or a security deposit option. See OPCC, *PIPEDA Case Summary #2003-204, Telecommunications company accused of refusing services unless SIN was provided* (5 August 2003).

[2075] OPCC, *PIPEDA Case Summary #2007-368, Insurance adjusters' consent form considered overly broad* (11 January 2007).

In Quebec, the CAI found that organizations were collecting unnecessary information in the following instances: request of a social insurance number or driver's license number for the purpose of verifying the client's credit (telecom service provider);[2076] request an authorization for a credit record as part of a rental application (landlord);[2077] or a credit enquiry request for an entry-level position in management (employer).[2078]

In France, the CNIL confirms that employers should not collect the employee's banking information, his credit situation (loans subscribed to, etc.), as well as any debt or payment for which the employee is in default, unless this information is specifically linked to, and relevant for, the employment.[2079] In one specific case, the CNIL has taken the position that the collection of the banking information of a "potential" employee was not yet relevant.[2080] The CNIL has also found that the registration by an organization at a national database detailing the defaults of individuals with regards to the payment of loans or debts (the fichier FICP)[2081] of an incident which took place over

[2076] Although the CAI did not specifically rule on the legitimacy of conducting a credit verification in such situation. *Comeau v. Bell Mobilité*, AZ-50110177 (C.A.I.).

[2077] *A. v. C.*, [2003] C.A.I. 534. The CAI has determined that only the following information meets the necessity criterion in a residential rental agreement: *surname and given name; telephone number; names and contact information of the owner (or landlord) of the residence being occupied, in order to establish the payment habits of this applicant; an excerpt from the credit records of the applicants with their consent. The respondent may also require the date of birth*. In addition, the CAI confirmed that a credit record cannot be accessed without consent. See also *Perrault v. Blondin*, A.I.E. 2006AC-42. The information that may be collected is limited to information on the potential tenant's previous landlord – in order to verify their payment history – and only their name and date of birth – in order to complete a credit check. See *Julien*, *supra* note 1302.

[2078] *Delaney v. Les associés, services financiers du Canada Limitée* (2001), Montréal PV 00 03 47, AZ-50110191 (Azimut) (C.A.I.). Other illustrations of the test of necessity: *X. c. Résidence L'Oasis Fort St-Louis*, [1995] C.A.I. 367 [*Résidence L'Oasis*]; *Perreault c. Blondin*, [2006] C.A.I. 162. This position is in line with Alberta, a jurisdiction in which the Information and Privacy Commissioner of Alberta recently ordered Marks' Work Wearhouse to stop carrying out routine credit checks on prospective employees. See Alberta Office of the Information and privacy Commissioner, *Report of an Investigation into the Collection of Personal Information* (16 February 2010), online: <http://www.oipc.ab.ca/downloads/documentloader.ashx?id=2529>.

[2079] CNIL, *Guide* 2010, *supra* note 2031 at 8: "La collecte des informations suivantes n'est pas pertinente, sauf cas particuliers justifiés par la nature très spécifique du poste à pourvoir ou par une obligation légale: (…) domiciliation bancaire, emprunts souscrits, défauts de paiement."

[2080] *Délibération n°2010-113*, *supra* note 2036.

[2081] Fichier national des Incidents de remboursement des Crédits aux particuliers (FICP).

sixteen years ago was illegal as it was at that point irrelevant, and should have been made upon the incident taking place.[2082]

In light if these various decisions rendered on the "relevancy" criteria in the context of evaluating the financial situation of an individual, it is therefore debatable whether information found online by employers, landlords and lenders about employees or potential ones, tenants or borrowers on OSNs (which could be used in a harmful way towards these individuals) would found to be considered as "relevant" or "necessary" according to DPLs (on top of being potentially inaccurate).

(iii) Assessing Suitability Candidates for Employment

Employers may wish to use information pertaining to their employees or applicants, found online or on OSNs, in order to assess their suitability for a position. In Quebec, discrimination is prohibited due to section 18.1 of the *Charter of Human Rights and Freedoms* (the "Quebec Charter").[2083] The Quebec Charter stipulates that employers are not allowed to request information regarding race, skin colour, gender, pregnancy, sexual orientation, civil status, age (except as provided by law), religion, political convictions, language, ethnic or national origin, social condition, a handicap, unless the information is useful for the application.[2084]

Canadian and French employers are usually within their rights to verify the information provided by a candidate, such as credentials and education; in France, it can only be done with the employee's prior knowledge.[2085] In Quebec, an employer would be

---

[2082] *Délibération n°2006-245*, *supra* note 1940.

[2083] R.S.Q., c. C-12. Section 10 of *Charter of Human Rights and Freedoms*. In *Résidence L'Oasis*, *supra* note 2078, the CAI took the position that at the pre-hiring stage, only the information that the Quebec Charter allows an employer to ask for shall be necessary, that is, the information that is indispensable for evaluating whether a candidate has the qualifications and aptitudes required for the purposes of the job.

[2084] Quebec *Charter of Human Rights and Freedoms*, *supra* note 2083 at s. 18.1.

[2085] CNIL, *Guide* 2010, *supra* note 2031 at 8: "Le recueil de références auprès de l'environnement professionnel du candidat (supérieurs hiérarchiques, collègues, maîtres de stages, clients, fournisseurs...) est permis dès lors que le candidat en a été préalablement informé." In Quebec, there is a similar requirement. See *Prelco Inc. et Syndicat national de l'automobile, de l'aérospatiale, du transport et des autres travailleurs et travailleuses du Canada, section locale 1044*, D.T.E. 99T-41 (T.A.); *Syndicat québécois des employées et employés de service, section locale 298 and Jardins du Haut-St-Laurent (1990) enr.*, [2003] R.J.D.T. 1026 (T.A.); *Scobus St-Hubert Inc. et Syndicat international des travailleurs et travailleuses unis de l'alimentation et du commerce, section locale 501*, [1992] T.A. 497.

deemed to have been using "relevant" or "necessary" information when verifying the credentials of an employee, but the key element (for instance to justify using this information to dismiss an employee) would be that the employer would never have hired the person in question had he been correctly informed about the applicant's credentials. Supposing there had been no prejudice to the employer, the "necessity" criterion would not have been fulfilled.[2086] In France, the French labor code prohibits the collection by employers of employee's information which is not directly linked to, or is necessary for, the employment.[2087] The CNIL also confirms that irrelevant and unnecessary information of employees, such as their personal situation (including any information on their husband, wife, kids, extended family), nationality or origins, religion, political views, military situation, whether the employee is the owner of a house vs. renting, or the social security number of an applicant (not yet employee) shall not be collected by employers.[2088] In addition, employers shall not include, in the employees' files, information irrelevant to the individual in his capacity of employee, such as "annoying", "smells bad", or "no teeth and drinks a lot".[2089] In one specific case, the CNIL took the position that the collection of the national identity number, banking information and information about the family situation of a "potential" employee was not (at least yet) relevant,[2090] although the collection of the details of the family situation of

---

[2086] See *Syndicat national des employés de l'Aluminium d'Alma Inc., (section des employés horaires) et Société d'électrolyse et de chimie Alcan Ltée, usine Isle-Maligne, Alma*, D.T.E. 2001T-904 (T.A.), in which there was a grievance challenging the dismissal of the complainant, who had worked as an operator in the employer's smelter for over 27 years. Following verification with the Ministère de l'Éducation, it was found that the complainant had produced a false diploma and modified a transcript when applying for the job. In this case, the dismissal was replaced by a 16-month suspension because of the lack of prejudice for the employer.

[2087] See article L.1221-6 of the French Code du travail: "les informations demandées, sous quelque forme que ce soit, au candidat à un emploi ne peuvent avoir comme finalité que d'apprécier sa capacité à occuper l'emploi proposé ou ses aptitudes professionnelles". De sorte que ces informations "doivent présenter un lien direct et nécessaire avec l'emploi proposé ou avec l'évaluation des aptitudes professionnelles".

[2088] CNIL, *Guide* 2010, *supra* note 2031 at 3, 8.

[2089] *Ibid*. at 9: "Conformément aux articles 45 et suivants de la loi du 6 janvier 1978 modifiée, la formation contentieuse de la CNIL a prononcé, le 11 décembre 2007, une sanction pécuniaire d'un montant de 40 000 euros à l'encontre de cette société, compte tenu de la gravité des manquements constatés *(Délibération n° 2007-374 du 11 décembre 2007)*."

[2090] *Délibération n°2010-113*, *supra* note 2036.

an employee will be relevant to issue the appropriate employee benefits (once the applicant is in fact employed).[2091]

In certain situations, employers may want to access the criminal records of employees but these records must be relevant or necessary to assess suitability for employment. In Canada, in *Therrien (Re)*,[2092] the Supreme Court took the position that criminal records were not essential conditions (pre-employment) if the offence was in no way connected with the employment or if the person has obtained a pardon for the offence. Section 18.2 of the Quebec Charter[2093] in fact prohibits employers from dismissing, refusing to hire or otherwise penalizing a person owing to the mere fact that he was convicted of a penal or criminal offence; if the offence is in no way connected with the employment or if the person has obtained a pardon for the offence.[2094] A slot machine maintenance technician was dismissed because he had admitted being an accomplice to a criminal offence involving fraud.[2095] The employer was found to be using "necessary" information and was therefore well within his rights concerning the dismissal. A woman's application for the position of police officer was refused since she had once pleaded guilty to shoplifting (for which she received a conditional discharge).[2096] In this case, the court found that this information should not have been used by the employer, since it was irrelevant for the position applied for

In France, the Chambre sociale of the Cour de cassation has taken the position that the employer's request to obtain the communication of certain interdictions issued against the employee by his former employer was illegal as it was unrelated to the evaluation of the individual in his capacity of employee and was in no way relevant to evaluate his professional experience or credentials.[2097] The Paris Appeal Court has

---

[2091] CNIL, *Guide* 2010, *supra* note 2031 at 3.

[2092] [2001] 2 R.C.S. 3.

[2093] *Supra* note 2083.

[2094] *Ibid*. at s. 18.2.

[2095] *Syndicat canadien de la fonction publique, section locale 3892 et Société des casinos du Québec Inc.*, [2001] R.J.D.T. 548 (T.A.).

[2096] *Commission des droits de la personne et des droits de la jeunesse c. Montréal (Service de police de la Communauté urbaine de)*, [2002] R.J.Q. 824.

[2097] Cass. civ., 19 January 2010, No. 08-42.519.

also adopted the position that the personal information of teachers (contact information) and students' notations of these teachers collected by the French website Note2be.com were illegal, in part because there was no warranty as to their relevancy.[2098]

This illustrates the challenge that organizations are facing when they want to use information publicly available or found online to make judgments about potential employees (which may be used in decisions harmful to these individuals) since in many cases, this information may be considered as being irrelevant or unnecessary for the intended use and therefore, contrary to DPLs.

3.2.2.3.3. Challenge with the Information Age

The "relevancy" criterion is extremely important in the context of the Information Age and new technologies, in the sense that a lot of information is made available to organizations that would like to use them for various purposes.[2099] With web 2.0, individuals, themselves, disclose and share their personal information with friends or with the public and publish their thoughts, social connections and activities.[2100] The fact that the information is available online also triggers the situation in which information may also be collected without knowledge of individuals, who have no idea how their data will be used. This translates in the fact that an individual may share information on an OSN website and not realize that it could be used to deny him or her a job or admission to college.[2101]

Calo suggests that objective privacy harms may involve the "unanticipated" use of personal information.[2102] In the series of FIPs, one provides that there must be a way for an individual to prevent his or her information obtained for one purpose from being

---

[2098] CA Paris, RG 08/04727, *supra* note 413.

[2099] See section 1.2 entitled "Technological Background Affecting Personal Information" which elaborates on this issue.

[2100] See section 1.2.1.2 entitled "New Ways of Using the Internet: Web 2.0" which elaborates on this issue.

[2101] A 2009 study showed that 45 percent of employers surveyed used OSNs to evaluate potential employees. See Wortham, *supra* note 1979. A more recent study commissioned by Microsoft found that 70 percent of human resource professionals surveyed have turned down a potential job application based solely on online reputation information. See CrossTab, *Online Reputation*, *supra* note 1979.

[2102] Calo, "The Boundaries", *supra* note 443 at 21.

used or made available for other purposes without his or her consent. This principle, known as the "purpose specification" principle, has been embodied in various DPLs including Canadian and French DPLs.[2103] A so-called "secondary use" is the use of data for purposes unrelated to the purposes for which the data was initially collected, and without the data subject's consent. Supposing someone provides an email address for the purpose of participating in an online forum. If an organization then collects the email address and uses it for a different purpose than to allow this user to participate in the forum (such as marketing to this user) then we can refer to this as a "secondary use". Solove states that there are certainly many desirable instances of secondary use,[2104] but that secondary uses can cause problems and create a dignitary harm, as it involves using information in ways to which a person does not consent and might not find desirable.[2105] He articulates the view that secondary use resembles breach of confidentiality, in that there is a betrayal of the person's expectations when initially giving out information.[2106] The concern of having data used for a new and unrelated purpose of the collection of data is not a new one. As early as 1972, the fact that computers would have the capacity of identifying persons of a particular ethnic group in a particular area, and to incorporate this information with previous information (perhaps about criminal convictions) was already seen as infringing the principle that information collected for one purpose should not be available for any other purpose.[2107]

At the same time, certain DPLs allow for organizations to use publicly available information or information that individuals have themselves made public (since this

---

[2103] See PIPEDA, *supra* note 63 at principle 4.2.4; In Europe, this principle is partially embodied in article 6(1)(b) of the Directive 95/46/EC which, among others, prohibits a further processing which is incompatible with the purpose(s) of the collection. Pursuant to Article 7 of the Directive 95/46/EC, personal data may be processed only if such processing can be based on one of the grounds for legitimize data processing.

[2104] Since it might be used to stop a crime or to save a life and that the variety of possible secondary uses of data range from benign to malignant. See Solove, "A taxonomy", *supra* note 339 at 519.

[2105] *Ibid*. at 520: "Secondary uses thwart people's expectations about how the data they give out will be used. People might not give out data if they know about a potential secondary use, such as for telemarketing, spam, or other forms of intrusive advertising. Fingerprints of United States military recruits originally collected to screen their backgrounds were sent to the FBI and incorporated into the FBI's criminal fingerprint database. Such individuals may not have expected nor desired to have their fingerprints maintained in a law enforcement database of convicts and criminals."

[2106] *Ibid*.

[2107] *Report of the Committee on Privacy*, *supra* note 3 at 180, para. 582.

information is excluded from the application of the law).[2108] To complicate things even more, certain DPLs also have various "reasonableness" or "legitimacy" tests, which are very subjective.[2109]

I have an issue with the choice and consent model in the context of having organizations use information in a harmful way (in which case, under the proposed approach, the data would be considered as *personal information*). First, I maintain that it is strange to request individuals to "consent" to having their information used against them. Second, one could make the argument that the individual doesn't have a "real choice" if the request for information is linked with their wish to obtain employment, financing, insurance, or other services.[2110] Third, with new types of business models that provide free products or services in exchange for personal information,[2111] organizations can claim that consent may have been obtained; although individuals may still not appreciate the value that they are obtaining in exchange for their data.[2112] As a matter of fact, this "relevance" (or "necessity") criterion is so important when the information is in fact "used", that certain DPLs, such as the Quebec DPL, have even

[2108] See section 3.1.2.2.3(a)(i) entitled "Publicly Available Information" and section 3.1.2.2.3(a)(ii) entitled "Data Made Available by the Individual" which elaborate on this issue.

[2109] See section 2.2.1.3.2(a)(i) entitled "Reasonableness or Legitimacy Tests" which elaborates on this issue. See also Dolin, *supra* note 371 at 156: "The aforementioned grounds include, for example, that the user has "unambiguously given his consent," or that the processing is "necessary for the purposes of the *legitimate interests* pursued by the controller." This begs the question – what constitutes such legitimate interests? How broadly or narrowly are they interpreted, who should decide, and what is an appropriate doctrinal basis for answering these questions?"

[2110] I have also already discussed in section 2.1.1.2 entitled "Notice and Choice Approach Challenged" how the notice and choice model is challenged with the volume of data available on the Internet, and with the number of "consents" provided by individuals for various uses that they have not anticipated. With the volume of consents provided by individuals every day for various purposes and the evidence that more than often these individuals consent without being aware of what they are consenting to, whether the proper consent has or has not been obtained for a specific use may be difficult to assess.

[2111] See section 1.2.4.1 entitled "New Business Models (Customization and Sponsored Services)" which elaborates on this issue.

[2112] See section 2.1.1.2.1(a) entitled "Policies are Overly Vague" which elaborates on this issue. Van den Hoven believes that consumers do not always know what the implications are of what they are consenting to when they sign a contract for the use of identity-relevant information, that we cannot assume that the conditions of the developing market for identity-relevant information guarantees fair transactions by independent standards and that constraints on the flow of personal data need to be put in place in order to guarantee equality of arms, transparency, and a fair market for identity-relevant information as a new commodity. See Van den Hoven, "Information Technology", *supra* note 642 at 312-13; Solove articulates the view that even with privacy policies stating that information might be used in secondary ways, people often do not read or understand these policies. Nor can they appropriately make an informed decision about secondary uses since they might have little idea about the range of potential uses. See also Solove, "A taxonomy", *supra* note 339 at 520.

gone as far as prohibiting the "use" of irrelevant or unnecessary information even if the individual consents to such use.[2113]

In certain cases, certain pieces of data may end up in the hands of an organization without any effort or solicitation on the part of the organization, or even in the absence of any fault from this organization.[2114] It may not be clear whether this data may be used by the organization, if it otherwise complies with the "accuracy" and "relevancy" tests.[2115]

(a) Data Relevant but Obtained in Breach of DPLs

In certain cases, information can be made available to certain organizations in breach of DPLs (without the individual's prior consent). Perhaps a distinction should be made between the organization that committed a fault or illegally accessed the information vs. the organization that happened upon the data, without doing anything wrong; such as in the context of a third party security breach or by having a third party disclose this information without the individual's prior consent. If the information is "relevant" for a certain intended use (and "accurate"), it is not clear if the organization can use this information without prior consent of the relevant individual.

To illustrate this point, I will refer to a recent decision rendered by the Federal Court of Canada, which I discuss further in section 3.1.2.1.2(b). In *Stevens v. SNF Maritime Metal Inc.,*[2116] an employee of a company that collected and recycled scrap metal was tasked with delivering the scrap metal to a buyer. He opened a personal account with the buyer and had the proceeds of any delivery credited to his own personal account as opposed to his employer's. The buyer disclosed Stevens' personal account

---

[2113] In Quebec, in *Laval*, *supra* note 2018, Justice Filion of the Court of Québec held that the "necessity" criterion cannot be "overridden" by the individual's consent. Even if one consents to the collection of personal information, the criterion that this information be "necessary" to maintain in a specific file or record must still be demonstrated. In the absence of an express exception, both necessity and consent apply as cumulative conditions for the collection or use of personal information. See *Tremblay*, *supra* note 1967; see also *Julien*, *supra* note 1302; *A. v. C.*, *supra* note 1302; *Agyemang v. Ipex Inc.*, [2001] C.A.I. 201.

[2114] If the organization breached the law to have access to certain information, then the situation should be different. This issue is further discussed in section 3.2.2.3.3(a) below.

[2115] See section 3.2.2.2 and section 3.2.2.3 which detail these tests.

[2116] *Supra* note 599.

information to his employer who then fired him. The plaintiff did not argue that his employer "used" information obtained illegally, without his prior consent. Perhaps he did not argue this, because the information disclosed to the employer was in fact "relevant" for the decision of the employer: the information disclosed to the employer by the buyer provided evidence to the employer that its employee had been stealing from him. The court never took into consideration the fact that information disclosed "illegally" to the employer had then been used to dismiss the employee Stevens. Perhaps things would have been different if the employer was the party who had breached the law by illegally accessing his employee's account, in which case the employer may have had more difficulty using the information if it was acting in breach of DPLs when accessing the information in the first place. This simply illustrates the kind of challenges that we are facing in light of the amount of data currently available, and the fact that organizations may wish to use the data which they have access to, and which may be relevant for the intended use.

(b) Using Relevant Data Publicly Available Without Consent

Nowadays, as we have already seen, there is more and more information becoming available to us.[2117] With new technologies, for instance, facial recognition technology, even more data will become available, potentially publicly, with the potential that this information be "used" against the individual to which they pertain to, as illustrated as follows:

> "The figures above don't even count the fact that some forms of advocacy corporate surveillance would increase in a world with easy facial recognition. Why would anti-abortion groups not photograph every person who walks into an abortion clinic, use facial recognition to identify them, and use public name-and-address databases (see below) to target mailings (or harassment) to each person's home? Why would anti-gay advocates not do the same for people who frequent gay bars, or liberals target "Tea Party" activists, or statists target libertarians, etc? Or insurance companies outside bars to monitor drinking and driving, smoking, or any other risk factor that could increase rates? What does this mean for privacy? (…) Should it be a privacy tort to publicly identify private citizens by name if they are walking into an abortion clinic, a gay

[2117] See section 1.2.1 entitled "Increase in Volume of Information" which elaborates on this issue.

> bar, a Tea Party rally, a divorce lawyer's office, a police station (to "snitch"), or a substance abuse treatment facility? (…)"[2118]

Van den Hoeven, who proposes a classification of four types of harm that may arise in the context of organizations using personal information, refers to one of these types of harm as "Information Injustice".[2119] This type of harm would take place where information presented in one context, is used in another. Already back in 1973, certain authors had articulated their concern that data may be used "outside of their appropriate context".[2120]

A good example would be where prospective employers are searching OSNs for personal information on job candidates, or lenders using OSNs such as Facebook and Twitter to gather information about borrowers or potential ones. Data found on OSNs or on the web may be relevant for organizations making a decision (offering employment, granting a loan, etc.) that could have an impact on the life of the individual.

A main issue or concern is whether the information made available in one context (or sphere) may be used in another. The PIAC has warned that consumer tracking, profiling and data mining threatens the consumer's ability to control the flow of their personal information, as the privacy implications change from one social context to another.[2121] Likewise, van den Hoven believes that while many people do not object to the "use" of their personal medical data for medical purposes, they will however object for understandable reasons to being "disadvantaged socio-economically, discriminated against on the work floor, refused services, denied benefits, or turned down for insurance coverage" on the basis of their medical records, since these records were created to cure them from diseases. He states:

[2118] Thompson, *supra* note 257.

[2119] See generally, Van den Hoven, "Information Technology", *supra* note 642 at 311.

[2120] U.S. Department of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *supra* note 57 at s. IV: "Poorly conceived data collection can result in various kinds of injury to individuals. As observed earlier, any file of personal data is a potential source of harm to individuals when it is used outside its appropriate context, and much of the personal data in administrative files either is a public record or is vulnerable to legal process."

[2121] PIAC, *supra* note 448 at 9-10.

> "The type of injustice I would like to draw your attention to here comes into existence when certain distinctions and associated information (the use of which may be perfectly unobjectionable in one sphere) carry over into another sphere. If difference in health status would be allowed to determine one's educational opportunities, or one's socio-economic achievements (that is information about them) would lead to preferential treatment in the legal setting, or political offices (information about the fact that someone holds them) would advance your entrepreneurial opportunities, and family relations (the fact that you are known to be the presidents nephew) would determine eligibility for political office, these would be perceived as injustices, because of the fact that distinctions - information about properties and qualities in one sphere - are imported into another one. This is an important aspect of what people fear when they object to their data being made available without their informed consent."[2122]

Certain authors have provided guidance on this issue. For instance, Nissenbaum in her article entitled "Privacy as Contextual Integrity" posits a new construct, "contextual integrity," as an alternative benchmark for privacy, to capture the nature of challenges posed by information technologies.[2123] Contextual integrity ties adequate protection for privacy to norms of specific contexts, demanding that information gathering and dissemination be appropriate to that context and obey the governing norms of distribution within it. Building on the idea of "spheres of justice," developed by political philosopher Michael Walzer, Nissenbaum's article argues that certain activities (such as public surveillance) may violate a right to privacy because it violates contextual integrity:

> "Contexts, or spheres, offer a platform for a normative account of privacy in terms of contextual integrity. As mentioned before, contexts are partly constituted by norms, which determine and govern key aspects such as roles, expectations, behaviors, and limits. There are numerous possible sources of contextual norms, including history, culture, law, convention, etc. Among the norms present in most contexts are ones that govern information, and, most relevant to our discussion, information about the people involved in the contexts. I posit two types of informational norms: norms of appropriateness, and norms of flow or distribution. Contextual integrity is maintained when both types of norms are upheld, and it is violated when either of the norms is violated. The central thesis of this Article is that the benchmark of privacy is contextual integrity; that in any given situation, a complaint that privacy

[2122] Van den Hoven, "Moral Wrong-doing", *supra* note 272 at 35-36.

[2123] Nissenbaum, *supra* note 230 at 119.

> has been violated is sound in the event that one or the other types of the informational norms has been transgressed."[2124]

Nissenbaum refers to Ferdinand Schoeman ("Schoeman"), a philosopher who has offered a deep and subtle account of privacy and its value to humans when he writes, "[p]eople have, and it is important that they maintain, different relationships with different people."[2125] She provides the example of an individual who may be active in the gay pride movement in San Francisco, but be private about his or her sexual preferences vis-à-vis his or her family and coworkers in Sacramento. Another example could be a professor who may be highly visible to other gays at the gay bar but discreet about sexual orientation at the university. Does appearing in some public settings as a gay activist, Nissembaum asks, mean that the individual concerned has waived his or her rights to civil inattention, to feeling violated if confronted in another setting?[2126] She suggests that these cases illustrate Schoeman's sense that appropriating information from one situation and inserting it in another can constitute a violation and that violations of this type are captured with the concept of appropriateness.[2127]

As for consumer profiling and data mining, Nissenbaum suggests that the crucial issue is not whether the information is private or public, gathered from private or public settings, but "whether the action breaches contextual integrity". She mentions that the use of credit cards and the emergence of information brokers have altered patterns of availability and flow in well-known ways.[2128] While it is integral to the transaction between a merchant and a customer that the merchant would get to know what a customer purchased (for purposes of managing inventory, etc.) things may be different if the merchant bombards shoppers with questions about other lifestyle choices as this

---

[2124] *Ibid*. at 137-38 □footnotes omitted□

[2125] Ferdinand David Schoeman, "Privacy and Intimate Information" in Ferdinand David Schoeman, ed., *Philosophical Dimensions of Privacy* (New York: Cambridge University Press, 1984) at 403, 408, discussed in Nissenbaum, *supra* note 230 at 140.

[2126] Ferdinand David Schoeman, "Gossip and Privacy" in Robert F. Goodman & Aaron Ben-Ze'ev, eds., *Good Gossip* (Lawrence: University Press of Kansas, 1994) 72 at 73, discussed in Nissenbaum, *supra* note 230 at 139-40.

[2127] *Ibid*.

[2128] *Ibid*. at 152-53: "Although the online bookseller Amazon.com maintains and analyzes customer records electronically, using this information as a basis for marketing to those same customers seems not to be a significant departure from entrenched norms of appropriateness and flow."

would breach norms of appropriateness. According to Nissenbaum, a merchant who provides information about grocery purchases to vendors of magazine subscriptions or information brokers like Seisint and Axciom would be responsible not only for breaches of norms of appropriateness, but also norms of flow.[2129]

I maintain that if public or available information is not used in such a way as to create an objective harm on the individual (section 3.2.1.2), then there is no issue for an organization using the information. But, if public or available information is used in such a way which may trigger an objective harm for the individual, then the information will be subject to the relevant DPLs, meaning that the information shall be of "quality" and "relevant" for the intended purpose, and the individual should be informed of, and consent to, such new use.[2130]

In the next section, I will provide practical examples/applications of the proposed approach, with a focus on assessing if there is an objective harm that may result from the use of personal information.

3.2.3. Objective Harm: Applying the Approach to Business Cases

Under the proposed approach detailed in section 3 of this thesis, new types of data would be treated in accordance with the *risk of harm* that they may trigger, while first taking into account the data handling activity at stake. Section 3.1.2.2 discusses the test to follow to determine if certain information "disclosed" triggers a risk of subjective harm, while section 3.2.1 discusses the fact that information should be governed by DPLs if it is used in such a way which will trigger an objective harm to individuals.

If this information is used in such a way that there is no impact for the individual concerned or that the impact is positive, then the information should not be governed by the relevant DPL (i.e. no disclosure and consent necessary, no need to provide access to this information, etc.). On the other hand, if this information is used in a way which may have a negative impact on the individual (objective harm), then the data

---

[2129] *Ibid*.

[2130] Still, van den Hoven and Nissenbaum each raise an interesting point when they discuss blocking information exchanges between different spheres and proposing "contextual integrity" as a benchmark for privacy breaches, which we may wish to further explore.

should be governed by the relevant DPL (and therefore, notice and consent would be necessary). If the data will be used in a negative impactful way, it will also have to comply with the data "accuracy" test[2131] and the "relevancy" test.[2132] I will illustrate how the proposed approach would work in practice, first by applying the approach to new types of data, then, to recent types of online practices.

3.2.3.1. Objective Harm Test Applied to New Types of Data

I will discuss whether new types of data, such as IP addresses, log files, information collected by cookies, search queries, RFID tags and location information should qualify as *personal information* using the proposed approach.

3.2.3.1.1. IP addresses, Log files, Cookies

Organizations active in the online space are collecting new types of data and using new types of collection tools and using the data collected for various purposes.[2133] I maintain that the purpose behind the use will determine if the information used qualifies as *personal information* and is therefore governed by DPLs.

Information, such as IP addresses or cookies may be used in such a way as to create no impact for individuals (or a positive impact). For example, the information may be collected and used to improve user experience on the website; for instance to remember what is in the user's shopping cart or to remember the language of preference etc. In such situations, the data should not be governed by DPLs. On the other hand, if the information will be used to reduce the type of discounts that an individual (or a web profile) may receive, the data should be governed by the relevant DPL and therefore, it may be necessary, for the organization using the data, to disclose this practice and obtain prior consent. The organization would also have to comply with the data "accuracy" and "relevancy" tests.

[2131] See section 3.2.2.2 which elaborates on this test.

[2132] See section 3.2.2.3 which elaborates on this test.

[2133] See section 1.2.2 entitled "New Types of Information and Collection Tools" and section 1.2.4 which elaborate on this issue.

Nowadays, many organizations create profiles which may or may not be governed by DPLs.[2134] A concern usually arises when a decision is taken towards a profile, which may be harmful for the individual behind the profile.[2135] The issue, then, is to determine how a profile is in fact used. If the profile is used by the organization to determine which web pages to present to the user (in the right language, etc.), then it may not have a negative impact for the individual. If the profile information is used to present personalized advertising which takes into account prior searches or purchase history from this specific user (instead of random advertising), then it could also be arguable that there would be no objective harm and that the information would not be subject to DPLs, subject to the concerns which are raised in section 3.2.3.2.2. If a certain profile will be used to categorize this individual and the individual will be refused certain services based on his or her profile, then the use would trigger an objective harm (since the impact would be a negative one). The user should promptly be made aware of the information use, in order to be in a position to consent to such collection and use and be in a position to determine whether the information used by the organization complies with the data "quality" or "relevancy" tests.

3.2.3.1.2. Search Queries

Search engines allow web users to find information pertaining to the topic that they are searching. Search queries may be useful for various potential uses other than simply processing the individual's search request. Some of these uses may have a positive impact for the individual, a negative impact (objective harm), or no impact whatsoever.

First, search queries may be used in such a way that may create a negative impact (objective harm) for the individual. For example, an insurance company could have the intention to raise insurance premiums by 5% upon finding out that a certain individual has researched a number of books on a particular type of cancer. Since this would constitute a use triggering an objective harm for the individual, the data used in this context would be governed by the relevant DPL. This means that the insurance company would have to inform the user of this use, the consent of the individual prior

[2134] See section 2.1.2.1.2(a) entitled "Data not Identifying but Impacting on Individuals" which elaborates on this issue.

[2135] Clarke, "Profiling", *supra* note 622.

to such use would be necessary and the data used would have to comply with the "accuracy" and the "relevancy" tests discussed in section 3.2.2.2 and 3.2.2.3 respectively.[2136]

Search engines may collect and use search query data for purposes which may benefit individuals. A registered search history may be used to reduce irrelevant advertising, it can help differentiate ambiguous terms on an individual basis (e.g., jaguar – car vs. cat); help with personalized spell corrections and term substitution; indicate which languages someone has used (football vs. soccer); and aid in determining appropriate levels of filtering for profanity (sexual content, etc).[2137] Google mentions that it is collecting search queries for various purposes, including keeping their services secure,[2138] their users safe from *malware* or *phishing* attacks,[2139] and to detect and prevent advertising "click fraud".[2140] All of these uses could be considered as having a potentially positive impact for an individual, as they would improve the user's experience, increase the effectiveness of his or her web search and protect him or her against certain unwanted viruses or content.[2141] These types of uses being harmless to individuals, I maintain that search query information strictly used for these purposes should not be governed by the relevant DPLs.[2142]

[2136] It is unlikely that the search query data used for this purpose would found to comply with these data quality and relevancy tests.

[2137] Dolin, *supra* note 371 at 142.

[2138] For instance, Google claims that it needs users data for improving security and fighting webspam. Web spam is junk that the user sees in search results when websites successfully cheat their way into higher positions in search results or otherwise violate search engine quality guidelines. See Cutts, *supra* note 388.

[2139] Provos, *supra* note 389.

[2140] For example, services such as clicks on sponsored links, where there is a contractual and accounting obligation to retain data, this data would be useful at least until invoices are paid and the period for legal disputes has expired. See Article 29 Data Protection Working Party, *Opinion 1/2008*, *supra* note 207 at 15-16.

[2141] Unless we consider that personalized advertising may instead create a negative impact for the individual as it may reduce the choices offered to the individual. See section 3.2.1.2.2(d) entitled "Behavioral Marketing" which elaborates on this issue.

[2142] Although if the information collected by the search engine creates a risk of subjective harm upon being disclosed, for instance in the context of a security breach (as per the test detailed in section 3.1.2.2 entitled "Risk of Subjective Harm: Revisiting the Sensitivity Criteria"), then the information collected would be considered as *personal information*. This translates into individuals having to be made aware that the search engine is collecting and storing this information which is of an "intimate" nature, not "available" and "identifiable", and agreeing to such collection and storage.

Search query data may also be used for purposes which may have no impact for individuals. For instance, this kind of data may be used by search engines to improve their search algorithms and the quality of their search services.[2143] In such cases, search engine data would be used to provide knowledge for the organization, and potentially, such uses would have no direct impact for individuals. An example illustrating how search engine data may be used is with Google Flu Trends, a service provided by Google, which furthers early detection of influenza epidemics throughout the world by monitoring health-seeking behavior, specifically the online web search queries that millions of individuals submit to the Google search engine each day. I maintain that the use of search queries for the purpose of providing this kind of service has no negative impact for individuals (potentially no impact and perhaps even a positive one) and that therefore, search queries used for this purpose should not be subject to the DPL's requirements of obtaining the prior consent of individuals.

This being said, in certain situations, the data collected for such purposes, while it may not create a risk of objective harm for individuals, it may create a risk of subjective harm upon this data being disclosed.[2144] As a matter of fact, in accordance with the test proposed in section 3.1.2.2, if the information is of an "intimate" nature, it was not previously "available" and it is "identifiable", then search query data may be subject to the application of the relevant DPL.

3.2.3.1.3. RFID and Location Information

RFID tags may be used by organizations in a variety of ways. In some instances, the use may create a positive impact for the individuals concerned, while other uses may create a negative impact or have no impact whatsoever for individuals.

[2143] Varian, *supra* note 387; For more details see Shuman Ghosemajumder, "Using data to help prevent fraud" (18 March 2008), online: Google Blog <http://googleblog.blogspot.com/2008/03/using-data-to-help-prevent-fraud.html>; Provos, *supra* note 389.

[2144] This risk of subjective harm is further illustrated by the AOL breach discussed in section 1.2.1.3 entitled "Easier Identification of Individuals". See also Schwartz & Solove, *supra* note 529 at 1882-83: "When one clicks on Google Flu Trends, there is only high level information that is safely aggregated. Identifiable information is capable of identification, even if this risk is not significantly probable. Thus, companies cannot merely release it or allow unmonitored access to it. Depending on the kind of potential harm to individuals and the likely threat model, companies should also be required to use a 'track and audit' model for some identifiable information. An example would be information used in health care research. Access to such data should be accompanied by obligations that travel with the information."

In the event that retailers use RFID tags with the goal of simply controlling in-store inventory, then this data would not be subject to the relevant DPL since this use creates no impact for individuals.[2145]

Certain retailers may use RFID tags to track customers in order to take certain decisions which will have a potential impact on the individual. In such cases, there is the possibility for a chain of grocery stores to give out tagged devices to customers (e.g., like tokens) enabling the operation of shopping carts, which customers re-use each time they visit the store. This mechanism would enable stores to monitor which products an individual (identified by the token) purchases, how often such products are used and in which of the chain grocery stores the consumer buys them. The store could then make inferred assumptions about an individual's income, health, lifestyle, buying habits etc., which profile information could then be used for taking various decisions.

This information pertaining to the RFID tag may, for instance, be used for personalized marketing purposes. In such case, the information used would have an impact on the individual, but potentially a positive one (if something is "given" to the individual), unless we take the position that the direct advertising may have a negative impact (be harmful) on individuals because it may limit its choices (in which case the data would be subject to the relevant DPL).[2146] This information may also be used for purposes of dynamic pricing[2147] in which case it would be subject to the relevant DPL (the individual would have to be informed of this use and consent to it, etc.) since the use would be

[2145] The organization which is handling this data would still have to determine if there would be a risk of subjective harm upon this information being disclosed as per the test detailed in section 3.1.2.2 entitled "Risk of Subjective Harm: Revisiting the Sensitivity Criteria", in order to determine if it is subject to the application of the relevant DPL. If there is such risk of subjective harm, it would have to adopt the proper security measures and other obligations provided by DPLs (notice and choice) would have to be complied with. See Hariton, Lawford & Palihapitiya, *supra* note 197 at 4: "Retailers with more modest goals of controlling in-store inventory, rather than tracking customers will face less rigour in informing customers of RFID use. But, they will still be required as a matter of course to 'kill' RFID tags at the point-of sale or undertake encryption or similar technological measures to safeguard the personal information of their shoppers from third party interception post-sales."

[2146] See section 3.2.1.2.2(d) and section 3.2.3.2.2 which elaborate on how according to some direct marketing may be harmful to individuals.

[2147] See section 3.2.1.2.2(a) entitled "Adaptive Pricing" which elaborates on dynamic pricing.

harmful. This information would then also have to pass the "accuracy" and "relevancy" tests discussed in sections 3.2.2.2 and 3.2.2.3 respectively.

Location information may be collected using various methods, and for different purposes.[2148] Organizations managing trucks or taxis may use location tracking technology to track their vehicles strictly for fleet management purposes. In such cases, since this use triggers no impact for individuals, this information should not be considered *personal information* governed by DPLs.[2149] An organization may also track the location of a vehicle for security purposes (knowing that a certain truck containing valuable merchandise is at a given location). Information used for this purpose would also not be governed by DPLs, since it may have no impact for the individual (or even potentially a positive impact, i.e. for the security of the driver).[2150] In the event that the location data is used to evaluate an employee (such as the driver of a taxi or a truck) and to potentially reprimand this employee, then the information would be subject to the relevant DPL as this use of information may trigger a risk of objective harm. This means that employees would have to be informed of this collection and use, and consent to it, and the location information would have to be "accurate" and "relevant" for the intended use.[2151]

3.2.3.2. Objective Harm Test Applied to Different Types of Uses

I maintain that the type of use which will be made of the information should be useful in determining whether the information at stake qualifies as *personal information*. I will discuss three types of uses of information: email marketing, behavioural marketing and analytics.

[2148] Gratton, *Internet and Wireless Privacy*, *supra* note 193 at 24-29.

[2149] Again, if the data, upon being "disclosed", may create a risk of subjective harm, then it would be governed by the relevant DPL and notice would have to be provided to the relevant individuals, consent would have to be obtained, etc.

[2150] Subject to the subjective harm test discussed in section 3.1.2.2 entitled "Risk of Subjective Harm: Revisiting the Sensitivity Criteria".

[2151] See section 3.2.2.2.1(a) entitled "The Higher the Risk of Harm, the More important the Accuracy" which elaborates on the quality of location data depending on the intended use for this data.

3.2.3.2.1. Email marketing

Back in the early 1970s, some organizations argued that the exchange of mailing and customer lists, and the uses made of such lists in direct marketing, were legitimate commercial practices which should not be restricted, and that "any restriction on sources of information available to the industry would result in a lower rate of response from mailing shots, with a consequent rise in costs which would be passed on in higher prices to the consumer."[2152] In the U.K., the Younger Committee had even declared that the sending of unsolicited advertising was an unobjectionable practice and that they did not think that new legislative safeguards were warranted at that time.[2153] The Lindop Report (U.K., 1978) mentioned that "The BDMMA told us that the use of computers in direct marketing is aimed at achieving perfect targeting with consequent economic benefits for industry and the consumer and that the proposed legislation should not inhibit the proper use of computers to this end."[2154] Still, when DPLs were discussed in the early 1970s, the fact that direct marketing (at that point, marketing by mail) raised special issues, including potential intrusion, was already of concern.[2155]

Many organizations may wish to use email marketing in order to promote their products and services. Calo argues that "We tend to think of unsolicited spam email as a privacy harm, for instance, and federal law regulates it in part on this basis".[2156] Unless the marketing messages are fraudulent, individuals may have a hard time sustaining that they are suffering a risk of objective harm, since in many cases, through the marketing message, something is being "offered" to them, nothing is necessarily "taken" from them unless we consider the fact that they are paying somehow for the content received (including the time spent reading, sorting and deleting the messages).[2157]

[2152] Lindop, *supra* note 96 at 140, para. 17.08.

[2153] *Ibid*. at 141, para. 17.11.

[2154] *Ibid*. at 142, para. 17.14.

[2155] *Ibid*. at 139, para. 17.03.

[2156] *Can-Spam Act*, *supra* note 1886; See also Calo, "The Boundaries", *supra* note 443 at 9.

[2157] One could claim that if individuals that receive marketing messages are not interested in the content of these messages, they can simply ignore the messages or delete them, but I suggest that there may be some type of financial harm surrounging spam practices, for consumers, for ISPs and even for employers. See Gratton, "Unsolicited Commercial Emails", *supra* note 1887 at 4: "A recent survey also revealed that consumers feel that spam is costing them time and money. The time-consuming process of deleting the unsolicited e-mails is added to the time taken to download spam. Furthermore, Internet users that have e-

Many jurisdictions have adopted anti-spam regulations to address these kinds of uses.[2158] Canadian policy on spam was initially articulated in 1999 in an online policy document from Industry Canada's electronic commerce branch.[2159] Industry Canada initially suggested that specific anti-spam legislation was not needed given that spam could in some cases be fought by existing laws such as the *Criminal Code*, the *Telecommunications Act* and PIPEDA.[2160] This changed in 2003, when Industry Canada realized the type of damages that email marketing could be causing to the organizations, creating harm on a larger scale (beyond being harmful for individuals), imposing costs to organizations and ISPs as well.[2161]

I maintain that this is an example under which DPLs may not be effective, because the risk of objective harm to individuals is not so clear (cut and dry) in this situation.[2162] Practices pertaining to direct marketing online or behavioral marketing raise other issues, which are discussed next.

3.2.3.2.2. Behavioural Advertising

I already discuss behavioral marketing under section 1.2.4.1. In section 3.1.2.3.1, I discuss how this kind of practice may prove to create a risk of subjective harm. I will now discuss whether this practice may create an objective kind of harm.

---

mail wireless devices that bill them based on the amount of data they download actually pay to receive spam. Certain users have limits on the amount of e-mail their ESP will hold. Spam can often mean a full mailbox, with the result of having desirable e-mails getting rejected. There are many other costs that ISPs and other businesses have to bear due to spam such as: bandwidth and network costs, downtime attributable to spam overload, clogging of computer servers of ISPs, and productivity cost to businesses caused by time taken by employees to open, read, and respond to such messages."

[2158] In Europe, spam is regulated by the EC, *Directive 2002/58/EC*, *supra* note 860; In the U.S., the *Can-Spam Act*, *supra* note 1886 regulates spam. In Canada, spam will be regulated by the CASL which will be coming in force in 2012. See Industry Canada, "Electronic Commerce in Canada", *supra* note 1886.

[2159] Industry Canada, The Working Group on Consumers and Electronic Commerce, "Internet and Bulk Unsolicited Electronic Mail" (SPAM), July 1999.

[2160] Industry Canada, The Working Group on Consumers and Electronic Commerce, "E-mail marketing: Consumer Choices and Business Opportunities", Discussion Paper, January 2003.

[2161] With the significant rise in the volume of junk e-mail experienced in 2000 and 2001, it published in January 2003 another discussion paper entitled *E-mail marketing: Consumer Choices and Business Opportunities* that raises different discussion points on the responsibility of ISPs, the value and role of filtering technologies and anti-spam policies, and the role of governments.

[2162] Also, certain email addresses may not qualify under the definition of *personal information* if they don't identify an individual. See Trudel, Abran & Dupuis, *supra* note 212 at 55.

The Article 29 Working Party suggests that there are two main approaches to building user profiles which can be combined. First, predictive profiles are established by inference from observing individual and collective user behaviour over time, particularly by monitoring visited pages and ads viewed or clicked on. Second, explicit profiles are created from personal information that data subjects themselves provide to a web service, such as by registering.[2163]

On the Internet, many industry players are claiming that online behavioural targeted advertising, online consumer tracking and profiling are intended to benefit to the online users. Proponents of online behavioural targeted advertising and consumer tracking often boast benefits to the online consumer, such as customized settings or product recommendations (personalised advertising) based on the consumer's previous purchases or tastes. Marketers may also argue that behavioural advertising provides a benefit to the consumer, resulting in increased efficiencies and increased social welfare.[2164]

Some raise that in the context of the Internet and the collection of information by online retailers or marketers: "there are no adverse consequences from data collection, except for greater volume of junk mail".[2165] In the U.S., the FTC staff also observed that targeted online ads may in fact, to a certain extent, benefit consumers.[2166]

But this issue is not black or white. Proponents of the fact that these practices benefit consumers may be tempted to argue that the analysis stops here. But many don't agree and believe that such practices may in fact have a negative impact on

---

[2163] Article 29 Data Protection Working Party, *Opinion 2/*2010, *supra* note 191 at 7. Additionally, predictive profiles may be made explicit at a later time, when a data subject creates login credentials for a website. Some ad networks allow registered users to view and edit their associated predictive profiles, at least to a certain degree.

[2164] PIAC, *supra* note 448 at 9-10.

[2165] Karas, *supra* note 362 at 18.

[2166] *See* Federal Trade Commission, "Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles" (20 December 2007), online: FTC <http://www.ftc.gov/opa/2007/12/principles.shtm>: "[B]ehavioral advertising provides benefits to consumers in the form of free web content and personalized ads that many consumers value."

individuals.[2167] If this use may create a negative impact for individuals, then one concern is that data mining used for the behavioral marketing purposes may not always be "accurate" information about individuals.[2168] Where errors are collected and become part of a consumer's profile, targeted online advertisements may be based on these errors and negatively affect the user's online experience.[2169]

Certain recent studies also suggest that a majority of consumers find online targeting activities problematic.[2170] In Canada, the OPCC has recently stated: "Online behavioural advertising may be considered a reasonable purpose under (…) PIPEDA, provided it is carried out under certain parameters, and is not made a condition of service."[2171] Similar to direct marketing, some jurisdictions have adopted (or are contemplating adopting) Do-not-track lists[2172] (U.S.), or Behavioral Marketing Guidelines[2173] (Canada).

Calo raises an interesting issue, which relates to online services which may be sponsored by advertising, such as Google Gmail's service. Gmail automatically scans the sender's incoming email and, alongside the offer of sale, Google might display links to bicycles sold by its paid advertisers. In other words, Google in some cases may scan the content of an incoming email and use it, without notice or consent, to compete directly with its author. Calo states: "The harm here may be negligible, but there is no

---

[2167] For instance, the PIAC, while it recognizes that these marketing techniques may improve aspects of the consumer experience, also submit that consumer tracking, profiling and data mining threatens the consumer's ability to control the flow of his or her personal information, as personal information has different privacy implications from one social context to another. See PIAC, *supra* note 448 at 9; In Canada, the Privacy Commissioner of Canada has voiced her position that accepting participation in online behavioural advertising should not be considered a term or condition for individuals to use the Internet generally. See Jennifer Stoddart, "Respecting Privacy Rights in the World of Online Behavioural Advertising" (Remarks delivered at the Marketing and the Law Conference, Toronto, 6 December 2011).

[2168] Lawson, *supra* note 1991 at 7: "Consumers may not realize that there are errors in their profile as they may not be aware of the existence of their consumer profile or they may have difficulty accessing database records in order to correct inaccurate information."

[2169] PIAC, *supra* note 448 at 9-10.

[2170] Joseph Turow et al., "American Reject Tailored Advertising and Three Activities that Enable It" (29 September 2009), online: SSRN <http://ssrn.com/abstract=1478214>, discussed in Calo, "The Boundaries", *supra* note 443 at 23.

[2171] OPCC, *Online Behavioural*, *supra* note 275.

[2172] See FTC, Preliminary Staff Report, *supra* note 372; FTC, *Recommendations* 2012, *supra* note 381.

[2173] OPCC, *Online Behavioural*, *supra* note 275.

basis to rule out even the *theoretical* possibility that this unwanted use of private information against its subject could implicate privacy".[2174] In such case, the use of the personal information of the author's incoming email may be used against that individual's, in order to create some type of economic (and therefore objective) harm. If one takes the position that this practice is potentially harmful to individuals, then the information would qualify as *personal information* and would be subject to the DPLs' consent and other requirements.

In the event that we consider the fact that behavioral marketing may negatively impact the individuals and create an objective harm, then the profile data would qualify as *personal information*, and this also translates into the information having to comply with the "quality" and the "relevancy" tests discussed in sections 3.2.2.2 and 3.2.2.3. The Article 29 Working Party explains how Ad networks construct predictive profiles by using a combination of tracking techniques, cookie based technologies and data mining software and as such, gender and age range can be deduced by analysing the pages the data subject visits and the ads to which he or she gravitates:

> "The profile based on analysis of the cookies stored on the terminal equipment of the data subject can be enriched with aggregated data derived from the behaviour of data subjects who exhibit similar behavioural patterns in other contexts. Online advertising systems often classify data subjects into segments, either by their areas of interest or by their marketing categories (examples are "gardening", "body care", "electronics", etc.)."[2175]

I have already explained how it is debatable whether assumptions made online would qualify as "accurate" data. At the same time, if the type of objective harm is relatively limited, than the level of accuracy is concurrently less important.[2176] If the information, once disclosed, may create a risk of subjective harm, then section 3.1.2.2 elaborates on how to deal with this data.

[2174] Calo, "The Boundaries", *supra* note 443 at 25.

[2175] Article 29 Data Protection Working Party, *Opinion 2/*2010, *supra* note 191 at 7.

[2176] See section 3.2.2.2.1(a) entitled "The Higher the Risk of Harm, the More important the Accuracy" which elaborates on this issue.

3.2.3.2.3. Analytics

I discuss in section 1.2.4.2 entitled "Knowledge, Analytics and Innovation" how analytics, through a series of algorithms, compiles data into aggregate statistics that may provide useful information for an organization. Many websites and online service providers disclose in their privacy policies that they may collect some type of information in order to "improve their websites, products our services".[2177] They wish to collect users' data in order to, using data mining, analytics and similar tools or calculations, capture, analyze and correlate the data in order to uncover hidden patterns in the otherwise raw information. They may be using web analytics tools to analyze their users' surfing behaviour (i.e. amount of website visits, number, duration and kind of websites accessed).

Some claim that the knowledge gained by using information collected for analytic purposes may allow organizations to better market their products or to develop new tools and services. And although analytics may provide certain benefits for an organization, this use may not necessarily have an impact or a direct impact for individuals. For instance, Neuralitic is a mobile analytic organization who owns a technology which will inform mobile operators which wireless devices are the most popular for accessing the Internet, which are the top applications downloaded, the most popular websites, or even the time of day with the most traffic.[2178] This may enable mobile operators to figure out better ways to sell their products. As an example to illustrate this, Star-Hub, a telecommunications provider in Singapore was able to figure out which of its phones, services and media channels were the most popular and market them to the public accordingly after installing Neuralitic's platform into its mobile

[2177] See Microsoft privacy policy, *supra* note 297 which states: "Microsoft collects and uses your personal information to operate and improve its sites and services. These uses may include (…) performing research and analysis aimed at improving our products, services and technologies."; See Google privacy policy, *supra* note 297 which states: "Google only processes personal information for the purposes described in this Privacy Policy (…) such purposes include: (…) protect and improve our services; (…) and Developing new services."; See Yahoo! Privacy Policy, *supra* note 228 which states: "Yahoo! uses information for the following general purposes: to customize the advertising and content you see, (…) improve our services (…)."

[2178] Eric Lam, "Smartphones are smarter than you are" *Financial Post* (31 May 2010), online: The Financial Post.

TV network. A few changes to its brand positioning triggered a jump in its subscriber base from 28% and its average viewing time grew by 16% within a month.[2179]

Foursquare, a location-based social network (which provides a service that allows users to share their location with a group of friends from "checking in" to a restaurant, business or other venue when they arrive), was looking to distributing a free analytics tool and dashboard to give organizations access to a range of information and statistics about visitors to their establishments.[2180] It is not clear from these examples that the use of certain data for analytic purposes have an impact on individuals and it is definitely debatable whether this impact, if there is such impact, is a negative one triggering an objective harm.[2181]

As further discussed in section 1.2.4.2, the knowledge gained by organizations using analytics solutions (and having them better understand the behavior of their users) may in certain cases be translated into direct benefits for consumers (personalized services, products and advertising) or indirect ones (new or upgraded products and services). Using the approach proposed, if the information collected may not be used in a way which may trigger an objective harm for individuals, the information may be used for analytic purposes without being covered by DPLs. The challenge though, will be to determine and extend of what exactly constitutes a "negative impact" for an individual, if, for example, the use of analytics provide the tools for organizations to limit certain services to all clients vs. one or a small group of clients. For example, in one case, latest features were intended to help local merchants run their stores by giving them more information about their customers, in order to provide businesses more retention with current customers and the ability to add new customers with specials.[2182] One

---

[2179] *Ibid*.

[2180] Nick Bilton, "Foursquare Introduces New Tools for Businesses" *The New York Times* (9 March 2010), online: The New York Times <http://bits.blogs.nytimes.com/2010/03/09/foursquare-introduces-new-tools-for-businesses/?partner=rss&emc=rss>.

[2181] See Gratton, "Personalization", *supra* note 16.

[2182] Bilton, *supra* note 2180: "With the new tool, businesses will be able to see a range of real-time data about Foursquare usage, including who has 'checked in' to the place via Foursquare, when they arrived, the male-to-female customer ratio and which times of day are more active for certain customers. Business owners will also be able to offer instant promotions to try to engage new customers and keep current ones. 'If a restaurant can see one of its loyal customers has dropped off the map and is no longer checking in, the owner could offer them incentives to come back,' said Mr. Walker."

could claim that providing only certain customers with specials, may trigger a risk of objective harm for other customers (discrimination). Others may find that similar to targeted advertising, this may end up limiting the various choices which may be offered to consumers. This means that whether information used for analytic purposes is considered *personal information* will depend on the exact use and whether this specific use may create an objective harm for an individual.

This having been said, organizations would also have to adopt the proper security measures to ensure that there is no "disclosure" of the data that they are handling in order to avoid the risk of subjective harm that may arise, for instance if they are handling information which may be harmful upon this information being disclosed.[2183] In the case that the information collected may create a subjective risk of harm, users should be informed of the collection of this data, and consent would be required before collecting this data.

[2183] See section 3.1.2.1.1 entitled "Harm Directly Linked to Disclosure: Subjective (and Psychological)" which elaborates on this issue.

CONCLUSION

What is personal *information*? The answer to this question is crucial because DPLs govern only information that qualifies as *personal.* The fact that certain information is *personal* triggers certain rights for individuals with respect to the processing or handling of information relating to them under DPLs: right to be informed of the collection, use and disclosure of their personal information and right to consent to it - what I refer to as the "notice and choice" approach - access rights to the information to ensure the accuracy of the information, etc. Organizations handling personal information also have certain duties, for instance the obligation to only use accurate information and to ensure the confidentiality and security of this personal information.

I have detailed how the current definition of *personal information* is problematic when using a literal approach to interpreting it and that with new Internet technologies, this definition may be over-inclusive, under-inclusive, may create uncertainties and be obsolete at some levels. I have explained how, instead of using a literal interpretation, we should use a purposive approach to interpreting the notion of *personal information* in order for DPLs to do what they were suppose to do.

While I do have issues with the "notice and choice" model which forms the basis of these FIPs (since individuals may be overloaded with information in quantities that they cannot realistically be expected to process or comprehend, obtaining their valid consent may be impossible in many cases), the goal of this thesis is not to re-open and challenge the notion of privacy as "individuals in control of their personal information". The goals of this thesis is rather to test-drive the current data protection legal framework (DPLs), assess its viability in light of recent Internet and related technologies and propose a guide to interpreting the notion of *personal information* in order to ensure that the information which were meant to be protected by DPLs are in fact considered *personal information*, the remaining of the information being able to free flow in the society.

The ultimate purpose of DPLs was to protect individuals against a *risk of harm* which may take place upon their information being collected, used or disclosed. Therefore, in the approach proposed, I maintain that information should only qualify as *personal* if the information upon being collected, disclosed or used creates such risk. Since each

data handling activity triggers different sets of concerns, I have analyzed them separately, to come to the realization that while certain data handling activities such as the collection and disclosure of information trigger a more subjective kind of harm to individuals, the use of this information usually triggers a more objective kind of harm. In section 3, I propose a decision tree which may be used in determining which data is or should be covered by DPLs and more specifically, what are the risks associated with the collection, use or disclosure of data.

I maintain that information collected creates problems often through its use or disclosure. The collection "per se" or the means by which personal information is gathered is an activity that is not as efficiently regulated by DPLs. Although the collection may increase the risk of harm resulting from the disclosure or use of the personal information, the type of harm that the collection in itself usually triggers is more likely to be associated with some type of psychological harm (such as the "feeling of being under surveillance") or some type of dignitary harm. Since DPLs were not meant to address the first kind of harm (feeling of being under surveillance), and that they have proven to be inadequate in addressing dignitary harm (through the inefficient notice and choice model) I argue that we should focus on the risks of harm which may take place at the "disclosure" and "use" levels. Therefore, upon information being collected, the analysis which should take place in order to determine whether the information collected is *personal*, is whether the information collected may create a *risk of harm* upon being disclosed (for instance in the context of a security breach) or upon being used, in which case it will qualify as *personal information*. This translates in data ***collected*** only having to be disclosed to individuals (and their consent having to be obtained) if the data creates a risk of harm at the "disclosure" or "use" levels.

When the data is to be ***disclosed***, to determine if the data qualifies as *personal information*, the question should not be "is this information relating to an identifiable individual?" Instead, it should be an assessment of whether the disclosure will create a *risk of subjective harm* to the individual. This subjective harm can be assimilated to a feeling of being embarrassed or uncomfortable upon the information being disclosed. I elaborate on why, therefore, the test should be whether the data to be disclosed is of "intimate" nature (the more intimate, the higher the risk of harm), whether the data is "identifiable" (the more identifiable to a unique individual, the higher the risk of harm),

and last, the extent of the "availability" of the data (the less it was previously available prior to the disclosure or the more available it may become post disclosure, the higher the risk of harm). If the data to be disclosed result in very low risk of harm to the individual (the data is not of "intimate" nature, it is not "identifiable" to a unique individual or small group of people, and it is already very widely or publicly "available"), the information should not qualify as *personal information*, and the disclosure of the data would therefore fall outside of the scope of DPLs.

When the data is to be ***used,*** to determine if the data qualifies as *personal information*, the question should not be "is this information relating to an identifiable individual?" Instead, the test to follow would indicate to determine if the data used will have an impact on the individual and if so, a negative one. If there is no impact for an individual or the impact is positive, then I maintain that the data should not qualify as *personal information* and it can be used without further restrictions, as this data was not meant to be covered by DPLs. If there is a negative impact (or what I refer to as an objective harm, such as a financial harm, physical harm or some type of discrimination), then the information would qualify as *personal information* and it would have to be "accurate" and "relevant" for the intended use. If the information is not accurate and relevant, then the data should simply not be used for the purpose intended. The fact that the information *can or can't identify a unique individual* does not need to be taken into account at the use level and may usually not need to be included in the assessment test at that point.

Interestingly, the test which I propose illustrate that the criteria which pertains to the data that are relevant when establishing the *risk of harm* generated by the *use* of certain information (objective harm) are different when establishing the risk of harm generated by the *disclosure* of the information (subjective harm). At the *use* level, in the event that the data "used" will trigger an objective harm on the individual, only the criteria of "accuracy" and "relevancy" are important to assess this risk of harm (the criteria of "availability" of the data, "identifiability" and "intimate" nature of the data are not very important to assess this risk). The picture is flipped when we are assessing the risk of subjective harm at the *disclosure* level. In the event that the data is disclosed, the three criteria which are important to assess this risk are the "availability" of the data, the "identifiability" and the "intimate" nature of the data (the criteria of

"accuracy" and "relevancy" are much less important to assess this risk of subjective harm). The criteria that were relevant in order to assess the risk of harm under the activity of **using** the data are not relevant when assessing the risk of harm under the activity of **disclosing** the data, and vice versa (the criteria that were not relevant in order to assess the risk of harm under the activity of **using** the data are the ones that are in fact relevant when assessing the risk of harm under the activity of **disclosing** the data).

The objective of the present thesis is to come to a common understanding of the notion of *personal information*, the situations in which national DPLs should be applied, and the way it should be applied. Working on a common interpretation of the definition of *personal information* is tantamount to defining what falls inside or outside the scope of DPLs. A corollary of this work is to provide guidance to lawmakers, policymakers, privacy commissioners, courts, organizations handling personal information and individuals assessing whether certain information are or should be governed by the relevant DPLs, depending on whether the data handling activity at stake creates a *risk of harm* for an individual. This will provide for a useful framework under which DPLs remain efficient in light of modern Internet technologies. It may also guide the law toward a more coherent understanding of data protection and privacy and to serve as a framework for the future development of the field of data protection and privacy law.

BIBLIOGRAPHY

LAWS AND REGULATIONS

Constitutional Documents

Canadian Charter of Rights and Freedoms, Part I of the *Constitution Act, 1982*.

Charter of Human Rights and Freedoms, R.S.Q., c. C-12.

Canada (Federal)

Bill C-12*, An Act to amend the Personal Information Protection and Electronic Documents Act*, 1st Sess., 41st Parl., 2011.

Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5.

Regulations Specifying Publicly Available Information, SOR/2001-7 (PIPEDA).

Privacy Act, C. 1980, c. P-21.

Canada (Provincial)

Alberta

Personal Information Protection Act, S.A. 2003, c. P-6.5.

Health Information Act, RSA 2000, c H-5.

British Columbia

Personal Information Protection Act, S.B.C. 2003, c. 63.

Personal Health Information Access and Protection of Privacy Act, SBC 2008, c 38.

Manitoba

Personal Health Information Act, CCSM c P33.5.

New Brunswick

Personal Health Information Privacy and Access Act, SNB 2009, c P-7.05.

Newfoundland and Labrador

Personal Health Information Act, SNL 2008, c P-7.01.

Nova Scotia

Personal Health Information Act, Chapter 41 of the Acts of 2010.

Ontario

Personal Health Information Protection Act, 2004, SO 2004, c 3, Sch A.

Quebec

An Act Respecting the Protection of Personal Information in the Private Sector, R.S.Q. 1993, c. P-39.1.

An Act respecting access to documents held by public bodies and the protection of personal information, R.S.Q., chapter A-2.1.

An Act to establish a legal framework for information technology, RSQ, c. C-1.1.

Civil Code of Quebec, LRQ, c C-1991.

Saskatchewan

Health Information Protection Act, SS 1999, c H-0.021.

France

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, J.O., 7 January 1978, c. 1.

European Union

European Commission

EC, *Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, [1995] OJ, L. 281/31.

EC, *European Parliament and Council Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)***,** [2002] O.J., L 201/37.

EC, *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC*, [2006] O.J., L. 105/54.

European Data Protection Laws (Other than France)

German Federal Data Protection Act, The Federal Ministry of the Interior, January 1, 2002.

Data Protection Act 1998 (UK), c. 29.

Personal Data Protection Act of the Republic of Slovenia, No. 001-22-148/04, Llubljana, 23 July 2004.

Swedish *Personal Data Act* (1998:204).

Loi fédérale sur la protection des données, 235.1, 1992 (Suisse).

United States

Cable Communications Policy Act of 1984, 47 U.S.C. §§ 551(b)-(c) (2000).

California Health and Safety Code § 199.21 (West 1990) (repealed 1995).

California Online Privacy Protection Act, Bus & Prof. Code §§ 22575-22579 (2004).

The CAN-Spam Act of 2003, 15 U.S.C. § 7701.

Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501 – 6506 (Pub.L. 105-277, 112 Stat. 2581-728, enacted October 21, 1998).

Driver's Privacy Protection Act of 1994, 18 U.S.C. §§ 2721-2725 (2000).

Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2510-2522).

Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g(b)(1) (2000).

Gramm-Leach-Bliley Act, Statute (*Public Law* 106-102, 15 U.S.C. § 6801, et seq.) enacted November 12, 1999.

Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. §§ 1320d–1320d-8 (2000).

New York Public Health Law § 17 (McKinney 2001).

Privacy Act of 1974, 5 U.S.C. § 552a(e)(10) (2000).

Rick Boucher, *A bill to require notice to and consent of an individual prior to the collection and disclosure of certain personal information relating to that individual*, 1st Sess. H. R., 111th Cong., (3 May 2010).

Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401–3422.

Stored Communications Act, Codified at 18 U.S.C. ch. 121 §§ 2701–2712.

USA Patriot Act, Public Law 107-56, Stat. 115 Stat. 272 (2001).

Video Privacy Protection Act of 1988, 18 U.S.C. § 2710(b)(1) (2000).

71 PA. STAT. ANN. § 1690.108 (West 1990).

Other Instruments

ASIA-PACIFIC ECONOMIC COOPERATION, *APEC Privacy Framework* (2005).

CANADIAN STANDARDS ASSOCIATION, *Model Code for the Protection of Personal Information* (CSA Publications, 1996).

Convention for the Protection of Human Rights and Fundamental Freedoms. *European Convention for the Protection of Human Rights and Fundamental Freedoms,* 4 November 1950, 213 U.N.T.S. 221, E.T.S. 5.

COUNCIL OF EUROPE, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, E.T.S. 108 (1981).

COUNCIL OF EUROPE, *Explanatory Report: Convention for the Processing of Individuals with regard to Automatic Processing of Personal Data*, ETS no. 108.

International Covenant on Civil and Political Rights, 19 December 1966, 999 U.N.T.S. 171, arts. 9-14, Can. T.S. 1976 No. 47, 6 I.L.M. 368 (entered into force 23 March 1976, accession by Canada 19 May 1976).

OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Paris: OECD Publications, 1980).

OECD, *OECD Declaration on Transborder Data Flows* (11 April 1985), online: OECD <http://www.oecd.org/document/60/0,3343,en_2649_34225_2373500_1_1_1_1,00.html>.

Universal Declaration of Human Rights, G.A. res. 217(III), U.N.G.A.O.R., 3d Sess., Supp. No. 13, U.N. Doc A/810, (1948) 71.

U.S., *Safe Harbor framework*, online: <http://export.gov/safeharbor/>.

JURISPRUDENCE

Canadian Case Law (Federal)

BMG Canada v. John Doe, 2004 FC 488 (CanLII), aff'd 2005 FCA 193 (CanLII).

BMG Canada v. John Doe, 2004 FC 488 (CanLII), aff'd 2005 FCA 193 (CanLII), Factum of the Intervener Canadian Internet Policy and Public Interest Clinic.

Canada (Information Commissioner) v. Canada (Minister of Ctizenship and Immigration), 2002 FCA 270 (CanLII).

Canada (Information Commissioner) v. Canada (Transportation Accident Investigation and Safety Board), 2006 FCA 157 (CanLII).

Dagg v. Canada (Minister of Finance), [1997] 2 S.C.R. 403.

Gordon v. Canada (Health), 2008 FC 258 (CanLII).

Hunter v. Southam, [1984] 2 S.C.R. 14.

Randall v. Nubodys Fitness Centres, 2010 FC 681 (CanLII).

R. v. Dyment, [1988] 2 S.C.R. 417.

R. v. Edwards, [1996] 1 S.C.R. 128.

R. v. *Oakes,* [1986] 1 S.C.R. 103.

R. v. Plant 84 C.C.C. (3d) 203, [1993] 3 S.C.R. 281, 24 C.R. (4th) 47, 1993 CarswellAlta 94, 1993 CarswellAlta 566 (S.C.C.).

R. v. Tessling, [2004] 3 S.C.R. 432, 2004 SCC 67.

Stevens v. SNF Maritime Metal Inc., 2010 FC 1137 (CanLII).

Stubart Investments Ltd. c. La Reine, [1984] 1 R.C.S. 536.

Therrien (Re), [2001] 2 R.C.S. 3.

Wyndowe v. Rousseau, 2008 FCA 39 (CanLII).

Findings Rendered by the Office of the Privacy Commissioner of Canada

OPCC, *PIPEDA Case Summary #2001-10, Trucking company collects personal information intended for Canada Customs* (17 August 2001).

OPCC, *PIPEDA Case Summary #2001-15, Privacy Commissioner releases his finding on the prescribing patterns of doctors* (2 October 2001), online: <http://www.priv.gc.ca/media/an/wn_011002_e.cfm>.

OPCC, *PIPEDA Case Summary #2001-25, A Broadcaster accused of collecting personal information via Web site* (20 November 2001), online: <http://www.privcom.gc.ca/cf-dc/2001/cf-dc_011120_e.asp>.

OPCC, *PIPEDA Case Summary #2002-45, Bank accused of misrepresenting purposes in collecting date of birth* (11 April 2002).

OPCC, *PIPEDA Case Summary #2002-46, Bank accused of inappropriately demanding birthdates from account applicants* (26 April 2002).

OPCC, *PIPEDA Case Summary #2002-53, Bank accused of providing police with surveillance photos of the wrong person* (28 June 2002).

OPCC, *PIPEDA Case Summary #2002-94, Individual objects to request for information as condition of supply of service* (2 December 2002).

OPCC, *PIPEDA Case Summary #2003-118, Employer's effort to collect personal medical information deemed appropriate; no evidence of inappropriate disclosure* (17 February 2003).

OPCC, *PIPEDA Case Summary #2003-119, Employer's policy and practices regarding the collection of personal medical information deemed appropriate* (17 February 2003).

OPCC, *PIPEDA, Case Summary #2003-162, Customer complaints about airline's use of cookies on its Web site* (16 April 2003).

OPCC, *PIPEDA Case Summary #2003-169, Individual objects to bank's requirements to provide Notice of Assessment for income verification purposes* (24 April 2003).

OPCC, *PIPEDA Case Summary #2003-191, Company's collection and disclosure of employee sick leave information* (11 July 2003).

OPCC, *PIPEDA Case Summary #2003-204, Telecommunications company accused of refusing services unless SIN was provided* (5 August 2003).

OPCC, *PIPEDA Case Summary #2003-209, Individual alleged that bank request for SIN was unnecessary* (5 August 2003).

OPCC, *PIPEDA Case Summary #2003-217, A telecommunications company requires two pieces of identification from a subscriber* (5 August 2003).

OPCC, *PIPEDA Case Summary #2003-220, Telemarketer objects to employer sharing her sales results with other employees* (15 September 2003).

OPCC, *PIPEDA Case Summary #2003-223, Bank accused of collecting too much information from credit card applicant* (16 September 2003).

OPCC, *PIPEDA Case Summary #2003-257, Employees objected to corporation's requirement for medical diagnosis on sick leave certificates* (Fall 2003).

OPCC, *PIPEDA Case Summary #2003-233, An individual challenged the requirement to provide the medical diagnosis on her doctor's certificate for sick leave* (3 October 2003).

OPCC, *PIPEDA Case Summary #2003-226, Company's collection of medical information unnecessary; safeguards are inappropriate* (31 October 2003).

OPCC, *PIPEDA Case Summary #2003-237, Individual accuses employer of disclosing personal information to co-workers* (20 November 2003).

OPCC, *PIPEDA Case Summary #2003-251, A question of responsibility* (12 December 2003).

OPCC, *PIPEDA Case Summary #2003-255, Airport authority's collection and retention practices questioned* (24 December 2003).

OPCC, *PIPEDA Case Summary #2004-269, Employer hires private investigator to conduct video surveillance on employee* (23 April 2004).

OPCC, *PIPEDA Case Summary #2004-275, A bank provides inaccurate information to credit agencies* (24 August 2004).

OPCC, *PIPEDA Case Summary #2004-276, The privacy implications of pay per view and piracy prevention measures* (2 September 2004).

OPCC, *PIPEDA Case Summary #2004-281, Organization uses biometrics for authentication purposes* (3 September 2004).

OPCC, *PIPEDA Case Summary #2004-286, Bank customers required to declare citizenship* (21 December 2004).

OPCC, *PIPEDA Case Summary #2005-295, Customer concerned about mysterious debits from bank account* (14 March 2005).

OPCC, *PIPEDA Case Summary #2005-299, Thief cashes convenience cheque on cancelled credit card account* (31 March 2005).

OPCC, *PIPEDA Case Summary #2005-303, Real estate broker publishes names of top five sales representatives in a city* (31 May 2005).

OPCC, *PIPEDA Case Summary* #313, *Bank's notification to customers triggers PATRIOT Act concerns* (19 October 2005).

OPCC, *PIPEDA Case Summary #2005-317, Fax from debt collector contained debtor's personal information* (24 October 2005).

OPCC, *PIPEDA Case Summary #2006-332, Bank issues new guidelines and educates employees after customer information is faxed to the wrong individual* (12 April 2006).

OPCC, *PIPEDA Case Summary #2006-344, Couple's safety box opened in error* (17 July 2006).

OPCC, *PIPEDA Case Summary # 333, Canadian-based company shares customer personal information with U.S. parent* (19 July 2006).

OPCC, *PIPEDA Case Summary #2006-349, Photographing of tenants' apartments without consent for insurance purposes* (24 August 2006).

Office of the Privacy Commissioner of Canada, *PIPEDA Case Summary #2006-351: Use of personal information collected by Global Positioning System considered* (9 November 2006).

OPCC, *PIPEDA Case Summary #2006-362, Insurance adjuster readjusts its collection practices* (14 December 2006).

OPCC, *PIPEDA Case Summary #2006-363, Registrar collects personal information to combat domain name hijacking* (14 December 2006).

OPCC, *PIPEDA Case Summary #2007-368, Insurance adjusters' consent form considered overly broad* (11 January 2007).

OPCC, *PIPEDA Case Summary #2007-381, Bank improves safeguards after individual's personal information used fraudulently to open credit card account* (15 March 2007).

OPCC, *PIPEDA Case Summary #2007-374, Bank faxes credit card account statement to fraudster* (23 March 2007).

OPCC & Office of the Information and Privacy Commissioner of Alberta, *Findings under the Personal Information Protection and Electronic Documents Act (PIPEDA): Report of an Investigation into the Security, Collection and Retention of Personal Information, TJX Companies Inc. /Winners Merchant International L.P.* (25 September 2007), online: <http://www.priv.gc.ca/cf-dc/2007/TJX_rep_070925_e.cfm>.

OPCC, *PIPEDA Case Summary #2008-390, Residential Property Appraisal Documents are Owners' Personal Information* (7 May 2008).

OPCC, *PIPEDA Case Summary #394, Outsourcing of canada.com e-mail services to U.S.-based firm raises questions for subscribers* (19 September 2008).

OPCC, *PIPEDA Case Summary #2009-004, No Consent Required for Using Publicly Available Information Matched with Geographically Specific Demographic Statistics* (9 January 2009).

OPCC, *PIPEDA Case Summary #2009-002, Realtor advertises purchase price of condominium in trade publication without buyer's consent* (20 February 2009).

OPCC, *PIPEDA Case Summary #2009-018, Psychologist's anonymized peer review notes are the personal information of the patient* (23 February 2009).

OPCC, *PIPEDA Case Summary #2009-014, Fraud detection not an acceptable reason to collect driver's licence numbers for store memberships* (29 May 2009).

Office of the Privacy Commissioner of Canada, *PIPEDA Case Summary #2009-008, Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc., Under the Personal Information Protection and Electronic Documents Act by Elizabeth Denham, Assistant Privacy Commissioner of Canada* (16 July 2009).

OPCC, *Report of Findings, Complaint under PIPEDA against Accusearch Inc., doing business as Abika.com* (31 July 2009).

OPCC, *PIPEDA Case Summary #2009-010, Assistant Commissioner recommends Bell Canada inform customers about Deep Packet Inspection* (13 August 2009).

OPCC, *PIPEDA Case Summary #2009-012: Bank not responsible after new account was opened using stolen identity* (24 August 2009).

OPCC, *PIPEDA Report of Findings #2011-001, Report of Findings: Google Inc. WiFi Data Collection* (20 May 2011).

Alberta Case Law

Leon's Furniture Limited v. Alberta (Information and Privacy Commissioner), 2011 ABCA 94 (CanLII).

Ontario Case Law

Her Majesty the Queen v. *Arthur Kwok*, Ontario Court of Justice W.A. Gorewich J., January 25, 2008, Docket: Newmarket 06-06029.

Jones v. Tsige, 2012 ONCA 32.

Quebec Case Law

Courts (Quebec)

Boulerice c. Acrofax inc., [2001] R.L. 621 (C.Q.).

Commission des droits de la personne et des droits de la jeunesse c. Montréal (Service de police de la Communauté urbaine de), [2002] R.J.Q. 824.

Demers v. Banque Nationale du Canada, B.E. 97BE-330 (C.Q.).

Larochelle c. Association des personnes handicapées de Lévis, D.T.E. 2006T-359 (C.Q.).

Laval (Ville) c. X., 2003 CanLII 44085 (C.Q.).

La Personnelle vie, Corporation d'Assurance v. Cour du Québec, [1997] C.A.I. 466 (S.C.).

Roy v. Société sylvicole d'Arthabaska-Drummond, J.E. 2005-279 (C.Q.).

St-Amant c. Meubles Morigeau ltée, [2006] R.J.Q. 1434 (C.S.).

Decisions Rendered by the Commission d'Accès à l'Information du Québec

A. v. C., AZ-50195726 (C.A.I.).

A. v. C., [2003] C.A.I. 534.

Agyemang v. Ipex Inc., [2001] C.A.I. 201

Benoit c. Dr Maurice Leduc, [1995] C.A.I. 270.

Bilodeau c. Dr Benoit Goulet, [2004] C.A.I. 366.

Chamberlain c. Association québécoise d'aide aux personnes souffrant d'anorexie nerveuse et de boulimie, [2003] C.A.I. 544.

Comeau v. Bell Mobilité, AZ-50110177 (C.A.I.).

Delaney v. Les associés, services financiers du Canada Limitée (2001), Montréal PV 00 03 47, AZ-50110191 (Azimut) (C.A.I.).

Deschênes c. Groupe Jean Coutu, PV 98 08 42 (C.A.I.).

Duchesne v. Great-West (La), compagnie d'assurance-vie, [1995] C.A.I. 493.

Hallis v. Équifax Canada, [1996] C.A.I. 107.

J.B. c. Commission de la santé et de la sécurité du travail, [2009] C.A.I. 43.

Julien v. Domaine Laudance, [2003] C.A.I. 77.

M. B. c. Anapharm inc., [2006] C.A.I. 484.

M. C. c. Champoux, [2008] C.A.I. 587.

M.C. c. Champoux, [2008] C.A.I. 230.

Perrault v. Blondin, A.I.E. 2006AC-42.

Perreault c. Blondin, [2006] C.A.I. 162.

Ravinsky v. Équifax Canada, [2003] C.A.I. 46.

S.R. c. Côté, [2009] C.A.I. 172.

Tremblay v. Caisse populaire Desjardins de St-Thomas, [2000] C.A.I. 154.

X. v. Agence de recouvrement Réjean Aubé, A.I.E. 96AC-75 (Inquiry Report).

X. et Aventure Électronique inc., AZ-96151506 (C.A.I.)

X. v. Banque nationale du Canada, A.I.E. 96AC-103 (Inquiry Report).

X. and Banque Royale du Canada, A.I.E. 95AC-72 (Inquiry Report).

X. v. Centre de protection et de réadaptation de la Côte-Nord, (24 July 2003), CAI 02 06 08, v. D. Boissinot.

X. v. Équifax Canada, [1995] C.A.I. 286.

X. v. Le Groupe Jean Coutu (P.J.C.), [1995] C.A.I. 128.

X. v. Ministère de la Sécurité Publique, (4 August 2003), CAI 02 06 20, v. D. Boissinot.

X et Ordre des comptables agréés du Québec, AZ-95151513 (C.A.I. enquête).

X. c. Résidence L'Oasis Fort St- Louis, [1995] C.A.I. 367

X. v. Services aux marchands détaillants ltée, A.I.E. 96AC-101 (Inquiry Report).

X. and Synergic International 1991, [1995] C.A.I. 361.

X. v. Ville de Saint-Laurent, (14 June 2000), CAI 97 04 78, v. P.-A. Comeau.

X. and Y. v. Hôpital du Sacré-coeur de Montréal, (16 July 2002), CAI 98 13 00, v. C. Constant, J. Stoddart and M. Laporte.

Arbitrators' decisions (Quebec)

Fraternité nationale des forestiers et travailleurs d'usines et Groupe Bocenor, usine de Ste-Marie, D.T.E. 2005T-545 (T.A.).

Groupe Champlain inc. (Gatineau) et Syndicat québécois des employées et employés de service, section locale 298 (FTQ), D.T.E. 2009T-431 (tribunal d'arbitrage).

Métallurgistes unis d'Amérique, section locale 696 et Waterville TG, D.T.E. 2002T-1078 (T.A.).

Prelco Inc. et Syndicat national de l'automobile, de l'aérospatiale, du transport et des autres travailleurs et travailleuses du Canada, section locale 1044, D.T.E. 99T-41 (T.A.).

Scobus St-Hubert Inc. et Syndicat international des travailleurs et travailleuses unis de l'alimentation et du commerce, section locale 501, [1992] T.A. 497.

Syndicat canadien de la fonction publique, section locale 3892 et Société des casinos du Québec Inc., [2001] R.J.D.T. 548 (T.A.).

Syndicat des employées et employés de métiers d'Hydro-Québec, section locale 1500 – SCFP (FTQ) et Hydro-Québec, D.T.E. 2009T-273.

Syndicat des employées et employés professionnels et de bureau and others, D.T.E. 2009T-170**.**

Syndicat des employées et employés professionnels et de bureau, section locale 57 and Caisse populaire St-Stanislas de Montréal, D.T.E. 99T-59 (T.A.)

Syndicat des fonctionnaires municipaux et professionnels de la Ville de Sherbrooke et Sherbrooke (ville de), D.T.E. 2009T-309.

Syndicat des travailleuses et travailleurs du CSSS du Sud de Lanaudière (CSN) and others, D.T.E. 2009T-253.

Syndicat national des employés de l'Aluminium d'Alma Inc., (section des employés horaires) et Société d'électrolyse et de chimie Alcan Ltée, usine Isle-Maligne, Alma, D.T.E. 2001T-904 (T.A.).

Syndicat québécois des employées et employés de service, section locale 298 and Jardins du Haut-St-Laurent (1990) enr., [2003] R.J.D.T. 1026 (T.A.).

France

Courts (France)

CA Dijon, 14 September 2010, online: <http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=2999>.

CA Paris, 1 February 2010, *Cyrille S. c. Sacem*.

CA Paris, 25 June 2008, (2008) RG 08/04727.

CA Paris, 15 May 2007, No. 06/01954.

CA Paris, 27 April 2007, No. 06/02334.

CA Rennes, 22 May 2008, No. 07/01495.

Cass. civ., 19 January 2010, No. 08-42.519.

Cass. crim., 13 January 2009, No. 08-84088.

Trib. gr. inst. Paris, 24 June 2009, *Jean-Yves Lafesse et autres c. Google et autres.*

Trib. gr. inst. Paris, 1re chambre section sociale, 28 October 2008, Association Union Fédérale des Consommateurs Que Choisir vs. Amazon, available in French at <http://www.foruminternet.org/specialistes/veille-juridique/jurisprudence/IMG/pdf/tgi-par20081028.pdf>.

Trib. gr. inst. Paris, 3 March 2008, ord. Réf. RG 08□51650.

Trib. gr. inst. Paris, 19 April 2005, *Comité d'entreprise Effia Services, Fédération des syndicats Sud Rail c. Effia services*, No. 05-00382.

Délibérations of the Commission Nationale de l'Information et des Libertés (France)

CNIL, *Délibération n° 2007-374 du 11 décembre 2007.*

CNIL, *Délibération no. 96-069 du 10 septembre 1996 relative à la demande d'avis portant création à titre expérimental d'un traitement automatisé d'informations nominatives ayant pour finalité principale la lecture automatique des plaques d'immatriculation des véhicules en mouvement par la société des autoroutes Paris-Rhin-Rhône (SAPR).*

CNIL, *Délibération No. 97-050 du 24 juin 1997 relative à une demande d'avis présenté par France Télécom concernant un traitement automatisé d'informations nominatives dénommé "Minitelnet".*

CNIL, *Délibération No. 97-051 du 30 juin 1997 concernant une demande d'avis présenté par la Mairie de Paris relative à un traitement d'informations nominatives mis en oeuvre dans le cadre du site Internet de la Ville de Paris.*

CNIL, *Délibération n°2006-245 du 23 novembre 2006 prononçant une sanction pécuniaire à l'encontre de la Caisse régionale de crédit agricole mutuel de centre France*.

CNIL, *Délibération n°2008-470 du 27 novembre 2008 de la formation restreinte prononçant une sanction pécuniaire à l'encontre de la société ISOTHERM.*

CNIL, *Délibération n°2010-113 du 22 avril 2010 de la formation restreinte portant avertissement à l'encontre de la société AIS 2 exerçant sous l'enseigne ACADOMIA Respecter.*

United States

Daily Times Democrat v. Graham, 162 So. 2d 474 at 476 (Ala. 1964).

Doe v. Southeastern Pennsylvania Transportation Authority, 72 F. (3d) 1133 (3d Cir. 1995).

Duran v. Detroit News, Inc., 504 N.W. 2d 715 (Mich. Ct. App. 1993).

Haynes v. Alfred A. Knopf, Inc. 8 F.3d 1222 (7th Cir. 1993) (Posner, J.).

J. Roderick MacArthur Found. v. FBI, 102 F. (3d) 600 (D.C. Cir. 1996) (Tatel, J., dissenting).

Katz v. United States, 389 U.S. 347 (1967).

Margan v. Niles, 250 F. Supp. 2d 63 at 68-69 (N.D.N.Y. 2003).

McNamara v. Freedom Newspapers, 802 S.W. 2d 901 at 903 (Tex. App. 1991).

McVeigh v. Cohen, 983 F. Supp. 215 (D.D.C. 1998).

Multimedia WMAZ v. Kubach, 443 S.E. 2d 491 at 500 (Ga. Ct. App. 1994).

Northwestern Memorial Hospital v. Ashcroft, 362 F. (3d) 923 at 929 (7th Cir. 2004), Posner, J.

Olmstead v. United States, 277 U.S. 438 (1928), rev'd *Katz v. United States*, 389 U.S. 347 (1967).

Paul v. Davis, 424 U.S. 693 (1976).

Planned Parenthood of the Columbia/Williamette, Inc. v. Am. Coalition of Life, Activists, 244 F. 3d 1007 (9th Cir. 2001).

Reeves v. Equifax Information Services, No. 09-CV-00043, 2010 BL 113325 (S.D. Miss. May 20, 2010).

Remsburg v. Docusearch, Inc., 816 A. (2d) 1001, 1005-06 (N.H. 2003).

Shibley v. Time Inc., 45 Ohio App. 2d 69, 341 N.E. 2d 337, 74 Ohio Op. 2d 101, 82 A.L.R. 3d 765 (1975).

Sipple v. Chronicle Publishing Co., 201 Cal. Rptr. 665 (Ct. App. 1984).

Times Mirror Co. v. Superior Court, 244 Cal. Rptr. 556 at 558 (Ct. App. 1988).

TJX Companies Retail Sec. Breach Litigation, 564 F. 3d 489 at 491 (1st Cir. 2009).

U.S., Federal Communications Commission, *In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles: Intelligent Transportation Society of America Reply Comments* (WT Docket No. 01-72) (Washington, D.C.: 24 April 2001).

U.S., Federal Trade Commission, *In the Matter of Realtime Targeting and Auctioning, Data Profiling Optimization, and Economic Loss to Consumers and Privacy, Complaint, Request for Investigation, Injunction, and Other Relief: Google, Yahoo, PubMatic, TARGUSinfo, MediaMath, eXelate, Rubicon Project, AppNexus, Rocket Fuel, and Others* (Washington, D.C., 8 April 2010).

U.S. v. Jones, 565 U.S. 132 S. Ct. 945 at 955 (2012).

U.S., *Cong. Rec.*, vol. 140, at H9797, H9810 (27 September 1994) (Rep. Kennedy).

U.S., *Financial Privacy and Consumer Protection Hearing Before the Senate Comm. on Banking, Housing and Urban Affairs*, 107th Cong. (2002) (statement of William H. Sorrell, Attorney General, State of Vermont).

United States v. Reporters' Comm. for Freedom of the Press, 489 U.S. 749 (1989).

Whalen v. Roe, 429 U.S. 589 (1977).

Y.G. v. Jewish Hosp., 795 S.W. 2d 488 at 500 (Mo. Ct. App. 1990).

Declarations and Statements (U.S. Proceedings)

FTC v. Citigroup, No. 1:01-CV-00606, Decl. of Gail Kubiniec, 10 (May 2001).

U.S., *Financial Privacy and Consumer Protection Hearing Before the Senate Comm. on Banking, Housing and Urban Affairs*, 107th Cong. (2002) (statement of Mike Hatch, Attorney General, State of Minnesota).

Foreign Case Law

District Court of Munich, 30 September 2008, 133 C 5677/08, online: Medien Internet und Recht <http://medien-internet-und-recht.de/volltext.php?mir_dok_id=1769>. (Germany)

District Court Berlin-Mitte, 27 March 2007, 5 C 314/06. (Germany)

Durant v Financial Services Authority [2003] EWCA Civ. 1746. (U.K.)

Stockholm Lænsrætt, 8 June 2005, No. 593-2005. (Sweden)

DOCTRINE

Books

ALLEN, A., *Uneasy access: privacy for women in a free society* (Totowa, New Jersey: Rowman & Littlefield, 1988).

BARAK, A., *Purposive Interpretation in Law* (Princeton: Princeton University Press, 2005).

BENN, S., "Privacy, Freedom, and Respect for Persons" in Ferdinand David Schoeman, ed., *Philosophical Dimensions of Privacy* (New York : Cambridge University Press, 1984).

BENNETT, C. & RAAB, C., *The Governance of privacy* (Cambridge: MIT Press, 2006).

BENNETT, C., "The Public Surveillance of Personal Data: A Cross-National Analysis" in David Lyon & Elia Zureik, eds., *Computers, surveillance, and privacy* (Minneapolis: University of Minnesota Press, 1996).

BENNETT, C. & CROWE, L., *Location-Based Services and the Surveillance of Mobility: An Analysis Of Privacy Risks In Canada* (Ottawa: OPCC, 2005).

BYGRAVE, L., *Data Protection Law: Approaching Its Rationale, Logic and Limits* (The Hague: Kluwer Law International, 2002).

CARLYLE BRECKENRIDGE, A., *The Right to Privacy* (Lincoln: University of Nebraska Press, 1970).

CATE, F., *Privacy in the Information Age* (Washington: Brookings Institution Press, 1997).

CÖTÉ, P.-A., *Interprétation des lois*, 3rd ed. (Montréal : Éditions Thémis, 1999).

CÖTÉ, P.-A., *Interprétation des lois* (Montréal: Éditions Thémis, 2009).

DECEW, J., *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology* (Ithaca: Cornell University Press, 1997).

DERIEUX, E. & TRUDEL, P., (eds.), *L'intérêt public, principe du droit de la communication* (Paris : Éditions Victoires, 1996).

DRIEDGER, E., *Construction of Statutes*, 2nd ed. (Toronto : Butterworths, 1983).

FEINBERG, J., *Freedom and Fulfilment: Philosophical Essays* (Princeton: Princeton University Press, 1994).

FLAHERTY, D., Protecting privacy in surveillance societies: the Federal Republic of Germany, Sweden, France, Canada, and the United States (Chapel Hill: University of North Carolina Press, 1989).

FRIED, C., *An Anatomy of Values: Problems of Personal and Social Choice* (Cambridge: Harvard University Press, 1970).

GANDY, O., *The panoptic sort: a political economy of personal information* (Boulder, Colo.: Westview, 1993).

GANDY, O., "Coming to Terms with the Panoptic Sort" in David Lyon & Elia Zureik, eds., *Computers, surveillance, and privacy* (Minneapolis: University of Minnesota Press, 1996).

GAUTRAIS, V. & TRUDEL, P., *Circulation des Renseignements Personnels et Web 2.0* (Montréal: Éditions Thémis, 2010).

GAUTRAIS, V., *Neutralité technologique: Rédaction et interprétation des lois face aux technologies* (Montréal : Éditions Thémis, 2012).

GILLIOM, J., *Overseers of the poor: surveillance, resistance, and the limits of privacy* (Chicago: University of Chicago Press, 2001).

GRATTON, E., *Internet and Wireless Privacy: A Legal Guide to Global Business Practices* (Toronto: CCH Canada, 2003).

HEISENBERG, D., *Negotiating privacy: the European Union, the United States and personal data protection* (Boulder: Lynne Rienner Publishers, 2005).

INNESS, J., *Privacy, Intimacy and Isolation* (New York: Oxford University Press, 1992).

KAUFMAN, J., ed., *Privacy law in the private sector: an annotation of the legislation in Canada* (Aurora: Canada Law Book, 2007).

KUNER, C., *European Data Privacy Law and Online Business* (Oxford: Oxford University Press, 2003).

LESSIG, L., *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999).

MCCARTHY, T., *The Rights of Publicity and Privacy*, § *5.59* (*2d ed. 2005*).

MCISAAC, B., *The law of privacy in Canada* 4-7 (2011).

MILLER, A., *The Assault on Privacy: Computers, Data Banks, and Dossiers* (Ann Arbor: The University of Michigan Press, 1971).

MOORE, B., *Privacy: Studies in social and cultural history* (Armonk, N.Y.: M.E. Sharpe, 1984).

MORGAN, R. & BOARDMAN, R., *Data protection Strategy. Implementing Data Protection Compliance* (London: Sweet & Maxwell, 2003).

NEWELL, F., *loyalty.com: Customer Relationship Management in the New Era of Internet Marketing* (New York: McGraw-Hill, 2000).

O'BRIEN, D., *Privacy, Law, and Public Policy* (Westport: Praeger Publishers, 1979).

ORWELL, G., *Nineteen eighty-four* (New York: Harcourt, 1949).

PEPPERS, D. & ROGERS, M., *The One to One Future: Building Relationships One Customer at a Time* (New York: Currency, 1997).

PERRIN, S. et al., *The personal information protection and electronic documents act: an annotated guide* (Toronto: Irwin Law, 2001).

PIGEON, L.-P., *Rédaction et interprétation des lois*, 1st ed., coll. "Études juridiques" (Québec: *Éditeur officiel*, 1978).

REGAN, P., *Legislating privacy: technology, social values, and public policy* (Chapel Hill: University of North Carolina Press, 1995).

ROSEN, J., *The unwanted gaze: the destruction of privacy in America* (Random House, 2000).

SCHOEMAN, F., "Privacy and Intimate Information" in Ferdinand David Schoeman, ed., *Philosophical Dimensions of Privacy* (New York: Cambridge University Press, 1984).

SCHOEMAN, F., "Gossip and Privacy" in Robert F. Goodman & Aaron Ben-Ze'ev, eds., *Good Gossip* (Lawrence: University Press of Kansas, 1994).

SMITH, G., *Internet Law and Regulation* (London: Sweet and Maxwell, 2007).

SMITH, H., *Managing privacy: information technology and corporate America* (Chapel Hill: University of North Carolina Press, 1994).

SOLOVE, D., *The Digital Person: Technology and Privacy in the Information Age* (New York: NYU Press, 2004).

TRUDEL, P., "Le rôle de la loi, de la déontologie et des décisions judiciaires dans l'articulation du droit à la vie privée et de la liberté de presse" in Pierre Trudel & France Abran, *Droit du public à l'information et vie privée : deux droits irréconciliables?* (Montréal : Éditions Thémis, 1992) 181.

VAN DEN HOVEN, J., "Information Technology, Privacy, and the Protection of Personal Data" in Jeroen van den Hoven & John Weckert, eds., *Information Technology and Moral Philosophy* (New York: Cambridge University Press, 2008) 301.

WALDO, J., LIN, H. & MILLETT, L., eds., Committee on Privacy in the Information Age, National Research Council, *Engaging Privacy and Information Technology in a Digital Age* (Washington, US: The National Academies Press, 2007).

WESTIN, F., *Privacy and Freedom* (New York: Atheneum, 1967).

Articles

ABRAMOVITCH, S., "Publicity Exploitation of Celebrities: Protection of a Star's Style in Quebec Civil Law" (1991) 32 C. de D. 301.

ALLEN, A., "Lying to Protect Privacy" (1999) 44 Vill. L. Rev. 161.

ALLEN, S. and al., *RFID Tagging: Final Report*, online: <http://www.rahulnair.net/files/RFID_Final_Report.pdf>.

ACQUISTI, A., & GROSS, R., "Predicting Social Security numbers from public data" (2009) 106:27 Proceedings of the National Academy of Sciences of the United States of America 10975.

BAYENS, S., "The Search and Seizure of Computers: Are We Sacrificing Personal Privacy for the Advancement of Technology?" (2000) 48 Drake L. Rev. 239.

BECKMANN, R., "Comment: Privacy Policies and Empty Promises: Closing the 'Toysmart Loophole'" (2001) 62 U. Pitt. L. Rev. 765.

BELGUM, K., "Who Leads at Half-time?: Three Conflicting Visions of Internet Privacy Policy" (1999) 6 Rich. J.L. & Tech. 1.

BENNER J., GIVENS, B., & MIERZWINSKI, E., "Nowhere to turn: victims speak out on identity theft" (1 May 2000) at pt. II, §§ 1, online: Privacy Rights Clearinghouse <http://www.privacyrights.org/ar/idtheft2000.htm>.

BENNETT, C., "The APEC Privacy Framework: A Trading-up of Standards or the Opposite?" (Paper delivered at the Conference on privacy and security, Victoria, 9 and 10 February 2006).

BENNETT MOSES, L., "Recurring Dilemmas: The Law's Race to Keep Up With technological Change" (2007) 7 University of Illinois Journal of Law, Technology and Policy 239.

BENZANSON, R., "The Right to Privacy Revisited: Privacy, News, and Social Change, 1890-1990" (1992) 80 Cal. L. Rev. 1133.

BERCIC, B. & GEORGE, C., "Identifying Personal Data Using Relational Database Design Principles" (2009) 17:3 International Journal of Law and Information Technology 233.

BERMAN J. & MULLIGAN, D., "Privacy in a Digital Age: Work in Progress" (1999) 23 Nova L. Rev. 551.

BOURCIER, D., "L'acte de juger est-il modélisable? De la logique à la justice" (2011) 54 Arch. phil. Droit 37.

BOURCIER, D., "Données sensibles et risque informatique: de l'intimité menacée à l'identité virtuelle", CURAPP – Questions sensibles, PUF (1998).

CALO, R., "The Boundaries of Privacy Harm" (2011) 86:3 Indiana Law Journal 1131.

CALO, R., “People Can Be So Fake: A New Dimension to Privacy and Technology Scholarship” (2010) 114 Penn. St. L. Rev. 809.

CATE, F., “The Changing Face of Privacy Protection in the European Union and the United States” (1999) 33 Ind. L. Rev. 173.

CAVOUKIAN, A., *Privacy as a Fundamental Human Right vs. an Economic Right: An Attempt at Conciliation* (Toronto: Information and Privacy Commissioner, 1999), online: Office of the Information and Privacy Commission for Ontario <http://www.ipc.on.ca/images/Resources/up-1pr_right.pdf>.

CAVOUKIAN, A., *Tag You’re It: Privacy Implications of Radio Frequency Identification (RFID) Technology* (Toronto: Information and Privacy Commissioner, 2004).

CLARKE, R., “Human Identification in Information Systems: Management Challenges and Public Policy Issues” (1994) 7 Info. Tech. & People 6, online: <http://www.rogerclarke.com/DV/HumanID.html>.

CLARKE, R., “Profiling : A hidden Challenge to the Regulation of Data Surveillance” (1993) 4 :2 J. of Law and Information Science 403.

CLARKE, R., “Information Technology and Dataveillance” (November 1987), online: <http://www.anu.edu.au/people/Roger.Clarke/DV/CACM88.html>.

CLARKE, R., “Introduction to Dataveillance and Information Privacy, and Definitions of Terms” (16 September 1999), online: <http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html>.

COCKFIELD, A., “Towards a Theory of Law and Technology” (2004) 30 Manitoba L.J. 383.

COHEN, J., “Examined Lives: Informational Privacy and the Subject as Object” (2000) 52 Stan. L. Rev. 1373.

COHEN, J., “Cyberspace as/and Space” (2007) 107 Colum. L. Rev. 210.

CORTESE, A., “Price Flexing: How the Web Adds New Twists”, *CIO Insight* (1 March 2002).

COTTERET J.-M., & EMERI C., “Vie privée des hommes politiques” (1979-80) 14 R.J.T. 335.

COUGHLAN, S., and al., “Global reach, Local Grasp: Constructing extraterritorial jurisdiction in the Age of Globalization”, (2007) 6 CJLT 29.

DANNA, A. & GANDY, O., “All That Glitters is Not Gold: Digging Beneath the Surface of Data Mining” (2002) 40 Journal of Business Ethics 373.

DEAN GERTZ J., “The Purloined Personality: Consumer Profiling in Financial Services” (2002) 39 San Diego L. Rev. 943.

DEARNE, K., “You are Being Monitored Online” (2002) The Australian.

DELWAIDE, K. & AYLWIN A., “Leçons tirées de dix ans d'expérience : la *Loi sur la protection des renseignements personnels dans le secteur privé* du Québec” (2005) 233 Développements récents en droit de l'accès à l'information.

DOLIN, R., “Search Query Privacy: The Problem of Anonymization” (2010) 2:2 Hastings Science and Technology Law Journal 137.

EL EMAM, K., *De-identification Risk Assessment Model* (30 May 2009), online: <www.healthinformation.ca>.

EL EMAM, K., De-identifying Health Data for Secondary Use: A Framework, online: <http://www.ehealthinformation.ca/documents/SecondaryUseFW.pdf>.

FARBER, D., “Book Review: Privacy, Intimacy, and Isolation by Julie C. Inness” (1993) 10 Const. Comment. 510.

FAERBER, C., “BookVersus Byte: The Prospects and Desirability of a Paperless Society” (1999) 17 J. Marshall J. Computer & info. L. 797.

MIN-CHEE FONG, A., “Unmasking the John Does of Cyberspace: Surveillance by Private Copyright Owners” (2005) 4:3 CJTL.

FRIED, C., “Privacy” (1968) 77 Yale L.J. 475.

FROOMKIN, A., “The Death of Privacy?” (2000) 52 Stan. L. Rev. 1461.

GANDY, O., “Exploring Identity and Identification” (2000) 14 Notre Dame J.L. Ethics & Pub. Pol’y 1085.

GARCIA, F., “Bodil Lindqvist: A Swedish Churchgoer’s Violation of the European Union’s Data Protection Directive Should Be a Warning to U.S. Legislators” (2005) 15 Fordham Intell. Prop. Media & Ent. L.J. 1206.

GARRIE, D., “The Legal Status of Software” (2005) 23 J. Marshall L J. Computer & Info. L. 711.

GAUTRAIS, V., “Introduction générale: Le défi de la protection de la vie privée face aux besoins de circulation de l’information personnelle” (2004) 9:2 Lex Electronica.

GAVISON, R., “Privacy and the Limits of Law” (1980) 89 Yale L.J. 421.

GERETY, T., “Redefining Privacy” (1977) 12 Harv. C.R.-C.L. L. Rev. 233.

GIVENS, B., “Privacy Expectations in a High Tech World” (2000) 16 Computer & High Tech. L. J. 347.

GLANCY, D., “At the Intersection of Visible and Invisible Worlds: United States Privacy Law and the Internet” (2000) 16 Santa Clara Computer & High Tech. L.J. 357.

GOLDBERG, G., et al., “Trust, Ethics, and Privacy” (2001) 81 B.U. L. Rev. 407.

GOLDMAN, E., “Data Mining and Attention Consumption” in Katherine Jo Strandburg & Daniela Stan Raicu, eds., *Privacy and Technologies of Identity: A Cross-Disciplinary Conversation* (New York: Springer, 2006, online: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=685241>

GOMEZ-VELEZ, N., "Internet Access to Court Reports: Balancing Public Access and Privacy" (2005) 51 Loyola L. Rev. 365.

GRATTON, E., "Personalization, Analytics, and Sponsored Services: The Challenges of Applying PIPEDA to Online Tracking and Profiling Activities" (2010) 8 CJLT 299.

GRATTON, E., "Dealing with Unsolicited Commercial Emails: A Global Perspective" (2004) Journal of Internet Law 3.

GRATTON, E., "Can Quebec Employers Search OSNs for Employee-related Information?" (2009) PrivacyScan.

GRATTON, E., MCWILLIAM, B., & WAN, C., *Canadian Legal Requirements for Electronic Marketing: International Privacy Guide*, vol. 2 (Thomson Reuters, 2010).

GRATTON, E., "Aiding-and Abetting Liability Exposure of Affiliate Program Service Providers Under the New U.S. Internet Gambling Law" (2007) 10:12 Journal of Internet Law.

GREENLEAF, G., "APEC's Privacy Framework: A New Low Standard" (2005) 11 Privacy Law & Policy Reporter 121.

GREENLEAF, G., "Criticisms of the APEC Privacy Principles (Version 9), and recommendations for improvements" (2004) [Prepared for publication and for consideration by the Australian Privacy Foundation (APF) and by the Asia-Pacific Privacy Charter Council (APPCC)].

GREENLEAF, G., "The APEC privacy initiative: 'OECD Lite' for the Asia-Pacific?" (2004) 71 Privacy Laws & Business 16.

GREENLEAF, G., "Five years of the APEC Privacy Framework: Failure or promise?" (2009) Computer Law & Security Report 25.

GROCHOWSKI, E. and HALERN, R., "Technological Impact of magnetic Hard Disk Drives on Storage Systems" (2003) 42:2 IBM Systems Journal 338.

GROSS, H., "The Concept of Privacy" (1967) 42 N.Y.U.L. Rev. 34.

HALPERIN, J.-L., "L'essor de la 'privacy' et l'usage des concepts juridiques" (2005) 61 Droit et Société 765.

HARITON, G., LAWFORD, J. & PALIHAPITIYA, H., *Radio Frequency Identification and Privacy: Shopping Into Surveillance* (Ottawa: Public Interest Advocacy Center, 2005).

HETCHER, S., "Changing the Social Meaning of Privacy in Cyberspace" (2001) 15 Harv. J.L. & Tech. 149.

HOOFNAGLE, C., & SMITH, K., "Debunking the Commercial Profilers' Claims: A Skeptical Analysis of the Benefits of Personal Information Flows" (June 2003), online: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=504622>.

HOOFNAGLE, C., & KING, J., "What Californians Understand about Privacy Online" (3 September 2008), online: <http://ssrn.com/abstract=1262130 or http://dx.doi.org/10.2139/ssrn>.

JOHNSON, E., *An Examination of the Role of Clickstream Data in Marketing through the Internet* (12 May 1997), online: <http://www.ftc.gov/bcp/privacy/wkshp97/comments2/johnson0.htm>.

KANG, J., "Information Privacy in Cyberspace Transactions" (1998) 50 Stan. L. Rev. 1193.

KARAS, S., "Privacy, Identity, Databases: Toward a New Conception of the Consumer Privacy Discourse" (2002) American University Law Review.

KATYAL, S., "The New Surveillance" (2004) 54:2 Case Western Law Review 297.

KEATS CITRON, D., "Technological Due Process" (2008) 85 Wash. U. L. Rev. 1249.

KENYON, A., and RICHARDSON, M., (eds), *New Dimensions in Privacy Law: International and Comparative Perspectives* (2006) 91.

KERR, I., & MCGILL, J., "Emanations, Snoop Dogs and Reasonable Expectation of Privacy" (2007) 52:3 Criminal Law Quarterly 392.

KERR, I., et al., "Soft Surveillance, Hard Consent" (2006) 6 Personally Yours 1.

KERR, O., "Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn't" (2003) 97 NW. U. L. Rev. 607.

KOOPS, B.-J., "Should ICT Regulation be Technology-Neutral?" in Bert-Jaap Koops et al., eds., *Starting points for ICT regulation: Deconstructing prevalent policy one-liners*, coll. IT & Law Series, vol. 9 (The Hague: TMC Asser, 2006) 77.

LAWSON, P., "Techniques of Consumer Surveillance and Approaches to their Regulation in Canada and the USA" (March 2005), online: <http://www.idtrail.org/index2.php?option=com_content&do_pdf=1&id=110>.

LEIBOWITZ, W., "Personal Privacy and High Tech: Little Brothers Are Watching You" (1997) Nat'l L.J. at B16.

LESSIG, L., "The Law of the Horse: What Cyberlaw Might Teach" (1999) 113 Harv. L. Rev. 501.

LO, J., *A "Do Not Track List" for Canada?* (Ottawa: Public Interest Advocacy Centre, 2009), online: <www.piac.ca/files/dntl_final_website.pdf>.

LUNDEVALL-UNGER, P., & TRANVIK, T., "IP Addresses: Just a Number?" (2011) 19:1 International Journal of Law and Information Technology 53.

MALIN, B., "Betrayed By My Shadow: Learning Data Identity via Trail Matching" (2005) Journal of Privacy Technology.

MANDEL, G., "History Lessons for a General Theory of Law and Technology" (2007) 8 Minn. J. L. Sci. & Tech. 551.

MCINTYRE, TJ., "Alternative routes to identifying 'anonymous' online users" (18 February 2010), online: IT Law in Ireland <http://www.tjmcintyre.com/2010/02/alternative-routes-to-identifying.html>

MILLAR, J., "Core Privacy: A Problem for Predictive Data Mining" in Ian Kerr, Valerie Steeves & Carole Lucock, eds., *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society* (New York: Oxford University Press, 2009) 103, online: <http://www.idtrail.org/content/view/799>.

MOORE, J., "Radical Behavioralism and the Subjective-Objective Distinction" (1995) 18 The Behavior Analyst 33.

MORROW MCLAUGLIN, M., & VAUPEL, S., "Constitutional Right of Privacy and Investigative Consumer Reports: Little Brother Is Watching You" (1975) 2 Hastings Const. L.Q. 773.

MOWBRAY, M., "The Fog over the Grimpen Mire: Cloud Computing and the Law" (2009) 6:1 *SCRIPTed* 129.

MURPHY, R., "Property Rights in Personal Information: An Economic Defense of Privacy" (1996) 84 Geo. L.J. 2381.

NARAYANAN, A., & SHMATIKOV, V., "De-anonymizing Social Networks" (2009) Proceedings IEEE Symposium on Security and Privacy 173.

NARAYANAN, A., & SHMATIKOV, V., **"**Robust De-anonymization of Large Sparse Datasets" (2008) University of Texas at Austin.

NISSENBAUM, H., "Privacy as Contextual Integrity" (2004) 79:1 Washington Law Review 119.

OHM, P., "Broken Promises of Privacy" (2010) 57 UCLA l. Rev. 1701.

OLSEN, T. & MAHLER, T., "Identity Management and Data Protection Law: Risk, Responsibility and Compliance in 'Circles of Trust'" (2007), online: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1015006>.

OVERTON, B., & GIDDINGS, K., "The Right of Privacy in Florida in the Age of Technology and the Twenty-First Century: A Need for Protection from Private and Commercial Intrusion" (1997) 25 Fla. St. U. L. Rev. 25.

PICKER, R., "Competition and Privacy in Web 2.0 and the Cloud" (2008) U. of Chicago Law & Economics, Olin Working Paper No. 414.

POLLACH, I., "A Typology of Communicative Strategies in Online Privacy Policies: Ethics, Power and Informed Consent" (2005) 62:3 Journal of Business Ethics 221.

POMERANCE, R., "Redefining Privacy in the Face of New Technologies: Data Mining and the Threat to the 'Inviolate Personality'" (2005) 9 Can. Crim. L. Rev. 273.

POSNER, R., "The Right of Privacy" (1978) 12 Ga. L. Rev. 393.

POST, R., "The Social Foundations of Privacy: Community and Self in the Common Law Tort" (1989) 77 Cal. L. Rev. 957.

PROSSER, W., "Privacy" (1960) 48 Cal. L. Rev. 383.

PUBLIC INTEREST ADVOCACY CENTRE, *2010 Consumer Privacy Consultations: Comments of PIAC on Behavioural Targeting* (15 March 2010), online: <http://www.piac.ca/privacy/piac_comments_to_privacy_commissioner_of_canada_on_behavioural_targeting>

REED, C., "Information 'Ownership' in the Cloud'" (2 March 2010), online: SSRN <http://ssrn.com/abstract=1562461>.

REIDENBERG, J. & SCHWARTZ, P., *Data protection law and online services: regulatory responses*, delivered to Commission of the European Communities (December 1998).

REIDENBERG, J., "Privacy Wrongs in Search of Remedies" (2003) 54 Hastings L.J. 877.

RESSLER, J., "Privacy, Plaintiffs, and Pseudonyms: The Anonymous Doe Plaintiff in the Information Age" (2004) 53 U. Kan. L. Rev. 195, online: <http://ssrn.com/abstract=542782>

ROBINSON, N., *Review of the European Data Protection Directive* (Santa Monica, CA: RAND Corporation, 2009).

SCASSA, T. et al., *An Analysis of Legal and Technological Privacy Implications of Radio Frequency Identification Technologies*, Prepared for the Office of the Privacy Commissioner of Canada (28 April 2005), online: <http://www.library.dal.ca/law/Guides/FacultyPubs/Scassa/RFIDs_Report2(Single).pdf>

SCHNEIER, B., "Privacy and Control" (6 April 2010), online: Schneier on Security <http://www.schneier.com/blog/archives/2010/04/privacy_and_con.html>.

SCHULTZ, B., "Electronic Money, Internet Commerce, and the Right to Financial Privacy: A Call for New Federal Guidelines" (1999) 67 U. Cin. L. Rev. 779.

SCHWARTZ, P., "Privacy and Democracy in Cyberspace" (1999) 52 Vand. L. Rev. 1609.

SCHWARTZ, P. & SOLOVE, D., "The PII Problem: Privacy and a New Concept of Personally Identifiable Information" (2011) 86 N.Y.U. Law Review 1814.

SCHWARTZ, P., "Privacy and Participation: Personal Information and Public Sector Regulation in the United States" (1995) 80:3 Iowa L. Rev. 553.

SCHWARTZ, P., "Internet Privacy and the State" (2000) 32 Conn. L. Rev. 815.

SIMITIS, S., "Revisiting Sensitive Data" (1999) Review of the answers to the Questionnaire of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108).

SKOK, G., "Establishing a Legitimate Expectation of Privacy in Clickstream Data" (2000) 6 Mich. Telecomm. Tech. L. Rev. 61.

SOLOVE, D., "A Brief History of Information Privacy Law" (2006) *Proskauer on Privacy PLI* at I-25.

SOLOVE, D., “Privacy and Power: Computer Databases and Metaphors for Information Privacy”, (2001) 53 Stan. L. Rev. 1393.

SOLOVE, D., “Conceptualizing Privacy” (2002) 90 Cal. L. Rev. 1087.

SOLOVE, D., “Access and Aggregation: Public Records, Privacy and the Constitution” (2002) 86 Minn. L. Rev. 1137.

SOLOVE, D., “A Taxonomy of Privacy” (2006) 154:3 U. Penn. L. Rev. 477.

SOLOVE, D., “I’ve Got Nothing to Hide’ and Other Misunderstandings of Privacy” (2007) 44 San Diego Law Review 745.

SOLTANI, A. et al., “Flash Cookies and Privacy” (10 August 2009), online: SSRN <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862>.

STRAHILEVITZ, L., “Reputation Nation: Law in an Era of Ubiquitous Personal Information” (2008) 102 N.W. U. L. Rev. 1667.

SWEENEY, L., “Uniqueness of Simple Demographics in the U.S. Population” (2000) Laboratory for Int’l Data Privacy, Working Paper LIDAP-WP4.

SWIRE, P., “Financial Privacy and the Theory of High-Tech Government Surveillance” (1999) 77 Wash. U. L.Q. 461.

TRUDEL, P., “Privacy Protection on the Internet: Risk Management and Networked Normativity” in Serge Gutwirth et al., eds., *Reinventing Data Protection?* (Dordrecht, London: Springer, 2009) 317.

TRUDEL, P., “La protection de la vie privée dans les réseaux: des paradigmes alarmistes aux garanties effectives” (2006) 61 *Annales des télécommunications* 950.

TRUDEL, P., ABRAN, F. & DUPUIS, G., *Analyse du cadre réglementaire québécois et étranger à l’égard du pourriel, de l’hameçonnage et des logiciels espions*, Rapport préparé pour la Direction des politiques du ministère des services gouvernementaux du Québec (Montréal : Chaire L.R. Wilson et CRDP, 2007).

TRUDEL, P. & BENYEKHLEF K., “Approches et Stratégies pour Améliorer la Protection de la Vie Privée dans le Contexte des Inforoutes”, in *Mémoire présenté à la Commission de la Culture de l’Assemblée Nationale dans le Cadre de son Mandat sur l’Étude du rapport quiquennal de la commission d’accès l’information* (Montréal : CRDP, Université de Montréal, 1997).

TUROW, J. et al., “American Reject Tailored Advertising and Three Activities that Enable It” (29 September 2009), online: SSRN <http://ssrn.com/abstract=1478214>

VAN DEN HOVEN, J., “Privacy and the Varieties of Moral Wrong-doing in an Information Age” (1997) Computers and Society 33, online: <http://www.interwebbeheer.nl/img/pdf/test.pdf>

VAN DEN HOVEN, J., & VERMAAS, P., “Nano-Technology and Privacy: On Continuous Surveillance Outside the Panopticon” (2007) 32:3 Journal of Medicine and Philosophy 283, online: <http://dx.doi.org/10.1080/03605310701397040>

VAN ROMPAY, T. et al., "The Eye of the Camera: Effects of Security Cameras on Prosocial Behavior" (2009) 41:1 Env't & Behav. 60.

WARREN S. & BRANDEIS, L., "The Right to Privacy" (1890) 4:5 Harvard Law Review 193.

WATERS, N., "Rethinking information privacy: a third way in data protection?" (2000) PLPR 6, online: <http://www.austlii.edu.au/au/journals/PLPR/2000/6.html>.

WESTIN, A., "Privacy in the Workplace: How Well Does American Law Reflect American Values" (1996) 72 Chi.-Kent L. Rev. 271.

WILLBORN, S., "Consenting Employees: Workplace Privacy and the Role of Consent" (2006) 66 Louisiana Law Review 975.

WILLIAMS, F., *Internet Privacy Policies: A Composite Index for Measuring Compliance to the Fair Information Principles* (2006), online: <http://www.ftc.gov/os/comments/behavioraladvertising/071010feliciawilliams.pdf>.

WONG, R. & GARRIER, D., "Demystifying Clickstream Data: A European and U.S. Perspective" (2006) 20:2 Emory International l. Rev. 563.

WONG, R., "Data Protection Online: Alternative Approaches to Sensitive Data?" (2007) 2:1 J. Int'L Com. L. & Tech.

WONG, R., "The Shape of Things to Come: Swedish Developments on the Protection of Privacy" (2005) 2:2 Script-Ed 98.

WUCHEK, W., "Conspiracy Theory: Big Brother Enters the Brave New World of Health Care Reform" (2000) 3 Depaul J. Health Care L. 293.

ZARSKY, T., "Mine Your Own Business!: Making the Case for the Implications of Data Mining of Personal Information in the Forum of Public Opinion" (2002-03) 5 Yale J.L. & Tech. 1.

ZIMMERMAN, R., "The Way the 'Cookies' Crumble: Internet Privacy and Data Protection in the Twenty-First Century" (2000-2001) 4 N.Y.U. J. Legis. & Publ. Pol'y 439.

PUBLIC SECTOR DOCUMENTS (ISSUED BY PRIVACY COMMISSIONERS)

Office of the Privacy Commissioner of Canada (Canada)

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "The Privacy Commissioner of Canada's Position at the Conclusion of the Hearings on the Statutory Review of PIPEDA", Appendix III, "Work Product" Information, online: <http://www.priv.gc.ca/parl/2007/sub_070222_03_e.cfm>.

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, *Annual Report to Canada 2001-2002* (Ottawa: Office of the Privacy Commissioner of Canada, 2003) at Part Two, "Report on the Personal Information Protection and Electronic Documents Act, The Definition of Personal Information".

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, *Key Steps for Organizations in Responding to Privacy Breaches: Guidelines* (August 2007), at 2, online: <http://www.priv.gc.ca/information/guide/2007/gl_070801_02_e.asp>.

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, *OPCC Guidance Documents: Guidance on Covert Video Surveillance in the Private Sector* (May 2009), online: <http://www.priv.gc.ca/information/pub/gd_cvs_20090527_e.cfm>.

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, *A Privacy Handbook for Lawyers, PIPEDA and Your Practice* (Ottawa: Office of the Privacy Commissioner of Canada, 2011).

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, *Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting, and Cloud Computing* (May 2011), online: <http://www.priv.gc.ca/resource/consultations/report_201105_e.cfm>.

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, *Privacy and Online Behavioural Advertising*, Guidelines, December 2011, online: <http://www.priv.gc.ca/information/guide/2011/gl_ba_1112_e.pdf>.

Quebec (Commission de l'Accès de l'information du Québec)

COMMISSION DE L'ACCÈS À L'INFORMATION, *Rules for use of surveillance cameras with recording in public places by public bodies*, Quebec (June 2004).

COMMISSION DE L'ACCÈS À L'INFORMATION, *Rapport quinquennal 2011 : Technologies et vie privée à l'heure des choix de société* (Québec: Gouvernement du Québec, 2011).

COMMISSION DE L'ACCÈS À L'INFORMATION, "Using a fax machine" online: <http://www.cai.gouv.qc.ca/index-en.html>.

Commission Nationale de l'Informatique et des Libertés (France)

CNIL, *17e Rapport d'activité*, 73 (1997).

CNIL, Une recommandation destinée à encadrer la géolocalisation des véhicules des employés, 27 April 2006, online: <http://www.cnil.fr/la-cnil/actualite/article/article/une-recommandation-destinee-a-encadrer-la-geolocalisation-des-vehicules-des-employes/>.

CNIL, "L'adresse IP est une donnée à caractère personnel pour l'ensemble des CNIL européennes" (2 août 2007), online : CNIL <http://www.cnil.fr/la-cnil/actu-cnil/article/article/ladresse-ip-est-une-donnee-a-caractere-personnel-pour-lensemble-des-cnil-europeennes/>.

CNIL, *2008 Annual Report of the Commission Nationale de l'Informatique et des Libertés* (Paris: CNIL, 2008) at c. 1 "Measuring Diversity: Ten Recommendations".

CNIL, "La CNIL se prononce : le site note2be.com est illégitime au regard de la loi informatique et libertés" (6 March 2008).

CNIL, *Guide pour les employeurs et les salariés* (CNIL, 2010), online : <http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL_GuideTravail.pdf>.

CNIL, "Carton rouge pour les Pages Jaunes" (23 September 2011), online: <http://www.cnil.fr/la-cnil/actu-cnil/article/article/carton-rouge-pour-les-pages-jaunes/>.

CNIL, "La vidéosurveillance sur les lieux de travail", online : <http://www.cnil.fr/la-cnil/actu-cnil/article/article/la-videosurveillance-sur-les-lieux-de-travail/>.

OTHER PUBLIC SECTOR DOCUMENTS

Canada (Federal)

DEPARTMENT OF COMMUNICATIONS AND DEPARTMENT OF JUSTICE, *Privacy and Computers: A Report of a Task Force* (Ottawa: Information Canada, 1972).

INDUSTRY CANADA, "Electronic Commerce in Canada: Government of Canada Introduces Anti-Spam Legislation (CASL)", online: <http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/gv00521.html>.

INDUSTRY CANADA, The Working Group on Consumers and Electronic Commerce, "Internet and Bulk Unsolicited Electronic Mail" (SPAM), July 1999.

INDUSTRY CANADA, The Working Group on Consumers and Electronic Commerce, "E-mail marketing: Consumer Choices and Business Opportunities", Discussion Paper, January 2003.

STANDING COMMITTEE ON CITIZENSHIP AND IMMIGRATION, *A National Identity Card For Canada?* (Ottawa: Communication Canada, 2003) at Appendix B ("Preliminary Research on National ID Documents in Other Countries").

TREASURY BOARD OF CANADA SECRETARIAT, 2006 *Guidance Document: Taking Privacy into Account Before Making Contracting Decisions*, Issued to federal government institutions by the Treasury Board of Canada Secretariat, 2006, online: <http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/gd-do/gd-do-eng.asp>.

Canada (Provincial)

Alberta

ALBERTA SELECT SPECIAL PERSONAL INFORMATION PROTECTION ACT REVIEW COMMITTEE, *Final Report: November 2007* (Edmonton: 2007).

ALBERTA OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER, *Report of an Investigation into the Collection of Personal Information* (16 February 2010), online: <http://www.oipc.ab.ca/downloads/documentloader.ashx?id=2529>.

SERVICE ALBERTA, PIPA *Information Sheet 11: Notification of a Security Breach* (April 2010).

Quebec (Travaux Parlementaires)

LES TRAVAUX PARLEMENTAIRES (Québec), 34th législature, 2nd session, Commission permanente de la culture, cahier no 11 (February 23, 1993), pages 337-396.

LES TRAVAUX PARLEMENTAIRES (Québec), 34th législature, 2nd session, Commission permanente de la culture, cahier no 12 (February 24, 1993), pages 397-437.

LES TRAVAUX PARLEMENTAIRES (Québec), 34th législature, 2nd session (du 19 mars 1992 au 10 mars 1994), Commission permanente de la culture, cahier no 13 (March 1, 1993), pages 439-475.

LES TRAVAUX PARLEMENTAIRES (Québec), 34th législature, 2nd session, Commission permanente de la culture, cahier no 14 (March 2, 1993), pages 477-543.

LES TRAVAUX PARLEMENTAIRES (Québec), 34th législature, 2nd session, Commission permanente de la culture, cahier no 15 (March 3, 1993), pages 545-595.

LES TRAVAUX PARLEMENTAIRES (Québec), 34th législature, 2nd session, Commission permanente de la culture, cahier no 16 (March 4, 1993), pages 597-643.

LES TRAVAUX PARLEMENTAIRES (Québec), 34th législature, 2nd session, Commission permanente de la culture, cahier no 23 (May 13, 1993), pages 837-874.

LES TRAVAUX PARLEMENTAIRES (Québec), 34th législature, 2nd session, Commission permanente de la culture, cahier no 32 (June 8, 1993), pages 1163-1187.

LES TRAVAUX PARLEMENTAIRES (Québec), 34th législature, 2nd session, Assemblée, cahier no 73 (March 16, 1993), pages 5357-5377.

LES TRAVAUX PARLEMENTAIRES (Québec), 34th législature, 2nd session, Assemblée, Motion, cahier no 73 (March 16, 1993), pages 5377.

LES TRAVAUX PARLEMENTAIRES (Québec), 34th législature, 2nd session, Assemblée, cahier no 112 (June 14, 1993), pages 7633-7647.

European Union

ARTICLE 29 DATA PROTECTION WORKING PARTY, *Working Document: Privacy on the Internet: An Integrated EU Approach to Online Data Protection*, [2000] 5063/00EN/FINAL, WP 37.

ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 2/2002: The Use of Unique Identifiers in Telecommunications Terminal Equipments: the Example of IPv6*, [2002] 10750/02/EN/Final, WP 58.

ARTICLE 29 DATA PROTECTION WORKING PARTY, *Working document on data protection issues related to RFID technology*, [2005] 10107/05/EN.

ARTICLE 29 DATA PROTECTION WORKING PARTY, *Results of the Public Consultation on Article 29 Working Document 105 on Data Protection Issues Related to RFID Technology*, [2005] 1670/05/EN.

ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 4/2007 on the concept of personal data*, [2007] 01248/07/EN WP 136.

ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 1/2008 on data protection issues related to search engines*, [2008] 00737/EN WP 148.

ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 1/2010 on the concepts of "controller" and "processor"*, [2010] 00264/10/EN, WP 169, online: <http://www.cbpweb.nl/downloads_med/med20100219_C.03%20DC-DP_Opinion_ADOPTED.pdf>.

ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 2/2010 on online behavioural advertising*, [2010] 00909/10/EN WP 171.

ARTICLE 29 DATA PROTECTION WORKING PARTY, *Letter from the Article 29 Working Party to search engine operators (Google, Microsoft, Yahoo!)* (26 May 2010), online: <http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2010-others_en.htm>.

CONSEIL DE L'EUROPE, Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, *Rapport sur l'application des principes de protection des données aux réseaux mondiaux de télécommunications. L'autodétermination informationnelle à l'ère de l'Internet : Éléments sur la réflexion sur la Convention no 108 destinés au travail futur du Comité consultatif*, Strasbourg, 18 novembre 2004.

COUNCIL OF EUROPE, PA, *Motion for a Resolution calling for a study of the problem of legislation and control with regard to new technical devices for eavesdropping*, Doc. 2226 (1967).

COUNCIL OF EUROPE, PA, *Motion for a Resolution on Human rights and modern scientific and technological developments*, Doc. 2206 (1967).

COUNCIL OF EUROPE, Explanatory Memorandum of the Consultative Assembly of the Council of Europe, *Report on human rights and modern scientific and technological developments*, Doc. 2326 (1968).

COUNCIL OF EUROPE, PA, 16th sitting, *on the Human rights and modern scientific and technological developments*, Doc. 2326 (1968), Directed to the Legal Committee.

COUNCIL OF EUROPE, Consultative Assembly of the Council of Europe, *Recommendation (509) 68 of 31 January 1968, on human rights and modern scientific and technological developments.*

COUNCIL OF EUROPE, PA, *Resolution 428 containing a declaration on mass communication media and human rights* (1970).

COUNCIL OF EUROPE, Committee of Ministers, 26 September 1973, 224th meeting of the Ministers' Deputies, *Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector*.

COUNCIL OF EUROPE, Committee of Ministers, *Explanatory Report: Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector.*

COUNCIL OF EUROPE, Committee of Ministers, 20 September 1974, 236th meeting of the Ministers' Deputies, *Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector.*

COUNCIL OF EUROPE, Committee of Ministers, *Explanatory Report: Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector.*

COUNCIL OF EUROPE, PA, *Report on data processing and the protection of human rights*, Doc. 4472 (1980).

COUNCIL OF EUROPE, PA, *Opinion on data processing and the protection of human rights presented by the Legal Affairs Committee*, Doc. 4484 (1980).

COUNCIL OF EUROPE, Committee of Ministers, *Recommendation No. R (97) 5, On the Protection of Medical Data.*

EC, *Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce*, [2000] O.J., L 215/7.

EC, Data Protection Commissioner, *Security Measures for Personal Data: A Guide to the New Data Protection Rules* (2001), online: <http://www.dataprotection.ie/documents/legal/6si626-01.htm>.

EC, *Commission Decision 2002/2/EC of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act*, [2002] O.J. L. 002/0013.

EC, Peter Hustinx, *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on the follow up of the Work Programme for better implementation of the Data Protection Directive*, [2007] O.J., C. 255/1.

EC, Commission, *Report from the Commission: First Report on the Implementation of the Data Protection Directive (95/46/EC)*, COM (2003) 265 (Brussels: EC, 2003).

The *2002 Proposals for Amendment of the Data Protection Directive (95/46/EC),* made by Austria, Finland, Sweden and the United Kingdom - Explanatory Note, online: <http://www.dca.gov.uk/ccpd/dpdamend.htm>.

Foreign Jurisdictions

Australia

AUSTL., COMMONWEALTH, LAW REFORM COMMISSION, *For Your Information: Australian Privacy Law and Practice* (Report No. 108) (Canberra: Australian Government Publishing Service, 2008).

AAMI, *Submission PR 147,* 29 January 2007 [Prepared for publication and for consideration by the Australian Commonwealth Law Reform Commission].

AUSTRALIAN FEDERAL POLICE, *Submission PR 186,* 9 February 2007 [Prepared for publication and for consideration by the Australian Commonwealth Law Reform Commission].

AUSTL., OFFICE OF THE PRIVACY COMMISSIONER, *Submission PR 499,* 20 December 2007 [Prepared for publication and for consideration by the Australian Commonwealth Law Reform Commission].

CENTRE FOR LAW AND GENETICS, *Submission PR 127*, 16 January 2007 [Prepared for publication and for consideration by the Australian Commonwealth Law Reform Commission].

CYBERSPACE LAW AND POLICY CENTRE UNSW, *Submission PR 487,* 19 December 2007 [Prepared for publication and for consideration by the Australian Commonwealth Law Reform Commission].

GOVERNMENT OF SOUTH AUSTRALIA, *Submission PR 187*, 12 February 2007 [Prepared for publication and for consideration by the Australian Commonwealth Law Reform Commission].

GREENLEAF, G., WATERS, N., and BYGRAVE, L., Cyberspace Law and Policy Centre UNSW, *Submission PR 183,* 9 February 2007 [Prepared for publication and for consideration by the Australian Commonwealth Law Reform Commission].

LAW COUNCIL OF AUSTRALIA, *Submission PR 177,* 8 February 2007 [Prepared for publication and for consideration by the Australian Commonwealth Law Reform Commission].

VEDA ADVANTAGE, *Submission PR 163,* 31 January 2007 [Prepared for publication and for consideration by the Australian Commonwealth Law Reform Commission].

NATIONAL HEALTH AND MEDICAL RESEARCH COUNCIL, *Submission PR 114,* 15 January 2007 [Prepared for publication and for consideration by the Australian Commonwealth Law Reform Commission].

China

OFFICE OF THE PRIVACY COMMISSIONER FOR PERSONAL DATA, Hong Kong, *Report Published under Section 48 (2) of the Personal Data (Privacy) Ordinance (Cap. 486), Report Number R07-3619* (14 March 2007).

GOVERNMENT OF HONG KONG, Press Releases, “LCQ17: IP addresses as personal data” (3 May 2006), online: <http://www.info.gov.hk/gia/general/200605/03/P200605030211.htm>.

Scotland

HOME OFFICE, LORD CHANCELLOR'S OFFICE' SCOTTISH OFFICE (Chairman The Rt. Hon, Kenneth Younger), *Report of the Committee on Privacy*, presented to Parliament by the Secretary of State for the Home Department, the Lord High Chancellor and the Secretary of State for Scotland by Command of Her Majesty, July 1972.

Spain

AGENCIA ESPANOLA DE PROTECCION DE DATOS, Statement on search engines (2007), online: <http://www.samuelparra.com/agpd/canaldocumentacion/recomendaciones/common/pdfs/declaracion_aepd_buscadores_en.pdf>.

United Kingdom

CHAIRMAN SIR NORMAN LINDOP, *Report of the Committee on Data Protection: Presented to Parliament by the Secretary of State for the Home Department by Command of Her Majesty* (London, UK: H.M.S.O., 1978).

INFORMATION COMMISSIONER'S OFFICE, *Data Protection Strategy, Consultation Draft*, U.K., June 2007.

INFORMATION COMMISSIONER'S OFFICE, *Personal Information online, Code of Practice,* U.K., July 2010.

United States

FEDERAL TRADE COMMISSION, "Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles" (20 December 2007), online: FTC <http://www.ftc.gov/opa/2007/12/principles.shtm>.

FEDERAL TRADE COMMISSION, Staff, *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising* (February 2009), online: FTC <http://www.ftc.gov/os/2009/02/P0085400behavadreport.pdf>.

FEDERAL TRADE COMMISSION, *Protecting Consumer Privacy in an Era of Rapid Change*: *A Proposed Framework for Businesses and Policymakers*, Preliminary Staff Report (December 2010).

FEDERAL TRADE COMMISSION, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (March 2012).

OFFICE OF SCIENCE AND TECHNOLOGY OF THE EXECUTIVE OFFICE OF THE PRESIDENT, *Privacy and Behavioral Research* (Washington, D.C.: 1967).

U.S. DEPARTMENT OF HEALTH, EDUCATION AND WELFARE: U.S. Department of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens* (Washington: U.S. Government Printing Office, 1973).

PRESENTATIONS AND SPEECHES (CONFERENCES)

BOURCIER, D., *To Create Commons in order to Open Data* (CNRS and Creative Commons France, France).

EUROPEAN PARLIAMENT, COMMITTEE ON CIVIL LIBERTIES, Justice and Home Affairs, "Public Seminar Data protection on the Internet (Google-DoubleClick and other case studies)", Monday 21 January 2008, Brussels, Room PHS 3C50.

RADWANSKI, G., "Address to the Privacy Lecture Series" (Toronto, 26 March 2001), online: <http://privacy.openflows.org/pdf/radwanski_march26_2001.pdf>.

SERRES, M., "Les nouvelles technologies: révolution culturelle et cognitive", online conference: <http://interstices.info/jcms/c_33030/les-nouvelles-technologies-revolution-culturelle-et-cognitive?portal=j_97&printView=true>.

STODDART, J., "Respecting Privacy Rights in the World of Online Behavioural Advertising" (Remarks delivered at the Marketing and the Law Conference, Toronto, 6 December 2011).

NORDIC CONFERENCE, *Conclusions of the Nordic Conference of International Jurists on the Right of Privacy*, Stockholm, 1967.

PRIVACY COMMISSIONER OF CANADA, "Speech at the Freedom of Information and Protection of Privacy conference" (June 13, 2002) cited online: <http://www.tbs-sct.gc.ca/pgol-pged/piatp-pfefvp/course1/mod1/mod1-2-eng.asp>.

REMARKS OF FTC CHAIRMAN TIM MURIS, Privacy 2001 Conference (4 October 2001), online: <http://www.ftc.gov/speeches/muris/privisp1002.shtm>.

NEWSPAPER ARTICLES AND NEWS

AGENCE FRANCE-PRESSE WASHINGTON, "Twitter acquiert une entreprise de géolocalisation" *La presse affaires* (24 December 2009), online : Lapresse.ca <http://lapresseaffaires.cyberpresse.ca/economie/technologie/200912/24/01-933976-twitter-acquiert-une-entreprise-de-geolocalisation.php>.

ALAM KHAN, M., "Technology Creates Tough Environment for Retailers" (13 January 2003), online: DMNews <http://www.dmnews.com/cgi-bin/artprevbot.cgi?article_id=22682>.

ANDRES, "Information self-determination in the Google Age" (19 April 2010), online: Technollama Blog <http://www.technollama.co.uk/information-self-determination-in-the-google-age>.

ANDERSON, N., "AOL releases search data on 500,000 users (updated)" (7 August 2006), online: ARS technica <http://arstechnica.com/uncategorized/2006/08/7433/>.

ANDERSON, N., "FBI uses spyware to bust bomb threat hoaxters" (18 July 2007), online: ARS technica <http://arstechnica.com/security/2007/07/fbi-uses-virus-to-bust-bomb-threat-hoaxster/>.

ARTHUR, C., "iPhone keeps record of everywhere you go" *The Guardian* (20 April 2011), online: The Guardian <http://www.guardian.co.uk/technology/2011/apr/20/iphone-tracking-prompts-privacy-fears>.

BAIG, E., "Internet Users Say, Don't Track Me" (14 December 2010), online: USA TODAY <http://www.usatoday.com/tech/news/2010-12-14-donottrackpoll14_ST_N.htm>.

BANKSTON, K., "Facebook's New Privacy Changes: The Good, The Bad, and The Ugly" (9 December 2009), online: The Electronic Frontier Foundation <https://www.eff.org/deeplinks/2009/12/facebooks-new-privacy-changes-good-bad-and-ugly>.

BARNARO, M. & ZELLER, T., "A Face is Exposed for AOL Searcher No. 4417749", *New York Times* (9 August 2006) at A1.

BARWICK, H., "Facebook facial recognition should be opt in, not opt out" (10 June 2011), online: Computerworld <http://www.computerworld.com.au/article/389810/facebook_facial_recognition_should_opt_opt/>.

BERTOLUCCI, J., "Twitter Adds Location-Sharing: I'm Eating Tacos…In Texarkana" (12 March 2010), online: PC World <http://www.pcworld.com/article/191457/twitter_adds_locationsharing_im_eating_tacos_in_texarkana.html>.

BILTON, N., "Foursquare Introduces New Tools for Businesses" *The New York Times* (9 March 2010), online: The New York Times <http://bits.blogs.nytimes.com/2010/03/09/foursquare-introduces-new-tools-for-businesses/?partner=rss&emc=rss>.

BLATCHFORD, C., "A precedent on Internet privacy in the making", *The Globe & Mail* (9 April 2008).

BRANIGIN, W., "Employment Database Proposal Raises Cries of 'Big Brother'", *The Washington Post* (3 October 1995) at A17.

BROWN, D., "Happy 20th birthday, World Wide Web!" *Cnet news* (6 August 2011), online: cnet.com, <http://news.cnet.com/8301-10797_3-20089085-235/happy-20th-birthday-world-wide-web/>.

BROWNLEE, J., "Facebook to become location aware in April" (9 March 2010), online: geek.com <http://www.geek.com/articles/news/facebook-to-become-location-aware-in-april-2010039/#ixzz0ojX7rsOf>.

CANADIAN PRESS (THE), "Privacy commissioner looking at how Facebook gets data" (18 January 2010), online: ctv.ca <http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/20100118/facebook_privacy_100118/20100118/?hub=SciTech>.

CARLSON, N., "WARNING: Google Buzz Has A Huge Privacy Flaw" (10 February 2010), online: Business Insider <http://www.businessinsider.com/warning-google-buzz-has-a-huge-privacy-flaw-2010-2#ixzz1XIxQ9N8V>.

CBC, "Internet privacy attitudes shifting: report, Learning about privacy issues raises level of concern" (16 April 2010), online: CBC News <http://www.cbc.ca/consumer/story/2010/04/16/con-online-privacy.html>.

CBC NEWS, "Depressed woman loses benefits over Facebook photos" (21 November 2009), online: CBC News <http://www.cbc.ca/news/canada/montreal/story/2009/11/19/quebec-facebook-sick-leave-benefits.html>.

CHENG, J., "Apple announces iPhone launch in France: November 29", online: ars technica <http://arstechnica.com/apple/2007/10/apple-announces-iphone-launch-in-france-november-29/>.

CHENG, J., "iPhone user privacy at risk from apps that transmit personal info" (3 October 2010), online: Ars Technica <http://arstechnica.com/apple/news/2010/10/iphone-user-privacy-at-risk-from-apps-that-transmit- personal-info.ars>.

CLABURN, T., "Social Networks Leak Personal Information" *InformationWeek* (24 August 2009), online: <http://www.informationweek.com/news/internet/social_network/showArticle.jhtml?articleID=219401268>.

CLIFFORD, S., "Your Online Clicks Have Value, for Someone Who Has Something to Sell" *New York Times* (25 March 2009), online: The New York Times <http://www.nytimes.com/2009/03/26/business/media/26adco.html>.

DAVIS, W., "Court: IP Addresses Are Not 'Personally Identifiable' Information" (6 July 2009), online: Online Media Daily <http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=109242>.

EATON, K., "Geotagging's Seasonal Danger: Burglary" (29 December 2009), online: Fast Company <http://www.fastcompany.com/blog/kit-eaton/technomix/geotaggings-seasonal-danger-burglary?partner=rss>.

EDRI, "French minister: copyright above privacy" (3 November 2005), online: <http://www.edri.org/edrigram/number3.22/copyright>.

EUNJUNG CHA, A., "Mobile coupons track customers" *The Washington Post* (27 June 2010), online: The Washington Post <http://www.washingtonpost.com/wp-dyn/content/article/2010/06/26/AR2010062600223.html>.

FAUCHER, P., "Facebook : IBM règle son litige avec une employée" *Cyberpresse* (10 January 2012), online : Cyberpresse <http://technaute.cyberpresse.ca/nouvelles/internet/201201/10/01-4484477-facebook-ibm-regle-son-litige-avec-une-employee.php>.

FRIEDMAN, T., "Foreign Affairs: Little Brother", *The New York Times* (26 September 1999) at s. 4 at 17.

GABIZON, C., “Vers l'instauration d'un ‘droit à l'oubli’ numérique” *Le Figaro* (13 November 2009), online : <http://www.lefigaro.fr/web/2009/11/13/01022-20091113ARTFIG00012-vers-l-instauration-d-un-droit-a-l-oubli-numerique-.php>.

GLEICK, J., “Big Brother Is Us: Our Privacy is Disappearing, But Not by Force. We’re Selling it, Even Giving it Away”, *The New York Times* (29 September 1996) (magazine) at 130.

GONUL, F., “Stereotyping Bites the Dust; Marketers No Longer Focusing On Demographic Profiling” (2002) Pitt. Post-Gazette (Pa.) at B3.

GORDON CROVITZ, L., “Privacy Isn't Everything on the Web” *The Wall Street Journal* (24 May 2010), online: The Wall Street Journal <http://online.wsj.com/article/SB10001424052748704546304575260470054326304.html>.

GRALLA, P., “Google CEO Schmidt: We can know everything about you” (18 February 2010), online: Computer World <http://blogs.computerworld.com/15614/google_ceo_schmidt_we_can_know_everything_about_you>.

GRANT, T., “Lenders using Facebook, Twitter to gather borrower information” *Pittsburgh Post-Gazette* (28 May 2010), online: post-gazette.com <http://www.post-gazette.com/pg/10148/1061287-28.stm>.

GREENE, T., “Schneier: Fight for Privacy Or Kiss it Good-Bye” (9 March 2010), online: CIO <http://www.cio.com/article/569914/Schneier_Fight_for_Privacy_Or_Kiss_it_Good_Bye?page=2&taxonomyId=3089>.

HANNA, L., “Reputations Online, One in seven central Kentucky employers use social networking sites to screen candidates” Lex Weekly (15 April 2010), online: <http://www.lexweekly.com/Articles-c-2010-04-15-92201.113117_Reputations_Online.html>.

HOOFNAGLE, C., “The privacy Machiavellis” (25 May 2010), online: <http://www.sfgate.com/cgi-bin/article.cgi?f=%2Fc%2Fa%2F2010%2F05%2F24%2FED101DJPE1.DTL>.

HUFFINGTON POST (THE), “Craziest Google Street View Shots OF ALL TIME (PHOTOS, POLL)” (18 March 2010), online: The Huffington Post <http://www.huffingtonpost.com/2009/11/15/google-street-view-funny_n_357433.html>.

JERNIGAN, C. & MISTREE, B., “Gaydar: Facebook Friendships expose sexual orientation” (2009) 14:10 First Monday, online: First Monday <http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2611/2302>.

JESDANUN, A., “AOL: Breach of Privacy Was a Mistake”, *The Washington Post* (7 August 2006) at A1.

JORDAN PRESS, “Google tries to allay concerns over new privacy Policy” *The Montreal Gazette* (29 February 2012), online: <http://www.montrealgazette.com/technology/Google+tries+allay+privacy+concerns/6230292/story.html>.

KARI, S., “Television beer pitchman at centre of pornography, privacy battle”, *National Post* (9 April 2008).

KIRKPATRICK, M., “The Inner Circles of 10 Geek Heroes on Twitter” (20 March 2009), online: ReadWriteWeb <http://www.readwriteweb.com/archives/the_inner_circles_of_10_geek_heroes_on_twitter.php>.

KIRKPATRICK, M., “The Man Who Looked Into Facebook’s Soul” (8 February 2010), online: ReadWriteWeb <http://www.readwriteweb.com/archives/facebook_user_data_analysis.php>.

KIRKPATRICK, M., “Facebook Becomes More Racially Diverse, Ought to Release Data for Outside Analysis” (16 December 2009), online: ReadWriteWeb <http://www.readwriteweb.com/archives/facebook_scientists_dissect_facebook_say_its_alive.php>.

KIRKPATRICK, M., “Location Data Sensitive Like Medical Information, Says Congressional Witness” *The New York Times* (25 February 2010), online: The New York Times <http://www.nytimes.com/external/readwriteweb/2010/02/25/25readwriteweb-location-data-sensitive-like-medical-inform-75294.htm>.

KOLLEWE, J., “Office of Fair Trading to probe use of personal data by online retailers”, *The Guardian* (15 October 2009).

L. J., “L'Europe veut faire de la géolocalisation une donnée personnelle” (13 May 2011), online : Numerama <http://www.numerama.com/magazine/18787-l-europe-veut-faire-de-la-geolocalisation-une-donnee-personnelle.html>.

LAM, E., “Smartphones are smarter than you are” *Financial Post* (31 May 2010).

LAWFORD, J., counsel with the Public Interest Advocacy Centre in Ottawa, in Michael McKiernan, “New federal privacy, anti-spam bills get mixed reviews” *Law Times* (31 May 2010), online: Law Times <http://www.lawtimesnews.com/201005316982/Headline-News/New-federal-privacy-anti-spam-bills-get-mixed-reviews>.

LEE, J., “Fighting Back When Someone Steals Your Name”, *The New York Times* (8 April 2001) at 8, § 3.

LOHR, S., “How Privacy Vanishes Online” *The New York Times* (16 March 2010), online: The New York Times <http://www.nytimes.com/2010/03/17/technology/17privacy.html?emc=eta1>.

LOHR, S., “Netflix Cancels Contest After Concerns Are Raised About Privacy” *New York Times* (12 March 2010), online: The New York Times <http://www.nytimes.com/2010/03/13/technology/13netflix.html>.

LOHR, S., “Redrawing the Route to Online Privacy” *The New York Times* (27 February 2010), online: The New York Times <http://www.nytimes.com/2010/02/28/technology/internet/28unbox.html>.

LOWERY, A., “How Online Retailers Stay a Step Ahead of Comparison Shoppers” *The Washington Post* (12 December 2010), online: The Washington Post <http://www.washingtonpost.com/wp-dyn/content/article/2010/12/11/AR2010121100143.html>.

HAMILTON, D., Daniel Hamilton, “Big Brother Watch: Internet Eyes Invades Privacy” (4 March 2011), online: <http://www.outlookseries.com/A0998/Security/3603_Daniel_Hamilton_Big_Brother_Watch_Internet_Eyes_Invades_Privacy_Daniel_Hamilton.htm>.

HARTLEY, M., “YouTube told to hand over users’ data” *Globe and Mail* (3 July 2008).

HELFT, M., “Judge Sides With Google in Viacom Video Suit” *The NY Times* (23 June 2010), online: <http://www.nytimes.com/2010/06/24/technology/24google.html>.

MACAVINTA, C., “Privacy advocates rally against DoubleClick-Abacus merger” CNET News (22 November 1999), online: CNET <http://news.cnet.com/Privacy-advocates-rally-against-DoubleClick-Abacus-merger/2100-1023_3-233413.html#ixzz1O8HfI0GS>.

MACLEAN, W., “Is the Big Brother watching you??” *Balkan news* (28 June 2010), online: Balkans.com <http://www.balkans.com/open-news.php?uniquenumber=62265>.

MACRONIN, “Twitter & FaceBook Tapping / Law enforcement and its social surveillance” (13 December 2009), online: Privacy Digest <http://www.privacydigest.com/2009/12/13/twitter%20facebook%20tapping%20law%20enforcement%20and%20its%20social%20surveillance>.

MCKERNAN, M., “New federal privacy, anti-spam bills get mixed reviews” *Law Times* (31 May 2010), online: Law Times <http://www.lawtimesnews.com/201005316982/Headline-News/New-federal-privacy-anti-spam-bills-get-mixed-reviews>.

MCMILLAN, R., “Google Buzz Criticized for Disclosing Gmail Contacts” *IDG News* (10 February 2010), online: PC World <http://www.pcworld.com/article/189081/google_buzz_criticized_for_disclosing_gmail_contacts.html>.

MELANSON, M., “Facebook Adds Facial Recognition” (2 July 2010), online: Read Write Web <http://www.readwriteweb.com/archives/facebook_adds_facial_recognition.php?utm_source=twitterfeed&utm_medium=twitter&utm_campaign=Feed%3A+readwriteweb+%28ReadWriteWeb%29&utm_content=Twitter>.

MOSES, A., “Facebook users 'don't want complete privacy': Zuckerberg” (24 May 2010), online: theage.com <http://www.theage.com.au/technology/technology-news/facebook-users-dont-want-complete-privacy-zuckerberg-20100524-w54g.html>.

MURPHY, E., “Tracking Grocery Hot Spots”, *Portland Press Herald* (27 January 2004).

NAKASHIMA, E., "The Legal Tangles Of Data Collection" *The Washington Post* (16 January 2007) at A09, online: The Washington Post <http://www.washingtonpost.com/wp-dyn/content/article/2007/01/15/AR2007011501301_pf.html>.

OATES, J., "Sweden: IP Addresses are Personal… Unless You're a Pirate" (18 June 2009), online: The Register <http://www.theregister.co.uk/2009/06/18/sweden_ip_law>.

O'HARROW, R., "Bargains at a Price: Shoppers' Privacy; Cards Let Supermarkets Collect Data", *The Washington Post* (31 December 1998) at A1.

PARR, B., "Twitter's Website Now Attaches Location to Tweets [PICS]" (10 March 2010), online: Mashable <http://mashable.com/2010/03/10/twitter-geolocation-tweets/>.

POULSEN, K., "FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats" (18 July 2007), online: WIRED <http://www.wired.com/print/politics/law/news/2007/07/fbi_spyware>.

RFI, "La France plaide pour le 'droit à l'oubli' sur internet" (15 November 2009), online : RFI <http://www.rfi.fr/contenu/20091115-droit-loubli-internet>.

RICHMOND, R., "Apple's Plans for iPhone Location Privacy" *The New York Times* (8 April 2010), online: The New York Times <http://gadgetwise.blogs.nytimes.com/2010/04/08/apples-plans-for-iphone-location-privacy/>.

ROBBERSON, T., "Plan for Student Database Stirs Opposition in Fairfax", *The Washington Post* (9 January 1997) at A1.

SAWERS, P., "Could Facebook reach one billion users in 2011?" (10 July 2011), online: thenextweb <http://thenextweb.com/socialmedia/2011/01/20/could-facebook-reach-one-billion-users-in-2011/>.

SCHNEIER, B., "Google And Facebook's Privacy Illusion" (6 April 2010), online: Forbes.com <http://www.forbes.com/2010/04/05/google-facebook-twitter-technology-security-10-privacy.html>.

SHAH. D., "CCTV site Internet Eyes hopes to help catch criminals" *BBC News* (3 October 2010), online: BBC News <http://www.bbc.co.uk/news/uk-11460897>.

SHANKLAND, S., "Google begins blurring faces in Street View" *Cnet News* (27 August 2010), online: Cnet.com <http://news.cnet.com/8301-10784_3-9943140-7.html>.

SHEPPARD, M.-A., "Google Releases Data on Government Requests for Private User Data" (21 April 2010), online: Slaw <http://www.slaw.ca/2010/04/21/google-releases-data-on-government-requests-for-private-user-data/>.

SCHONFELD, E., "Privacy-Per-Post: Facebook Rolls Out Its New Privacy Settings" (9 December 2009), online: Tech Crunch <http://techcrunch.com/2009/12/09/facebook-privacy-per-post/>.

SCHUSTER, H., & FRIEDEN, T., "Lawyer wrongly arrested in bombings: 'We lived in 1984'" (29 November 2006), online: CNN Justice <http://articles.cnn.com/2006-11-29/justice/mayfield.suit_1_train-bombings-brandon-mayfield-madrid?_s=PM:LAW>.

SINGER, N., "When 2+2 Equals a Privacy Question" *The New York Times* (18 October 2009), online: The New York Times <http://www.nytimes.com/2009/10/18/business/18stream.html?_r=3&adxnnl=1&adxnnlx=1256572818-Q9UvohAQV7pfxZ1TkU/C+Q>.

THOMPSON, D., "The Future of Privacy: Facial Recognition, Public Facts, and 300 Million Little Brothers" (11 June 2010), online: The Volokh Conspiracy <http://volokh.com/2010/06/11/the-future-of-privacy-facial-recognition-public-facts-and-300-million-little-brothers/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+volokh%2Fmainfeed+%28The+Volokh+Conspiracy%29&utm_content=Google+Reader>.

THOMPSON, H., "Latest numbers show Canada has over 25.5 million wireless customers" (16 January 2012), online: digitalhome.ca <http://www.digitalhome.ca/2012/01/latest-numbers-show-canada-has-over-25-5-million-wireless-customers/>.

VALENTINO-DEVRIES, J., "As Location-Sharing Services Grow, Privacy Concerns Do Too" *The Wall Street Journal* (10 March 2010), online: The Wall Street Journal <http://blogs.wsj.com/digits/2010/03/10/as-location-sharing-services-get-more-popular-privacy-concerns-grow/?mod=wsj_share_twitter>.

VILCHES, J., "Google proposes global privacy standard" (14 September 2007), online: Techspot <http://www.techspot.com/news/27032-google-proposes-global-privacy-standard.html>.

WILLIAMS, C., "Apple under pressure over iPhone location tracking" *The Telegraph* (21 April 2011), online: The Telegraph <http://www.telegraph.co.uk/technology/apple/8466357/Apple-under-pressure-over-iPhone-location-tracking.html>.

WHITE, A., "IP Addresses Are Personal Data, E.U. Regulator Says", *Washington Post* (22 January 2008) at D01.

WHITTEN, A. & FLEISCHER, P., "Le droit à l'oubli ne doit pas aboutir à une possible censure" *Les Echos* (20 April 2010), online : LesEchos.fr <http://www.lesechos.fr/info/comm/020487929397--le-droit-a-l-oubli-ne-doit-pas-aboutir-a-une-possible-censure-.htm>.

WOOD, M., "Google Buzz: Privacy nightmare" (10 February 2010), online: cnet.com. <http://news.cnet.com/8301-31322_3-10451428-256.html#ixzz1XIwhyWHP>.

WORTHAM, J., "More Employers Use Social Networks to Check Out Applicants", *The New York Times* (20 August 2009).

RADIO-CANADA, "Le questionnaire court reste obligatoire" (30 June 2010), online: Radio-Canada.ca <http://www.radio-canada.ca/nouvelles/National/2010/06/29/003-recensement-fin-obligation.shtml>.

RADIO-CANADA, "Québec désapprouve à son tour" (15 July 2010), online: Radio-Canada.ca <http://www.radio-canada.ca/nouvelles/National/2010/07/15/003-recensememement-opposition-qc.shtml>.

RADIO-CANADA, “Trois plaintes en dix ans” (15 July 2010), online: Radio-Canada.ca <http://www.radio-canada.ca/nouvelles/National/2010/07/14/004-recensement-vie-privee.shtml>.

SEARCH ENGINE ONLINE, “Google Ordered To Turn Over All Personal YouTube Viewing Records To Viacom”, online: Search Engine World <http://www.searchengineworld.com/google-search/3458026.htm>.

SOCIALATOR, “Scientists Develop World’s Fastest Program to Find Patterns in Social Networks” (2 July 2012), online: Socialator <http://socialator.com/scientists-develop-worlds-fastest-program-to-find-patterns-in-social-networks/1609>.

WEEK (THE), “Why you can't get old in Hollywood: Hollywood industry groups are trying to stop the Internet Movie Database from publishing their members' birth dates. A serious privacy issue — or just Tinseltown vanity?” The week (21 June 2010), online: The Week <http://theweek.com/article/index/204277/why-you-cant-get-old-in-hollywood>.

WRIGHT, R., “Google Launches New Site Detailing Government Data Requests” (21 April 2010), online: CRN <http://www.crn.com/software/224500123;jsessionid=YGOXRKPKTN2A3QE1GHPCKHWATMY32JVN>.

OTHER DOCUMENTS (INDUSTRY, SURVEYS, STUDIES, BLOGS)

APPLE, “Apple Q&A on Location Data” *Apple Press Info* (27 April 2011), online: Apple <http://www.apple.com/pr/library/2011/04/27location_qa.html>.

BARTH, D., “The Bright Side of Sitting in Traffic: Crowdsourcing road congestion data” (25 August 2009), online: Official Google Blog <http://googleblog.blogspot.com/2009/08/bright-side-of-sitting-in-traffic.html>.

BIGRESEARCH, “Consumer Awareness of RFID Technology Now Stands at 42.4%, Up Dramatically From 28.2% Just One Year Ago” (15 November 2005), online: Marketwire <http://www.marketwire.com/press-release/consumer-awareness-rfid-technology-now-stands-424-up-dramatically-from-282-just-one-668531.htm>.

BERKMAN CENTER FOR INTERNET AND SOCIETY, Harvard University, “Tastes, Ties, and Time: Facebook data release” (25 September 2008), online: <http://cyber.law.harvard.edu/node/4682>.

BRICKLEY, D., “YouAndYouAndYouTube: Viacom, Privacy and the Social Graph API” (3 July 2008), online: danbri’s foaf stories <http://danbri.org/words/2008/07/03/359#comment-15692>.

BUSINESS SOFTWARE ALLIANCE (THE), “Online Security, Traffic Data and IP addresses” (2008) Review of the Regulatory Framework for Electronic Communications, online: <http://www.statewatch.org/news/2008/oct/eu-datret-bas.pdf>.

CANTON, D., “Changes to privacy laws vague” (28 June 2010), online: elegal <http://canton.elegal.ca/2010/06/28/changes-to-privacy-laws-vague/>.

CENTER FOR DEMOCRACY & TECHNOLOGY, *CDT's guide to online privacy* (22 October 2009), online: <http://www.cdt.org/privacy/guide/start>.

CLELAND, S., "Americans Want Online Privacy: Per New Zogby Poll" (8 June 2010), online: The Precursor Blog <http://www.precursorblog.com/content/americans-want-online-privacy-new-zogby-poll>.

CROSSTAB INC., *Online Reputation in a Connected World* (Jan. 2010).

CUTTS, M., "Using data to fight webspam" (27 June 2008), online: Official Google Blog <http://googleblog.blogspot.com/2008/06/using-data-to-fight-webspam.html>.

ELECTRONIC PRIVACY INFORMATION CENTRE & PRIVACY INTERNATIONAL, *Privacy and Human Rights 2002: An international Survey of Privacy Laws and Developments* (Washington, D.C., London, U.K.; Electronic Privacy Information Center, Privacy International, 2002).

FLEISCHER, P., "Are IP addresses 'Personal Data'?" *Peter Fleischer: Privacy…?* (5 February 2007), online: <http://peterfleischer.blogspot.com/2007/02/are-ip-addresses-personal-data.html>.

FLEISCHER, P., "Global privacy standards should focus on preventing harm to consumers" (14 November 2007), online: The Official Google Blog <http://googlepublicpolicy.blogspot.com/2007/11/global-privacy-standards-should-focus.html>.

FLEISCHER, P., "The data deluge" *Peter Fleischer: Privacy…?* (21 April 2010), online: <http://peterfleischer.blogspot.com/2010/04/data-deluge.html?spref=tw>.

FRASER, D., "Privacy Commissioner consultations on new technologies: a few thoughts" (12 February 2010), online: Canadian Privacy Law Blog <http://blog.privacylawyer.ca/2010/02/privacy-commissioner-consultations-on.html>.

GARFIELD, B., "FTC Privacy Review Could Mean Trouble for Online Marketing: A Worst-Case Scenario: Online Advertising Would Be Legislated Into Oblivion" (19 April 2010), online: AdAgeBlogs <http://adage.com/columns/article?article_id=143343>.

GEIST, M., "Privacy Commissioner of Canada on lawful Access: Deep Concerns" (28 October, 2011), online: Michael Geist <http://www.michaelgeist.ca/content/view/6093/125/>.

GEIST, M., "Quebecor Opens Door to Canadian Three Strikes Policy" (26 February 2006), online: Michael Geist <http://www.michaelgeist.ca/content/view/3706/125/>.

GEIST, M., "'Three Strikes and You're Out' Policy Strikes Out" (21 April 2008), online: Michael Geist <http://www.michaelgeist.ca/content/view/2851/135/>.

GHOSEMAJUMDER, S., "Using data to help prevent fraud" (18 March 2008), online: Google Blog <http://googleblog.blogspot.com/2008/03/using-data-to-help-prevent-fraud.html>.

GOMEZ, J., Travis Pinnick & Ashkan Soltani, *KnowPrivacy* (1 June 2009), online: <http://www.knowprivacy.org/report/KnowPrivacy_Final_Report.pdf>.

GOOGLE, "Response to the Article 29 Working Party Opinion On Data Protection Issues Related to Search Engines" (8 September 2008).

GOOGLE, *Letter to the Article 29 Working Party in answer to their Letter dated May 16, 2007* (10 June 2007).

HOCHHAUSER, M., "Lost in the Fine Print: Readability of Financial Privacy Notices" (1 July, 2001), online: Privacy Rights Clearinghouse <http://www.privacyrights.org/ar/GLB-Reading.htm>.

IAB & AAAA, *4A's/IAB Education Guide to the Standard Terms and Conditions for Interactive Advertising for Media Buys One Year or Less, Version 3.0* (February 2010).

IMS HEALTH, "European Commission Review of the EU Data Protection Directive (Directive 95/46/EC): Submission by IMS Health" (July 2002), online: <http://ec.europa.eu/>.

INTERNET ADVERTSINING BUREAU, *PIPEDA + IAB Canada's Industry Self-Regulation Initiatives: A Win-Win For Canadian Consumers, Web Publishers + Web Innovators Going Forward…*, Submission for the 2010 Privacy Commissioner Consultation, 15 March 2010.

INTERNET GOVERNANCE FORUM, *Internet Fact Sheet: The basics of worldwide Internet usage* (November 2007), online: <http://www.intgovforum.org/mediaup/IGF%20BN%20Internet%20Fact%20Sheet.pdf>.

KATIE, "20 Crimes Caught on Google Street View", online: Disordel Conduct <http://www.criminaljusticeschools.com/blog/20-crimes-caught-on-google-street-view>.

MANJOO, M., "No More Privacy Paranoia, Want Web companies to stop using our personal data? Be ready to suffer the consequences" (7 April, 2011), online: Slate <http://www.slate.com/articles/technology/technology/2011/04/no_more_privacy_paranoia.html?wpisrc=newsletter_tis>.

MCDONALD, A., & FAITH CRANOR, L.,*The Cost of Reading Privacy Policies* (CyLab, Carnegie Mellon University, 2008).

MICROSOFT CORPORATION, *Microsoft Response to the Commission Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data* (31 December 2009), online: <http://ec.europa.eu/justice_home/news/consulting_public/0003/contributions/organisations/microsoft_corporation_en.pdf>.

MITTMA, J., (posting of), "German Court Rules That IP Addresses Are Not Personal Data" (17 October 2008), online: Proskauer Privacy Law Blog <http://privacylaw.proskauer.com/2008/10/articles/european-union/german-court-rules-that-ip-addresses-are-not-personal-data>.

NEWLAND, E., "Should all sensitive data be treated the same?" (26 February, 2010), online: CDT <http://www.cdt.org/blogs/erica-newland/should-all-sensitive-data-be-treated-same#sf40182>.

OECD, *Report on the Cross-Border Enforcement of Privacy Laws* (Paris: OCDE, 2006), online: <http://www.oecd.org/dataoecd/17/43/37558845.pdf>.

OECD, *The Seoul Declaration for the Future of the Internet Economy* (OECD, 2008), online: <http://www.oecd.org/dataoecd/49/28/40839436.pdf>.

OFFICE OF FAIR TRADING, "OFT launches market studies into advertising and pricing practices" (15 October 2009), online: OFT <http://www.oft.gov.uk/news/press/2009/126-09>.

OUT-LAW.COM, "IP addresses and the Data Protection Act" (March 2008), online: out-law.com <http://www.out-law.com/page-8060>.

PHYSICS ARXIV BLOG (THE), "Breaking the Netflix Prize dataset" (27 November, 2007), online: The Physics arXiv blog <http://arxivblog.com/?p=142>.

POUNDER, C., "Why the APEC Privacy Framework is unlikely to protect privacy" (15 October 2007), online: Out-law.com <http://www.out-law.com/page-8550>.

POUNDER, C., in answer to blog: Alma Whitten, "Are IP addresses personal?" (22 February 2008), online: Official Google Blog <http://googlepublicpolicy.blogspot.com/2008/02/are-ip-addresses-personal.html>.

PRIVACY COMMISSIONERS, *Resolution on Privacy Protection and Search Engines*, 28th International Data Protection and Privacy Commissioners' Conference, London, UK, 2 and 3 November 2006.

PROVOS, N., "Using log data to help keep you safe" (13 March 2008), online: Official Google Blog <http://googleblog.blogspot.com/2008/03/using-log-data-to-help-keep-you-safe.html>.

RICHTER, M., "Another Step in Open Site Governance" (26 March 2010), online: The Facebook Blog <http://blog.facebook.com/blog.php?post=376904492130>.

ROTENBERG, M., President, EPIC, before a committee of the USA House of Representatives, in a hearing on "Protecting Consumer's Data: Policy Issues Raised by ChoicePoint" (15 March 2005), online: <http://www.epic.org/privacy/choicepoint/testimony3.15.05.pdf>.

TAYLOR, H., "Most People Are 'Privacy Pragmatists' Who, While Concerned About Privacy, Will Sometimes Trade It Off For Other Benefits" (2003) 17 The Harris Poll, online: <http://www.harrisinteractive.com/vault/Harris-Interactive-Poll-Research-Most-People-Are-Privacy-Pragmatists-Who-While-Conc-2003-03.pdf>.

VARIAN, H., & CHOI H., "Predicting the Present with Google Trends" (2 April 2009), online: Google Research Blog <http://googleresearch.blogspot.com/2009/04/predicting-present-with-google-trends.html>.

VARIAN, H., & CHOI H., "Predicting Initial Claims for Unemployment Benefits" (22 July, 2009), online: Google Research Blog <http://googleresearch.blogspot.com/2009/07/posted-by-hal-varian-chief-economist.html>.

VARIAN, H., "Why data matters" (3 April 2008), online: Official Google Blog <http://googleblog.blogspot.com/2008/03/why-data-matters.html>.

WARDEN, P., "How to harvest Facebook profiles from emails without logging in" (6 February 2010), online: Pete Warden blog <http://petewarden.typepad.com/searchbrowser/2010/02/how-to-harvest-facebook-profiles-from-emails-without-logging-in.html>.

WARDEN, P., "How to split the US" (6 February 2010), online: Pete Warden blog <http://petewarden.typepad.com/searchbrowser/2010/02/how-to-split-up-the-us.html>.

WARDEN, P., "The Facebook Whisperer" (10 February 2010), online: Pete Warden blog <http://petewarden.typepad.com/searchbrowser/2010/02/the-facebook-whisperer.html#idc-container>.

ZIMMER, M., "Is it Ethical to Harvest Public Twitter Accounts without Consent?" (12 February 2010), online: Michael Zimmer.org <http://michaelzimmer.org/2010/02/12/is-it-ethical-to-harvest-public-twitter-accounts-without-consent/>.

ZIMMER, M., "Why Pete Warden Should Not Release Profile Data on 215 Million Facebook Users" (12 February 2010), online: Michael Zimmer.org <http://michaelzimmer.org/2010/02/12/why-pete-warden-should-not-release-profile-data-on-215-million-facebook-users/>.

ZUCKERBERG, M., "An Open Letter from Facebook Founder Mark Zuckerberg" *Facebook Blog* (1st December 2009), online: Facebook <http://blog.facebook.com/blog.php?post=190423927130>.