Université de Montréal

The Challenge of Industry Challenges:
The Uneasy Encounter Between Privacy Protection and Commercial Expression

Par Danielle Miller

Faculté de droit

Mémoire présenté en vue de l'obtention du grade de maitrise en droit option droit des technologies

Septembre 2016

Résumé

En s'inspirant de l'exemple des défis corporatifs, c'est-à-dire, des initiatives déployées par les sociétés pour rendre le marché de l'emploi plus accessible aux membres de groupes perçus comme marginalisés, ce mémoire cherche à analyser le conflit qui pourrait surgir au Québec entre le droit à la vie privé, protégé notamment par la *Loi sur la protection des renseignements personnels dans le secteur privé*[1] et la *Loi sur la protection des renseignements personnels et des documents électroniques*[2] et le besoin croissant de l'entreprise d'utiliser les données privées de leurs employés pour vendre leurs biens et services.

Dans un premier temps, ce mémoire effectue un survol des régimes de protection de la vie privée des pays qui ont le plus influencé le droit québécois et canadien soit l'Europe, les États-Unis et le Royaume Uni en soulignant leur influence sur le régime en vigueur au Québec. Dans un second temps, il soulève les entraves que posent la LPRPS et la LPRPDE à la participation de l'entreprise aux défis corporatifs. Dans un troisième temps, il explore des pistes possibles à la fois interprétatives, législatives et contentieuses afin de rendre ces lois plus accommodantes aux besoins de l'entreprise.

Mots clé : Militantisme du consommateur; *Charte canadienne des droits et libertés*; défis corporatifs; expression commerciale; *Loi sur la protection des renseignements personnels dans le secteur privé; Loi sur la protection des renseignements personnels et des documents électroniques; Québec; vie privée.*

[1] P-39.1. ("**LPRPS**").

[2] L.C. 2000, ch.5. ("**LPRPDE**").

Summary

This essay uses the example of Industry Challenges - a technique deployed by companies to promote the hiring and advancement of certain members of society - to explore a conflict that could arise in Quebec between the individual's right to privacy as protected by *An Act Respecting the Protection of Personal Information In the Private Sector*[1] and the *Personal Information Protection and Electronic Documents Act*[2], and that of an organisation to use personal information relating to its workforce to market itself. It briefly reviews privacy protection in jurisdictions with the greatest legal influence on Quebec and Canada: the European Union, the United States and the United Kingdom (Chapter 2). It demonstrates how a blend of these influences is reflected in the Quebec and Canadian approaches to privacy and how existing privacy legislation might prevent a company from effectively and efficiently responding to Industry Challenges (Chapter 3). Finally, the last two chapters respectively explore the interpretive and legislative amendments that could be made to PPIPS and PIPEDA to enable companies to respond to Industry Challenges (Chapter 4) as well as the possible legal action a company could take on the ground that Quebec's privacy legislation violates its right to express itself commercially under s. 2(b) of the *Canadian Charter of Rights and Freedoms*[3] (Chapter 5).

Key words: *An Act Respecting the Protection of Personal Information in the Private Sector*; *Canadian Charter of Rights and Freedoms*; Commercial Expression;

[1] Chapter P-39.1 ("**PPIPS**")..
[2] S.C. 2000, c. 5 ("**PIPEDA**").
[3] *Constitution Act*, 1982 R.S.C., 1985, App.II, no 44.

Consumer Activism; Industry Challenge(s); *Personal Information Protection and Electronic Documents Act*; Privacy; Quebec.

Table of Content

List of Abbreviations

Alberta PIPA	*Personal Information Protection Act*
Aubry	*Aubry* v. *Les Éditions Vice-Versa Inc.*
BC PIPA	*Personal Information Protection Act*
Campbell	*Campbell* v. *MGN Limited*
Canadian Charter	*Canadian Charter of Rights and Freedoms*
CCQ	*Civil Code of Quebec*
Convention	*Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*
Directive	Directive 95/46/EC *on the protection of individuals with regard to the processing of personal data and of the free movement of such data*
DLPs	Data protection laws
Dyment	*R*. v. *Dyment*
ECPA	*Electronic Communications Privacy Act*
EUCR	*European Union Charter of Fundamental Rights*
Fearon	*R*. v. *Fearon*
Ford	*Ford* v. *Quebec*
FIPs	Fair information practices
Hutterian Brethren	*Alberta* v. *Hutterian Brethren of Wilson Colony*
McGill L.J.	McGill Law Journal

MLR	Modern Law Review
Nikon	Cass. Soc., 2 octobre 2001, Société Nikon France SA, Bull.Civ. 2001
Oakes	*R*. v. *Oakes*
Pillsburry	*Smyth* v*. Pillsburry Co.*
PIPEDA	*Personal Information Protection and Electronic Documents Act*
PPIPS	*An Act Respecting the Protection of Personal Information in the Private Sector*
Quebec Charter	*Quebec Charter of Human Rights and Freedoms*
Queen's L.J.	Queen's Law Journal
R. du B. can.	Revue du Barreau canadien
Spencer	*R*. v. *Spencer*
Supreme Court	Supreme Court of Canada
Temp. Int'l &Comp. L.J.	Temple International and Comparative Law Journal
Tessling	*R*. v. *Tessling*
UFCW	*Alberta (Information and Privacy Commissioner)* v. *United Food and Commercial Workers, Local 401*
Yale L.J.	Yale Law Journal

Chapter 1. Introduction
Privacy and Industry Challenges

In 2013 the Supreme Court of Canada ("**Supreme Court**"), in *Alberta (Information and Privacy Commissioner)* v. *United Food and Commercial Workers, Local 401*[1], held Alberta's *Personal Information Protection Act*[2] to be unconstitutional for violating a union's right to express itself as per s. 2(b) of the *Canadian Charter of Rights and Freedoms*[3]. The case concerned Local 401 of the United Food and Commercial Worker's Union's ("**Local 401**") recording and photographing employees crossing the picket line. Following a complaint to the Alberta Information and Privacy Commissioner, the Commission-appointed adjudicator found Local 401's behaviour to have violated Alberta PIPA. Local 401 challenged the constitutionality of the legislation and, on judicial review, Alberta PIPA was found to have breached the union's right to express itself pursuant to s. 2(b) of the Canadian Charter. The Alberta Court of Appeal and the Supreme Court both upheld the decision. The Alberta legislature received twelve months to bring Alberta PIPA in line with the Canadian constitution. What is most interesting in this decision is the court's reiteration that rights are not absolute and the importance it attributes to a purposeful interpretation of them. Abella and Cromwell JJ. write: "[i]t is enough to note that, like privacy, freedom of expression is not an absolute value and both the nature of the privacy

[1] [2013] 3 S.C.R. 733 ("**U.F.C.W.**").
[2] S.A. 2003, Chapter P-6.5 ("**Alberta PIPA**").
[3] *Constitution Act*, 1982 R.S.C., 1985, App.II, no 44 ("**Canadian Charter**").

interests implicated and the nature of the expression must be considered in striking an appropriate balance".[4]

The potential implications of U.F.C.W. on the notion of privacy are far reaching - especially at present when privacy must compete with other compelling interests such as security and law enforcement, advertising and marketing, or even health-care, social justice and equality. For example, whose interests should prevail when a company wishes to participate in or implement programmes encouraging the advancement of members of certain under-represented groups in a particular industry sector and that requires access to its workplace demographics to do so? Should the company be permitted to harness whatever available technology to collect, use, and communicate employees' Personal Information (as defined in Chapter 3) without their consent? What if a staff member refuses consent?

These are neither negligible nor unrealistic queries for goods and services providers in an age of consumer and industry activism in which decisions to purchase are no longer based solely on price and quality but on a number of other factors ranging from environmental consciousness to gender and social parity. Indeed, a growing trend among American companies is to launch "challenges" ("**Industry Challenges**" as defined below) in their procurement documents aimed at increasing the number of employees belonging to certain socio-economic, gender, and cultural groups and to which suppliers must respond if they wish their goods or services to be retained. This trend has become so strong that many goods and services providers, in an

[4] *Supra* note 1 at 753.

anticipatory gesture, institute their own programs and initiatives to increase gender and cultural diversity which they then promote in their marketing materials. In fact, these various diversity initiatives often become a form of advertising or commercial expression. In Quebec, however, companies that wish to respond to Industry Challenges or advertise certain types of diversity initiatives, soon encounter obstacles in the form of privacy legislation. Be it by the *Personal Information Protection and Electronic Documents Act*[5] or *An Act Respecting the Protection Of Personal Information In the Private Sector*[6], organisations are prevented, except in very limited circumstances, from collecting, using or communicating any personal information about their employees without their employees' specific and express consent.

In the absence of either case law or doctrine on the matter, this essay seeks to explore the tension that exists at present between Quebec's private sector privacy legislation and a company's right to use workforce demographics to market itself – a practice that arguably constitutes a form of commercial expression. It questions whether the blanket protection of personal information provided by PPIPS and PIPEDA is still relevant and effective and what interpretive or legislative changes should be made to these acts to enable them to accommodate responses to Industry Challenges. Before turning to these questions, however, the next few pages review what is meant by privacy as well as by an Industry Challenge.

1.1 What is Privacy?

Although frequently invoked, privacy remains a notion that is difficult to define with

[5] S.C. 2000, c. 5 ("**PIPEDA**").
[6] Chapter P-39.1 ("**PPIPS**").

any degree of consensus. Is it a human right - that is to say an inviolable claim of the individual on the society to which he or she belongs – or a property right that can be bartered or sold? Is it a right at all or perhaps more of a legal concept? Does the answer to any of these questions ultimately affect the protection we afford privacy?

Ironically, while Europe, the United States, and Canada have signed many of the same treaties recognising the right to privacy, they do not interpret this right the same way.[7] Even within Canada, explicit privacy protection is not uniform. Indeed, at the federal level, privacy, *per se* is not guaranteed by the Canadian Charter. Instead it is read into the Canadian Charter's sections 7 and 8 that respectively protect the right to life, liberty and security of the person, and against unreasonable search and seizure. In the province of Quebec, however, section 5 of the *Quebec Charter of Human Rights and Freedoms*[8] as well as articles 35 to 40 of the *Civil Code of Quebec*[9],

---

[7] For example, Article 12 of the United Nations' *Universal Declaration of Human Rights* states that "[n]o one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation", http://www.un.org/en/documents/udhr/. Article 17 of *The International Covenant on Civil and Political Rights* states that "[n]o one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation", http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx Likewise, while European members states, the United States and Canada are all members of the OECD, the United States has not implemented a federal law reflecting the eight principles of the OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

[8] "Every person has a right to respect for his private life." CQLR, c. C-12, ("**Quebec Charter**").

[9] "Art. 35. Every person has a right to the respect of his reputation and privacy.

No one may invade the privacy of a person without the consent of the person unless authorized by law.

Art. 36. The following acts, in particular, may be considered as invasions of the privacy of a person:

(1) Entering or taking anything in his dwelling;
(2) Intentionally intercepting or using his private communications;
(3) Appropriating or using his image or voice while he is in private premises;
(4) Keeping his private life under observation by any means;
(5) Using his name, image, likeness or voice for a purpose other than the legitimate information of the public;
(6) Using his correspondence, manuscripts or other personal documents.

Art. 37. Every person who establishes a file on another person shall have a serious and legitimate reason for doing so. He may gather only information which is relevant to the stated objective of the file, and may not, without the consent of the person concerned or authorization by the law, communicate such information to

recognise a right to privacy and enumerate what constitutes its breach. Neither law, however, explicitly defines the right. In other Canadian provinces such as British Columbia,[10] Manitoba,[11] Saskatchewan,[12] and Newfoundland and Labrador[13] privacy is protected by several statutory torts. In Ontario, it was recognised in 2012 under the Common Law as "intrusion upon seclusion", in *Jones* v. *Tsige*,[14] and more recently as "public disclosure of private facts", in *Jane Doe 464533* v. *ND*[15]. So then what is meant by a right to privacy?

1.1.1 The Evolution of Privacy

An approach that is frequently adopted to analyse privacy is to review the evolution of its protection. Alan Westin, in his classic work, *Privacy and Freedom*, shows concerns for privacy to have existed in what might be labeled pre-modern societies and argues

---

third persons or use it for purposes that are inconsistent with the purposes for which the file was established. In addition, he may not, when establishing or using the file, otherwise invade the privacy or injure the reputation of the person concerned.

Art. 38. Except as otherwise provided by law, any person may, free of charge, 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; he may also cause a copy of it to be made at reasonable cost. The information contained in the file shall be made accessible in an intelligible transcript.

Art. 39. A person keeping a file on a person may not deny him access to the information contained therein unless he has a serious and legitimate reason for doing so or unless the information may seriously injure a third person.

Art. 40. Every person may cause information which is contained in a file concerning him and which is inaccurate, incomplete or equivocal to be rectified; he may also cause obsolete information or information not justified by the purpose of the file to be deleted, or deposit his written comments in the file.

Notice of the rectification is 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. The same rule applies to an application for rectification, if it is contested." S.Q. 1991, c.64, ("**CCQ**").

[10] *The Privacy Act*, RSBC 1996, c 373.

[11] *The Privacy Act*, CCSM c P125.

[12] *The Privacy Act*, RSS 1978, Chapter P-24.

[13] *The Privacy Act*, RSNL 1990, Chapter P-22.

[14] 2012, ONCA, 32.

[15] [2016] O.J. No. 382, 2016 ONSC 541.

that “the notion put forward by legal commentators from Brandeis down to the present – that privacy was somehow a ‘modern’ legal right which began to take form only in the late nineteenth century – is simply bad history and bad law”.[16] Nevertheless, as Eloise Gratton points out, it is generally agreed that privacy protection has evolved through three phases. During the first phase, privacy was associated with Justice Cooley’s definition, as the right to be left alone, and with Samuel Warren and Louis Brandeis’ article, “The Right to Privacy”, that criticised the press’ use of technology, such as instantaneous photography, to invade domestic life.[17] The second phase, which was largely in reaction to the atrocities of the Second World War, interpreted privacy to mean “respect for one’s private and family life, his home and his correspondences”.[18] Finally, the third phase, that began in the 1960s, conceptualized privacy as the right for individuals to control their personal information.[19] The main threat to privacy was deemed to come from automated data banks, the amount of information they could store, and the distances over which they could transmit data. As a result, the fair information practices (“**FIP**”s) around which much of our present privacy legislation, such as PPIPS and PIPEDA, are structured reflect an attempt to enable individuals to retain control over the information that concerns them.[20] These FIPs include the right to know that information is being collected, the right to know the

[16] NY, IG Publishing, 1967 at 377.

[17] Gratton, Eloise, *Understanding Personal Information: Managing Privacy Risks*, Markham, ON, Lexis Nexis Canada Inc., 2013 at 2.

[18] *Ibid.,* at 3.

[19] *Ibid*., at 6.

[20] *Ibid*., at 15.

use to which it will be put as well as how to correct any inaccuracies.[21]

In addition to the above three phases – or waves - Gratton proceeds to question whether with the advent of the Web 2.0, social media, and "big data", not to mention drones and other technological devises that have the ability to render privacy obsolete, it might be accurate to speak of a fourth wave of privacy protection in which society now finds itself.[22] She notes "[t]he recent changes triggered by the Internet and related technologies are important enough to suggest that we have entered a fourth wave, and we should therefore go back to the drawing board".[23] But before returning to the drawing board, a few words on the importance of privacy are warranted.

1.1.2 The Importance of Privacy

Over the past fifty years many authors have struggled to define privacy and explain its importance. For example, Westin states that "[p]rivacy 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".[24] He describes its importance to personal and organisational development. According to Westin, whereas privacy allows for the autonomy, emotional release, self-evaluation and limited and protected communication necessary to individuals in democratic societies,[25] it provides organisations in these same societies with the organizational autonomy, release from public roles, evaluative periods for decision making and protected communications

[21] *Ibid*., at 10.
[22] *Ibid*., at 56.
[23] *Ibid*.

they need to thrive.[26]

More recently, an author whose definition has been retained by the Supreme Court[27] is Chris Hunt who defines the right to privacy as:

> "X's claim to be free from unwanted sensorial access in relation to information and activities which are intimate; or, if not intimate, information and activities which are personal in the sense that most people in our society would not want them to be widely known or widely observed; or, if neither intimate nor personal, information and activities about which X feels acutely sensitive and in which he claims a privacy interest."[28]

Hunt provides two philosophical approaches to justify the importance of privacy. He explains that from a deontological perspective, privacy is valuable because it provides "dignity and autonomy"[29] and it preserves the individual's right to shape their destiny[30]. Violating this right to privacy places the violator's choice above that of the victim, demonstrates disrespect for the victim and, in essence, transforms the victim from subject to object as he or she no longer controls the choices that concern him or her.[31] From a consequentialist perspective privacy fosters: 1. the individual's development by providing a place where they are free from the social pressure to conform -;[32] 2. his or her ability to form relationships – since keeping some aspects of

---

[24] *Supra* note 6 at 5.

[25] *Ibid*. at 35.

[26] *Ibid*. at 46-56.

[27] See for example U.F.C.W. or *R*. v. Spencer, 2014 SCC 43. ("**Spencer**").

[28] Hunt, Chris D.L., "Conceptualizing Privacy and Elucidating its Importance: Foundational Considerations for the Development of Canada's Fledgling Privacy Tort", (2011) 37 Queen's L.J. 167, p.217-218.

[29] *Ibid*. at 203.

[30] *Ibid*. at 207.

[31] *Ibid*. at 203-209.

[32] *Ibid.* at 210

oneself private are the heart of intimacy -;[33] and 3. his or her participation in a liberal society since principles of dignity and autonomy are at the very core of liberal society[34]. Violating this privacy, therefore, destroys the person's development as an individual, his or her ability to form relationships and ultimately the development of his or her society.[35] The strength of Hunt's definition is its implicit recognition that individuals do not all have the same sensitivities with respect to what they consider to be their private lives. Its weakness lies in its failure to consider that the importance societies and individuals attribute to privacy may not be static but wax and wane in response to other competing rights and interests. Either way, it is difficult to build a legal definition of privacy from Hunt's study.

1.1.3 Privacy as a Concept

Perhaps instead of speaking of privacy as a right in absolute terms, it might be more accurate to speak as Jean-Louis Halpérin does, of privacy as a concept, that is, an artifact produced by the human mind for the specific world of law.[36] Characterising privacy as a shifting border, a rampart built by law to protect against encroachments from other private persons, such as the press or other organisations possessing private information, Halpérin states : "[l]a privacy n'est pas une créance sur des individus ou sur la société, elle ne consiste pas non plus dans un droit réel sur une chose, c'est la liberté de conserver la tranquillité de sa vie privée sans interférences

[33] *Ibid.* at 213.

[34] *Ibid.* at 216.

[35] *Ibid*. at 209-217.

[36] Halpérin, Jean-Louis, "L'essor de la 'privacy' et l'usage des concepts juridiques", *Droit et Société* 61/2005, 765 at 775.

extérieures".[37] The challenge is to establish where, in a given instance, the border should be drawn. This is precisely the difficulty that arises when rights to privacy enter into conflict with the subject of this essay, Industry Challenges.

1.2 What is an Industry Challenge

1.2.1 Definition

This essay uses the term "Industry Challenge", that is by no means a term of art, to refer to a technique deployed by companies that have undertaken to promote the hiring and advancement of certain members of society, notably women, visible minorities, and homosexuals/bisexual/transgender ("**Target Group**"), traditionally perceived as marginalised in a particular sector or industry. These Industry Challenges, among other things, consist in requiring the company's goods and service providers to commit to its causes. The company thus "challenges" its suppliers to espouse its causes failing which they risk losing the company's business.

A company typically launches its challenges in its tendering documents in which it asks its suppliers to provide information on their diversity programs as well as on the number of employees belonging to a Target Group and/or belonging to a Target Group and holding management or executive positions within the company. The company may also insist that its service providers, such as lawyers or accountants, build client teams led by or including a certain percentage of Target Group members. It will also reserve the right to privilege or conduct business only with suppliers that either employ a satisfactory number of people belonging to the Target Group or that

[37] *Ibid*., at 780, 779.

have implemented programmes for their advancement or both. Depending upon the level of detail required, a Quebec goods or service provider may be asked to give specific numbers concerning its employees' gender and/or their cultural background. It may also be asked to provide the professional resumes of members who qualify as Target Group members of a proposed client team – a disclosure that amounts to "outing" anyone who wished to remain anonymous. A goods or services provider that cannot communicate this information in the expected level of detail risks losing the company's business.

1.2.2 Example

A perfect illustration of a company capable of launching an Industry Challenge is Cummins that uses its commitment to diversity as a central feature of its marketing strategy. Its internet site not only lists the number of women holding senior positions but promotes a "diversity procurement initiative" which it states "reached its long-standing goal of $1 billion in spending with diverse suppliers across eight categories in 2014, and laid the foundation for future growth".[38] These eight categories include minority business enterprises; women business enterprises; service disabled veteran owned small businesses; lesbian, gay, bisexual, transgender owned businesses; historically under-utilized business zone businesses; small disadvantaged businesses and philanthropic enterprises.[39] The Cummins site exemplifies two trends that mark a new market reality and that are discussed briefly below: 1. the influence of consumer activism on the market – Cummins and companies like it, while perhaps motivated by

[38] http://sustainability.cummins.com/social/diversity/diversity-procurement

[39] *Ibid*. At the time of drafting Cummins only listed 7 categories on its web-site.

altruism are also responding to what they believe to be an important market trend; and 2. workforce demographics and the ability to package these, be it in response to Industry Challenges or otherwise, have become a form of advertising or commercial expression.

1.2.3 The Context to Industry Challenges: Consumer Activism

To fully understand the importance of Industry Challenges and their impact on a company's ability to sell its products, a few words on consumer activism are in order. Indeed, it is in response to an increasingly activist market that Industry Challenges and other industry-sponsored initiatives for social advancement have developed. Without entering into an extensive study of consumer activism, the movement can be loosely defined as the belief held by certain consumers that through their purchases they are expressing an ethical or moral choice that they believe will have an impact beyond their immediate purchase.[40] This movement appears to be linked to a belief that governments are either unable or unwilling to affect the type of change required to remedy certain social inequalities, both domestically and abroad, and therefore, it falls to the individual and to the private sector to make the changes governments cannot. As Ryan Calo observes, consumers are increasingly moving away from price and quality as the main factors motivating decisions to purchase, in favour of socio-political concerns such as the vendor's social engagement.[41] To attract consumers

[40] An example of consumer activism is the Responsible Investing movement that refers to the "integration of environmental, social, and corporate governance criteria (ESG) into the selection and management of investments ("**Responsible Investing**"). To date, there are 1 trillion dollars of assets under this form of management in Canada which represents a 68% increase in the last two years. The investment vehicles typically include stocks, bonds, mutual funds, retail venture capital and exchange and traded funds (RIA Canada https://riacanada.ca/trendsreport).

[41] "Privacy and Markets: A Love Story", *Legal Studies Research Paper* No. 2015-26, 1 at 7.

who hold these beliefs, companies develop marketing strategies equating their product to the cause in question. Mr. Bedbury, head of marketing at Starbucks and former head of marketing at Nike, explains the process as follows:

> [w]ith Starbucks, we see how coffee has woven itself into the fabric of people's lives, and that's our opportunity for emotional leverage. ….A great brand raises the bar – it adds a greater sense of purpose to the experience, whether it's the challenge to do your best in sports and fitness or the affirmation that the cup of coffee you're drinking really matters. [42]

The example of Responsible Investing and the changes it brought to Canadian securities regulations serves as a good illustration of how these market pressures function. Indeed, investment managers of funds that qualify as Responsible Investing must adhere to the "United Nations-supported Principles for Responsible Investing"[43] that require them to abide by principles that necessitate a certain degree of disclosure on the part of the companies seeking to be included in the funds – disclosure of information that would typically be deemed personal under PPIPS and PIPEDA. In October 2014, however, securities regulators in all Canadian provinces and territories except British Columbia, Alberta, and the Yukon amended corporate governance disclosure to allow companies to disclose policies regarding the representation of

---

[42] Klein, Naomi, *No Logo*, London, Flamingo, 2000, at 20-21.

[43] 1. To incorporate ESG issues into investment analysis and decision-making processes;
2. To be active owners and incorporate ESG issues into ownership policies and practices;
3. To seek appropriate disclosure on ESG issues by the entities in which [they] invest;
4. To promote acceptance and implementation of the principles within the investment industry;
5. To work together to enhance effectiveness in implementing the principles; and
6. To each report on activities and progress towards implementing the principles http://www.unpri.org/about/the-six-principles.

women on boards and in executive positions.[44] Companies must now disclose the number of women who hold board and executive-officer positions as well as the processes in place to increase gender diversity.[45] A company's ability to disclose specific numbers on workforce demographics is thus an essential form of advertising in a market of socially conscious investors and consumers.

1.2.4 Industry Challenges and Advertising

In light of consumer activism described above, a company's ability to respond to Industry Challenges and play to the socio-political demands of its potential purchasers is a vital aspect of its marketing strategy. In that they enable a purchaser – commercial or private - to make informed choices about their goods and services providers, these responses and any subsequent use that is made of the information to promote a company, should be considered a form of commercial expression[46] and protected as such under s.2(b) of the Canadian Charter. Indeed, a company's

[44] Règlement 58-101 sur l'information concernant les pratiques en matière de gouvernance, http://www.lautorite.qc.ca/files/pdf/reglementation/valeurs-mobilieres/58-101/2015-11-17/2015nov17-58-101-vofficielle-fr.pdf

[45] *Ibid*.

[46] In the same way that the Canadian Charter does not explicitly protect a right to privacy *per se* but allows it to be read into sections 7 and 8, it does not explicitly protect the right to "commercial expression". Rather commercial expression is a form of expression that qualifies for protection under s. 2(b) of the Canadian Charter. In fact, since 1988 and the case of *Ford* v. *Quebec (*[1988] 2. S.C.R. 712 ("**Ford**")*),* commercial expression generally, and advertising in particular, have been considered a form of expression worthy of Canadian Charter protection. Hogg justifies this by citing the facts that commercial expression "does literally fall within the meaning of the word 'expression'" and that it contributes "to the 'marketplace of ideas' that is fostered by the constitutional guarantee" and that "it is very difficult to distinguish commercial speech from other kinds of speech, in that a variety of political, economic and social ideas are inevitably inherent in commercial speech",(Hogg, Peter, *Constitutional Law of Canada*, 5th ed., vol 2 Toronto: Carswell, 2014 at 43-22). In Ford the Supreme Court clearly finds that:

> "there is no sound basis on which commercial expression can be excluded from the protection of s. 2(b) of the Charter. It is worth noting that the courts below applied a similar generous and broad interpretation to include commercial expression within the protection of freedom of expression contained in s. 3 of the Quebec Charter. Over and above its intrinsic value as expression, commercial expression which, as has been pointed out, protects listeners as well as speakers plays a significant role in enabling individuals to make informed economic choices, an important aspect of individual self-fulfillment and personal autonomy." (at 767)

Arguably, the value of this for form of expression is all the more important almost thirty years after the Ford decision was rendered with the rise of consumer, and in response, industry activism.

collection, use, and communication of its workforce demographics represents an essential feature of its advertising campaign as it informs consumers about important characteristics of a product.

As the law presently stands, however, goods and services providers in Quebec are often prevented from effectively responding to an Industry Challenge. They must seek "work arounds" in which diversity numbers are presented as a collated percentage rather than detailed figures regarding the number of employees belonging to a particular category. This may or may not satisfy the client that launched the Industry Challenge. It also makes Quebec companies' commitment to diversity appear weak when compared to that of their American competitors. It certainly places Quebec companies at a disadvantage in the eyes of clients that truly value diversity and use it as a ground on which to base their decision to purchase. Many calls for tenders frequently contain statements allowing companies to privilege suppliers with strong and explicit diversity policies, initiatives and results.

Clearly then, PPIPS, PIPEDA, and the FIPs on which they are based, may not be adapted to changes in market trends and the value some societies now place on diversity and inclusion. A rigid application of these laws that fails to provide industry with the appropriate leeway to adapt to new market realities may, in fact, leave both laws open to judicial review as was the case in U.F.C.W..

****

Returning to Halpérin's image of privacy as a shifting border, this essay seeks to establish how the border might be drawn between a company's right to use workforce

demographics to market itself and the right of the individual who works for the company to keep the same information private. It focuses on three themes in particular: the way privacy is perceived and protected in Canada with an emphasis on Quebec; the impediments PPIPS and PIPEDA pose to Industry Challenges; and the possible amendments, as well as judicial challenges that could be made to existing privacy legislation to enable companies to participate in Industry Challenges.

In addition to this Introduction and to a Conclusion, the pages that follow are divided into four chapters. Chapter 2 reviews the ways privacy has been protected in jurisdictions with the greatest influence on Canada and Quebec: the European Union, the United States and the United Kingdom. Whereas the United States and Europe explicitly recognise privacy as a right, they differ on the nature of this right. Europe perceives it as a human right. The United States views it more as a property right. In contrast, the United Kingdom and other Common Law jurisdictions protect privacy but have had difficulty explicitly recognising it as a right. These mixed influences are reflected in the Canadian approach to privacy (Chapter 3) where certain laws explicitly protect the use, collection, and communication of Personal Information thereby preventing a company from effectively and efficiently responding to an Industry Challenged, but where the courts, like their counterparts in the United Kingdom, are more likely to address privacy on a case by case basis, establishing what is reasonable under the circumstances. The last two chapters explore the interpretive and legislative amendments that could be made to PPIPS and PEPIDA to enable a company to respond to Industry Challenges. Chapter 4 argues that a purposive interpretation should be applied to the definition of Personal Information so

as to exclude: i) data made publicly available by the individual, ii) employee data necessary for the operation of an enterprise, and iii) data required by programs intended to remedy social inequalities. Chapter 5 explores the possible legal action a company could take on the ground that this legislation violates its right to express itself commercially under s. 2(b) of the Canadian Charter. While PPIPS' and PIPEDA's objectives may still seem worthy and the legislation rationally connected to these, the impairment PIPEDA inflicts on a company is more than minimal. Additionally, in that both laws limit a form of commercial expression, and therefore risk depriving consumers of information necessary to make informed decisions, threaten the competitiveness of Quebec businesses, and discourage private sector participation in affirmative action type programs, their overall impediment, in the case of an Industry Challenge, outweighs their benefit.

Chapter 2. Conflicting Origins:

The Legal Influences on Canadian Privacy Protection

As discussed in the Introduction, a marked absence of consensus reigns over the definition of privacy, not to mention whether it constitutes a right and if so, what type of right. The question becomes even more complicated in a country like Canada where two major private law regimes, the Common Law and the Civil Law, often merge to create hybrid, yet distinctly Canadian, solutions to legal problems. James Whitman, in "The Two Western Cultures of Privacy", describes the challenge in defining privacy in a given society as one that first requires identifying "the fundamental values that are at stake in the "privacy" question as it is understood in a given society".[1] The task, he explains, "is not to realize the true universal values of "privacy" in every society. The law puts more limits on us than that: The law will not work *as law* unless it seems to people to embody the basic commitments of their society".[2] In other words, the definition and protection of privacy in a given society is a reflection of that society's norms and values. Whitman goes on to observe: "[h]uman communities can be founded on the widest variety of norms. As for law: it is not about the worldly realizations of wisdom or sophistication as such. Law is about what works, what seems appealing and appropriate in a given society".[3]

Since the purpose of this essay is to explore the challenges the use of workforce demographics poses to Quebec private sector privacy legislation, this chapter begins

---

[1] (2003-2004) 113 Yale L.J. 1151 at 1220.
[2] *Ibid.*
[3] *Ibid*. at 1168.

by trying to understand the norms and values that have influenced and shaped Canada's approach to privacy. To do so it presents an overview and comparison of the privacy norms and legislation present in continental Europe – exemplified by France and Germany[4] -, the United States and the United Kingdom notably as they concern cases involving the workplace as well as competing rights such as freedom of expression. This comparison rapidly reveals three starkly different approaches. While Europe and the United States diverge on the type of right – human or property – privacy represents, they protect it explicitly. The United Kingdom, on the other hand, until recently, has adopted a custom-based interpretation of the right to privacy.

2.1 Privacy Protection in Continental Europe

2.1.1 Philosophical Origins

Continental Europe tends to perceive privacy as a human right. Its explicit and extensive protection by France and Germany, reflects the primordial importance Europeans attribute to dignity and honor and the resulting desire to protect these from "loose talk" and the "grubbiness of the world of buying and selling" or, in American terms, from freedom of the press and the market economy.[5] Although France and Germany both tend to protect the right to privacy more comprehensively than the United Kingdom or the United States, their reasons for doing so are quite different.

[4] As a review of each European member state's norms is too extensive and falls outside the scope of this paper, the following paragraphs discuss only those of France and Germany, archetypal civil law regimes the influence of which has generally marked the Continental approach and that, while resulting in similar protection, emerged from quite different histories.

[5] *Supra* note 1 at 1171.

2.1.1.1 France

According to Whitman, in France, the modern concern with privacy dates back to the French Revolution and the ideal of extending to all citizens the respect for private life that up until that point had only been enjoyed by the elite. The 1791 Constitution, therefore, included protection against calumnies and insults relative to private life.[6] The practical application of this provision was shaped by a number of cases, not the least of which was the trial involving Dumas, Père, who had been photographed with a mistress by a photographer who subsequently registered the copyright to the photographs with the intention of selling them to the press.[7] Dumas sued the photographer and the court held that while Dumas did not have a property right in the photographs, he had a countervailing right to privacy which enabled him, even after having given tacit consent to the publication, to retract this consent.[8] Whitman explains that "French privacy law was thus the product of the culture of the Paris art world, with its nude models, defiant immoralism, and large artistic egos. The cases that grew out of that world generally concluded that there was a right to one's image that was distinct from, and in tension with, rights of property".[9]

A more contemporary illustration of privacy protection in France, this time in an employment context, is the Nikon case.[10] In Nikon, the Cour de cassation overturned a court of appeal ruling allowing evidence, obtained by monitoring an employee without his knowledge, to be admitted to prove that the employee was transmitting

[6] *Ibid*.
[7] *Ibid*. at 1176.
[8] *Ibid*.
[9] *Ibid*. at 1178.
[10] Cass. Soc., 2 octobre 2001, Société Nikon France SA, Bull.Civ. 2001, ("**Nikon**").

confidential information to a competitor despite having signed a confidentiality agreement.[11] The Cour de cassation held instead that the employer had violated the employee's right to privacy.[12] It reasoned that:

> "[a]ttendu que le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée; que celle-ci implique en particulier le secret des correspondances; que l'employeur ne peut dès lors sans violation de cette liberté fondamentale prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur. "[13]

The Nikon decision, especially as it concerns an employment relationship, may seem extreme to a North American. It is, however, frequently touted as representative of the French approach to privacy.[14]

2.1.1.2 Germany

In Germany, while privacy rights evolved in reaction to some of the same concerns as in France, such as freedom of the press and the excesses of market economy, they were rooted in different preoccupations and history. According to Whitman, these rights developed from the German concept of personality. Unlike in the United States, where the opposite of freedom was tyranny, notably from the state, in Germany, the opposite of freedom was determinism.[15] Consequently, freedom represented the right to self-realisation and to develop one's personality - not the right to engage in

---

[11] *Ibid*.

[12] *Ibid*.

[13] *Ibid*.

[14] See for example Karen Eltis, "La surveillance du courrier électronique en milieu de travail : le Québec succombera-t-il à l'influence de l'approche américaine? ", (2006) 51 McGill L.J. 475 at 497.

[15] *Supra* note 1 at 1181.

unregulated market transactions.[16] The paradigm of the free actor in German society was the artist, not the consumer.[17] Despite much writing on the subject, however, Germany waited until 1949 to recognise the right of personality in its Civil Code - as the 1900 version did not include this right,[18] and the Nazi code, that endorsed a universal German right to the protection of personality, never came into effect.[19] The horrors of World War II further intensified the value that Germany placed on privacy and dignity. It is against this backdrop that comprehensive privacy legislation emerged in Europe.

2.1.2 Legislative Protection

European legislation tends to protect privacy as a human right that, while not absolute, receives prior protection to many other rights. Article 7 of the *European Union Charter of Fundamental Rights* states that "[e]veryone has the right to respect for his or her private and family life" and article 8 provides for "the protection of personal data".[20] The Council of Europe's *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*[21] as well as Directive 95/46/EC *on the protection of individuals with regard to the processing of personal data and of the free movement of such data* provide supranational privacy protection [22].[23]

---

[16] *Ibid*.

[17] *Ibid*.

[18] *Ibid.* at 1186.

[19] *Ibid.* at 1187-8.

[20] http://ec.europa.eu/justice/fundamental-rights/charter/index_en.htm, ("**EUCR**").

[21] http://www.conventions.coe.int/Treaty/en/Treaties/Html/108.htm, ("**Convention**").

[22] http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf, ("**Directive**").

[23] Directive 97/66/EC *concerning the processing of personal data and the protection of privacy in the telecommunications sector* (http://www.aip-bg.org/lichnidanni/pdf/directive_97_66.pdf) also protects data in the specific field of telecommunication. As this field is not the topic of this paper, this directive will not be discussed.

Although Daniel Newman's observation that "[m]uch like the EU Charter itself, a European Union member state's laws can protect privacy but still be unclear as to whether privacy is a fundamental human right",[24] both the Convention and the Directive repeatedly refer to privacy as a "fundamental right and freedom".[25] While the Directive also acknowledges the economic value of data and its importance to the internal European market,[26] it in no way attempts to balance, as does some Canadian legislation discussed in the next chapter,[27] competing commercial and individual rights.

Since the Directive, that ensures uniform privacy protection throughout European member states, contains the provisions that are of greatest interest to this study, a closer examination of this legislation is in order. As with the legislation applicable to the private sector in Quebec, it reflects a consent-based approach to the protection of personal information. It is founded on the OECD Principles,[28] the implementation of which was mandatory as of October 28 1998. The Directive thus applies to the processing[29] of personal data[30] by member states. Accordingly, data must be:

---

[24] Newman, Daniel E., "European Union and United States Personal Information Privacy, and Human Rights Philosophy – Is There a Match?", (2008) 22 Temp. Int'l & Comp. L.J. 307, at 329.

[25] *Ibid.* at 329.

[26] *Supra* note 22 Preamble (8).

[27] See for example the purpose of the federal *Personal Information Protection and Electronic Documents Act*, SC 2000, c. 5 ("**PIPEDA**") that seeks to balance the privacy right of an individual with the need of an organization to collect, use and disclose personal information. A similar purpose marks the provincial privacy legislation in British Columbia and Alberta. See for example s. 2 of the British Columbia *Personal Information Protection Act*, SBC 2003 Chapter 23 or s. 3 of the Alberta *Personal Information Protection Act*, S.A. Chapter P-6-5.

[28] These are: collection limitation, data quality, purpose specification, use limitation, security, openness, individual participation, and data accountability.

[29] *Supra* note 22, art. 2(b) defines processing 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."

[30] *Ibid*. art. 2(a) defines personal data as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference

processed fairly and lawfully; collected and used for specified, explicit and legitimate purposes; be adequate, relevant and not excessive, in relation to the purpose for which they are collected; as well as accurate and maintained up to date.[31] Subjects must be allowed to access their data and to rectify, erase, and block incorrect data.[32] Member states are required to create supervisory bodies that are to be notified when controllers are processing data,[33] and are prevented from transferring data to third countries which do not offer adequate protection.[34]

Although the Directive makes the data-subject's unambiguous consent a precondition to any processing, certain exceptions exists. For example, consent is not required for the performance of a contract to which the data-subject is party, or the protection of the data-subject's vital interest.[35] Likewise, art. 3 exempts the processing by natural persons of data in the course of "purely personal or household activities" as well as processing in the course of activity that falls outside the scope of Community law such as public security, defence and state security.[36] Interestingly, the Directive also allows member states to derogate from the scope of the law if the processing is carried out for journalistic, literary or artistic purposes *but only* if the derogation is necessary to reconcile the right to privacy with the rules of freedom of expression.[37]

---

to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".

[31] *Ibid*. at art. 6.

[32] *Ibid*. at art. 12.

[33] *Ibid*. at art. 28.

[34] *Ibid*. at art. 25.

[35] *Ibid*. at art.7.

[36] *Ibid*. at art. 3(2).

[37] *Ibid.* at art. 9.

Two provisions of particular interest for this essay are those pertaining to marketing and to the collection of special categories of data. With respect to the former, art. 14 (b) grants the data subject the right to object to having personal data processed for the purposes of direct marketing, or to be informed before personal data is disclosed for the first time to a third party or used on their behalf for the purposes of direct marketing, and to be given the right to object free of charge to such disclosure and uses. [38] This "opt-out" approach would appear more permissive than the legislation in effect in Quebec that requires the subject's consent to the processing and disclosure of personal information.

With respect to special categories of data, art. 8 requires member states to prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and processing of data concerning health or sex life unless the subject has explicitly consented.[39] Certain exceptions to this article exist including: a) where the subject has given their explicit consent; b) where processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law; (c) where the processing is necessary to protect the vital interest of the data-subject or another person and the data-subject is unable to provide consent; (d) where the processing is carried out in the course of a foundation's, association's or other non-for-profit-seeking body's legitimate activities with a political, philosophical religious or trade union aim or; e) where the processing relates to data which are manifestly

[38] *Ibid*. at art. 14 (b)
[39] *Ibid*. at art. 8.

made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.[40] The seemingly comprehensive privacy protection of the Directive stands in sharp contrast to that of other geographies, notably the United States.

2.2 Privacy Protection in the United States

Unlike many Common Law countries, the Unites States has a comparatively long tradition of recognizing privacy as a right in and of itself and of protecting it against violation from both public and private bodies. Its approach, however, is quite different from that of continental Europe. For instance, the United States provides strong protection against interference by public bodies but only sectorial legislation regulating the behaviour of private parties in sectors where information is deemed particularly sensitive. Companies operating outside these specific sectors are at liberty to develop their own privacy regulations and the Federal Trade Commission, the mandate of which is to protect consumers from unfair and deceptive business practices, is left to enforce these.[41]

2.2.1 Philosophical Origins

The American approach to privacy protection, much like the European approach, reflects the norms and values that shape its society. Instead of viewing privacy as an intrinsic part of an individual's honour and personality, the United States tends to treat it as a commodity governed by the rules of contract law. This perception is set out in the HEW Report which became the blueprint for the *Federal Privacy Act* of 1974 and

[40] *Ibid*. at arts. 8 (1) and (2).
[41] *Supra* note 24 at 336.

that treats information as a good that can be traded against other goods and services.[42] The Report, however, suggests that consent should be obtained from an individual whose information has been collected for a particular purpose before that information can be used for another purpose.[43]

As information is generally treated as a form of property in the United States, its greatest threat is perceived to come from government. This fear is reflected in the robust legislation protecting individuals from invasion of privacy by government but minimal legislation when it comes to regulating how private parties deal with each other's information.

A second feature distinguishing American from European privacy protection is the secondary place it takes to freedom of expression – notably the press – in the hierarchy of rights. Whereas, as described by Whitman, French and German-case law betrays suspicion of the press, and art. 9 of the Directive does not make an absolute exception for journalistic purposes but only allows these if it is necessary to reconcile privacy rights with members states' rules governing freedom of expression, in the United States freedom of expression and of the press are seemingly sacrosanct. Although certain American writers, such as Samuel Warren and Louis Brandeis, arguing for a French approach to privacy protection, criticised the press for "overstepping in every direction the obvious bounds of propriety and of decency",[44] their vision, by in large, has not prevailed in the United States. In fact, Whitman

[42] *Ibid*., at 337.

[43] *Ibid*.

[44] Warren, Samuel D. and Brandeis, Louis D., "The Right to Privacy", Harvard Law Review, V.IV, No.5, December 1890.

observes: “[f]reedom of expression has been the most deadly enemy of continental style privacy in America”.[45] The American understanding of privacy, therefore, renders its protection less comprehensive than in Europe. This nuance is particularly striking, as the next paragraphs discuss, when applied to the context of the workplace.

2.2.2 Legal Protection

2.2.2.1 Statutory

According to Charles Morgan, two federal laws protect an individual’s privacy right in the United States. While the United States Constitution’s Fourth Amendment protects against unreasonable search and seizure by government officials or by federal or state employers, the *Electronic Communications Privacy Act* (“**ECPA**”) Title 1 § 2511 prevents parties from “intentionally intercept[ing], endeavor[ing] to intercept, or procur[ing] any other person to intercept or to endeavor to intercept any … electronic communication” and from disclosing such information.[46] Morgan explains, however, that the protection this statute offers in the workplace is limited by its exceptions notably by § 2511(2)(d) that provides that such interception is not illegal if consent has been obtained, and by § 2511 (2)(a)(i) that creates a “business use exception” for any officer, employee or agent of wire or electronic wire or electronic communication services who “intercept[s], disclose[s], or use[s] that communication in the normal course of his employment while engaged in any activity which is necessarily incident to the rendition of his service or to the protection of the rights or property of the

[45] *Supra* note 1 at 1209.

[46] Morgan, Charles, “Employer Monitoring of Employee Electronic Mail and Internet Use”, (1999) 44 McGill L.J. 849 at 866-7.

provider of that service".[47] The exception applies when the employer is deemed to be the provider of the services, which is generally the case, and the activity occurs in the normal course of employment.[48] In addition, once the communication has been transmitted it falls outside the scope of Title 1.[49] Title 2, that protects against access to stored communication, contains an exception for "the person or entity providing the wire or electronic communications service" thus enabling the employer to access employee email as the employer is usually deemed to be the provider of the service.[50],[51]

In addition to the United States Constitution and to the ECPA, legislation such as the *Health Insurance Portability and Accountability Act*, the *Graham-Leach-Bliley Act*, the *Children's Online Privacy Protection Act*, the *Fair Credit Reporting Act* and the *Federal Videotape Privacy Protection Act* recognise and protect sensitive information respectively of medical records, financial records, child internet use, credit records and videotape.[52]

2.2.2.2 Tort

In addition to legislative protection, and contrary to many Common Law jurisdictions, American courts, for a long time, have recognised the tort of invasion of privacy. *The*

---

[47] *Ibid*. at 867-8.

[48] *Ibid*.

[49] *Ibid*.

[50] *Ibid*.

[51] It is interesting to note, as does Morgan, that while in Canada, s. 184(1) of the *Criminal Code* also punishes anyone who willfully intercepts a private communication by electro-magnetic, acoustic, mechanical or other devises and is therefore similar in wording to the ECPA, the protection afforded by the Canadian legislation is potentially broader first, because of the *prima facie* expectation of privacy that exists in Canada around means of communications, and second, because the definition of "intercepting" is broader in Canada than in the United States. The *Criminal Code* also makes it a crime to disclose any information that was intercepted illegally.

[52] *Supra* note 24 at 338.

Restatement (Second) of the Law of Torts § 652A states that:

> "the right of privacy is invaded by: (a) unreasonable intrusion upon the seclusion of another […]; (b) appropriation of the other's name or likeness […]; (c) unreasonable publicity given to the other's private life […]; or (d) publicity that unreasonably places the other in a false light before the public."[53]

By way of contrast to the Nikon case in France, it would appear that American privacy law would not unconditionally protect the privacy of an employee. Morgan explains that while the tort of invasion of privacy may be effective in defending against a variety of privacy breaches, in the context of the workplace, unless an employer discloses the information obtained through monitoring, the only violation for which it may be found liable is unreasonable intrusion into seclusion of another.[54] To succeed in his or her claim, however, the employee must prove that: 1. there was an "intrusion"; 2. the intrusion was "highly offensive"; and 3. to a "reasonable person".[55] While electronic surveillance usually satisfies the first requirement, in order to determine if the intrusion is highly offensive, the court will examine "the degree of intrusion, the context, conduct and circumstances surrounding the intrusion, as well as the intruder's motives and objectives, the setting into which he intrudes, and the expectations of those whose privacy is invaded".[56] While the employer can invoke express or implied consent as a defence, a good faith belief in consent is insufficient.[57] Finally, the employee must prove that he or she had a subjective expectation of privacy and that this expectation is objectively reasonable – a case

[53] *Restatement (Second) of the Law of Torts*, § 652A (1997).
[54] *Supra* note 46 at 689.
[55] *Ibid*.
[56] *Ibid*.
[57] *Ibid*.

that, as discussed below, is very difficult to make in a workplace environment in the United States.[58]

In the United States, therefore, the right of the employer to monitor its employees in the workplace, while not absolute, is certainly strong. This is explained by the fact that personal information is considered a commodity that the employee exchanges in consideration for employment and justified by the fact that the employer owns the work tool. Case-law, such as *Watkins* v*. L.M. Berry & Co*.[59] nevertheless suggests that the right to monitor is not absolute. In this case, the 11th Circuit Court of Appeals decided that while an employer had the right to monitor working calls so as to ensure quality control – a policy of which the employees were informed – this did not give it the right to monitor personal calls.[60] Consent to the monitoring of business calls, could not, in the court's mind, be interpreted as general consent to monitor all calls.[61]

The above reasoning, however, has not been followed when it comes to monitoring email. In *Smyth* v. *Pillsburry Co.*, in which an employee sued his employer for invasion of privacy after the employer breached its own privacy policy, protecting the confidentiality of email, by using an unprofessional message sent by the employee to his manager to dismiss the employee, the court held that the employee had no reasonable expectation of privacy.[62] It claimed not to find "a reasonable expectation of privacy in e-mail communications voluntarily made by an employee to his

---

[58] *Ibid*.

[59] *Carmie Watkins, Plaintiff-appellant*, v. *L.M. Berry & Company, et al., Defendants-appellees*, 704 F.2d 577 (11th Cir. 1983).

[60] *Ibid*.

[61] *Ibid*.

[62] *Smyth* v. *Pillsburry Co*., 914. Supp. 97 (E.D. Pa. 1996), 98 ("**Pillsburry**").

supervisor over the company e-mail system notwithstanding any assurances that such communications would not be intercepted by management" and proceeded to stat that:

> "even if we found that an employee had a reasonable expectation of privacy in the contents of his e-mail communications over the company e-mail system, we do not find that a reasonable person would consider the defendant's interception of these communications to be a substantial or highly offensive invasion of his privacy.[…] Moreover, the company's interest in preventing inappropriate and unprofessional comments or even illegal activity over its e-mail system outweighs any privacy interest the employee may have in those comments."[63]

It is worth noting, as Morgan does, that Pillsbury may be an example of bad facts making bad law as the email sent by the employee allegedly contained violent content thereby requiring special cause for concern and action on behalf of the employer.[64] Moreover, as discussed below, the United States is somewhat unique among Common Law traditions in its explicit and relatively long-standing recognition and protection of a privacy right.

2.3 Privacy Protection in the United Kingdom

Given Canada's long-time status as a British colony and its inheritance of similar judicial and governmental structures, a discussion of the legal traditions that have influenced Canada would be incomplete without an overview of the United Kingdom's approach to privacy protection. At present, the United Kingdom, unlike the United States and some Canadian provinces, does not recognise a private right of action for breach of privacy. Instead, it seems to have expanded the application of the Common

[63] *Ibid*., at 101.

[64] *Supra* note at 46 at 871.

Law tort of breach of confidence to cover damages similar to those suffered for breach of privacy in other jurisdictions. It should be noted, however, that Britain does provide for the protection of data in the *Data Protection Act*.[65]

In his comparison of the privacy tort in several Common Law jurisdictions, Chris Hunt explains the reluctance of these jurisdictions to recognise the tort of invasion of privacy by citing: 1. Scope – does invasion of privacy require disclosure of information to be actionable as in the United Kingdom and New Zealand or is physical intrusion sufficient as in the United States?; 2. Doctrine – is the action grounded in tort law as in the United States and New Zealand or a modified version of breach of confidence as in the United Kingdom?; and 3 Conflict with other rights – most particularly with freedom of expression that the United States seems to privilege while New Zealand appears to privilege privacy.[66]

The conflict between privacy and freedom of expression is particularly apparent in *Campbell* v. *MGN Limited*, one of the first cases in the United Kingdom to recognise a private right of action for behaviour that amounted to breach of privacy by the media.[67] It did so by expanding the scope of the tort of breach of confidence. In fact, the apparent favouring of freedom of the press over privacy by the British bench has led to chastisement by scholars such as Gavin Philipson who note that "the

---

[65] 1998 c. 29.

[66] "Conceptualizing Privacy and Elucidating its Importance: Foundational Considerations for the Development of Canada's Fledgling Privacy Tort", (2011) 37:1 Queen's L.J. 167 at 169-171.

[67] Declaring that "[t]he time has come to recognise that the values enshrined in articles 8 and 10 are now part of the cause of action for breach of confidence" and that " [t]he values embodied in articles 8 and 10 are as much applicable in disputes between individuals or between an individual and a non-governmental body", the House of Lords expanded the reach of the tort of breach of confidence to cover instances in which an individual's privacy has been violated – especially in the media, [2004] UKHL at para 17 ("**Campbell**").

predominant approach of the courts fails structurally to afford privacy the respect it deserves as a Convention right, while remaining uncritically receptive to the claims of what, in many cases, amounts to markedly 'low value' expression".[68] As the law presently stands in the United Kingdom, it would appear that the tort of breach of confidence has been expanded to cover invasion of privacy between private parties. It should also be recalled that as a European Union member state, the United Kingdom is subject to the same supra-national legislation as France and Germany.[69]

Irrespective of the fact that the United Kingdom would appear to lag behind many jurisdictions on explicitly recognising a tort of invasion of privacy, the role that custom plays in the court's interpretation of the law means that privacy is a principle that has served as a backdrop against which many cases have been heard, and as such, is very present in the legal culture of the country. Historically, the United Kingdom has been opposed to any form of written constitution including a Canadian-style charter of rights as the power it places in the hands of the judiciary would interfere with the sacrosanct principle of parliamentary sovereignty. Murray Hunt explains that:

> "for Dicey, the British constitution rested on twin foundations: the absolute and continuing legal sovereignty of Parliament and a judicial commitment to a rule of law ideal which, subject only to Parliament's sovereign will, guaranteed the protection of an individual's private rights of property and analogous freedoms from state interference."[70]

[68] "Transforming Breach of Confidence? Towards a Common Law Right of Privacy under the Human Rights Act", MLR 66:5, September 2003, 726 at 727.

[69] At the time of writing, the United Kingdom had just voted to exit the European Union and the legal ramifications of this vote on European legislation to which it was subject are not yet clear.

[70] *Using Human Rights Law in English Courts*, Oxford, Hart Publishing, 1997 at 3.

Traces of this thinking can be found in the *Canadian Charter of Rights and Freedoms* that while binding on Parliament, includes s. 33 enabling a legislature to declare an act of Parliament or of the legislature to operate notwithstanding a provision in sections 2 or 5 to 7 of the Canadian Charter.[71]

The absence of a written constitution or charter of rights does not mean that the United Kingdom does not recognise or protect rights. In fact, the effect of a non-written constitution on the protection of privacy is well explained in several post-1998 *Bill of Rights* cases in which the House of Lords grapples with the paradigm shift required to interpret and implement an explicit protection of rights – and most notably the EUCR that was introduced into British law through the 1998 Bill. The challenge seems not to have been so much the concept of privacy itself as expressed in art. 8 of the EUCR, but that in the court's mind a tort of invasion of privacy was not necessary to remedy a breach of art. 8. This appears vividly in the 2003 House of Lord's decision in *Wainwright* v. *Home Office* in which Lord Hoffman clearly rejects the tort of invasion of privacy in English law.[72] He explains that "[t]here seems to me a great difference between identifying privacy as a value which underlies the existence of a rule of law (and may point the direction in which the law should develop) and privacy as a principle of law in itself"[73]. This does not mean that a protection of privacy does not exist in the United Kingdom but rather that it forms one of the customs against which law is interpreted. This subtlety is explained in Campbell by Lord Hoffman who states: "[t]his House decided in *Wainright* v. *Home Office* that

[71] *Constitution Act*, 1982 R.S.C., 1985, App.II, no 44 (the "**Canadian Charter**").
[72] [2003] UKHL 53.
[73] *Ibid*. at para 31.

there is no general tort of invasion of privacy. But the right to privacy is in a general sense one of the values, and sometimes the most important value, which underlies a number of more specific causes of action, both at common law and under various statutes".[74] The reluctance to define a specific right to privacy but to use the value as a norm against which to interpret various cases has arguably marked the Canadian judiciary.

****

The above comparison of privacy protection in continental Europe, the United States, and the United Kingdom explains the varying influences upon Canada's approach to privacy as discussed in the next chapter. The comparison also raises the question of whether, in the context of the workplace, privacy should even be considered a "right", be it the human right essential to the employee's dignity that the employee holds against the world or a property right that the employee barters as consideration for employment. Pushed to the extreme, these positions and their application to the workplace, lead to decisions, such as Nikon or Pillsburry, that strike one as fundamentally unfair. Just as in Nikon an employer should have some mechanism to protect confidential information – even if this means monitoring those who have access to it in some form or other – in Pillsburry, an employee working for a company, the policy of which is to respect the confidentiality of the employee's correspondence, should have a reasonable expectation of privacy. Perhaps the seeming injustice of both these decisions flows from a failure to view the workplace as a space where a

[74] Supra note 67 at para 43.

number of rights and obligations interact lending credence to the distinction Lord Hoffman draws between privacy as an interpretive principle rather than a right in and of itself. The extremes reflected in both Nikon and Pillsburry stand in sharp contrast to the more tempered Canadian approach.

Chapter 3. Being Reasonable:

The Canadian Approach to Privacy Protection and the Impediments it Poses to Industry Challenge

The evolution of Canada's and Quebec's privacy regimes betrays the blend of influences discussed in the previous chapter. Up until 2001, the country's approach to privacy protection, at the federal level at least, resembled that of the United States in that it was mostly regulated on a sectorial basis through legislation such as the *Radio Communications Act*,[1] the *Telecommunications Act*,[2] the *Bank Act*[3] and the *Canada Post Act*[4]. At a provincial level, it was also protected by sector-specific legislation and statutory tort provisions. Over the course of four years, between 2000 and 2004, and in response to commercial pressures from the European Union, the *Personal Information Protection and Electronic Documents Act* came into effect, providing comprehensive private sector privacy protection in provinces that did not have their own legislation and across the country for organizations that handle information in connection with the operation of a federal work, undertaking or business or that conduct interprovincial or international trade activities.[5] It was followed shortly after by similar provincial laws in Alberta[6] and British Columbia.[7] In Quebec, an individual's personal information had been protected, since 1993, by *An Act Respecting the*

---

[1] R.S.C., 1985, c.R-2.
[2] S.C. 1993, c.38.
[3] S.C. 1991, c.46.
[4] R.S.C., 1985, c.C-10.
[5] S.C. 2000, c. 5 ("**PIPEDA**").
[6] *Personal Information Protection Act*, S.A. 2003, Chapter P-6.5 ("**Alberta PIPA**").
[7] *Personal Information Protection Act*, S.B.C. 2003, Chapter 63 ("**BC PIPA**").

Protection of Personal Information in the Private Sector,[8] but as of 2004, if that individual transacted with a federal work or undertaking or with an organization, this information could also be protected by PIPEDA.

At the same time these laws were being tabled, debated, and enacted, Canadian Courts were also active in defining privacy only in a pondered way reminiscent of the United Kingdom's bench. An important body of case law, then, was beginning to emerge largely in connection with section 8 of the *Canadian Charter of Rights and Freedoms* that protects against unreasonable search and seizure, and to a lesser extent, section 7 that provides for "the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice".[9] The analysis adopted by the Supreme Court of Canada ("**Supreme Court**") to interpret these provisions is neither a purely Civil Law nor a purely Common Law approach but consists in establishing whether an expectation of privacy exists, if so whether it was violated, and in the affirmative, whether this violation is justifiable given the context in which it occurred. At present, therefore, privacy protection in Canada reflects a tension between an explicit legislative recognition and protection of this right, as in Continental Europe and the United States, and a more normative interpretation of this right by the courts that, as in the United Kingdom, appear reluctant to define and defend it in absolute terms.

So as to understand the balance that might be struck between an organization's right to use workforce demographics to market itself and Quebec's private sector privacy

[8] Chapter P-39.1 ("**PPIPS**").

[9] *Constitution Act*, 1982 R.S.C., 1985, App.II, no 44 ("**Canadian Charter**").

legislation, the pages that follow will review the Canadian courts' analysis of privacy, first in search and seizure instances and then in cases between private parties, notably involving the workplace, before focussing specifically on the provisions of PPIPS and PIPEDA that most hinder an organization's response to an Industry Challenge (as defined in Chapter 1). The two impressions that stand out from such an analysis are first, the court's refusal to interpret privacy as an absolute right but rather as an interest to be weighed against competing interests, and second, the legislation's embodiment of values that have since evolved and may require adapting to a new reality.

3.1 Privacy Before the Courts

3.1.1 Search and Seizure Provisions Interpreted

Although it would be inaccurate to claim that the Supreme Court has followed the House of Lords in defining the content of a right to privacy – especially since the reverse appears to be the case[10] – its analytical approach to this right, to a certain extent, reflects the custom-based reasoning of the Law Lords. For example, while the Supreme Court has defined privacy as "a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state"[11], it has never enumerated specifically what this information might be. Instead, it has developed the notion of "interests", linked to individuals not to places, which must be attributed particular care by law enforcement

[10] See for example *Campbell* v. *MGN Limited*, [2004] UKHL, in which Lord Nicholls cites *R*. v. *Dymen*t [1988] 2 S.C.R. 417 ("**Dymen**t") and Lord Hope cites *Aubry* v. *Les Editions Vice-Versa Inc*. [1988] 1 S.C.R. 591 ("**Aubry**"), at paras. 12 and 120.

[11] *R*. v. *Plant* [1993] 3 S.C.R. 281 at 293.

officials who seek access to them. Two often intertwined inquiries mark the Supreme Court's analysis of what constitutes a protected interest. The first consists in establishing whether a person has a privacy interest in the matter before the court. To do so, a second step is required, that of determining whether the type of privacy violation alleged by the individual corresponds to one of the three types of interests that are worthy of protection

3.1.1.1 Striking a Balance

The Supreme Court weighs four elements to establish the existence of a privacy interest: 1. the subject matter of the alleged search; 2. the claimant's interest in the subject matter; 3. the claimant's subjective expectation of privacy in the subject matter; and 4. whether the subjective expectation is objectively reasonable given the totality of circumstances.[12] This analysis has led the Supreme Court to conclude that, for example, an individual does not have a privacy interest in energy patterns emanating from his home.[13] It also led to the ruling that the use of a computer belonging to a school board that has set policies regarding its use lowered but did not abolish the user's expectation of privacy.[14] Likewise, it held that the statutory and contractual framework governing an internet service provider's disclosure of subscriber information contributed to but were not determinative of a subscriber's reasonable expectation of privacy.[15]

---

[12] R. v. *Spence*r 2014 S.C.C. 43 (CanLII) at para. 18 ("**Spencer**").
[13] *R*. v. *Tessling* [2004] 3 S.C.R. 431 at 451 ("**Tessling**").
[14] *R*. v. *Cole*, [2012] 3 S.C.R. 34 at 51.
[15] *Supra* note 12, at para. 54.

3.1.1.2 Protected Interests

The second characteristic of the Supreme Court's analysis of a "privacy interest" is the notion of the interest protected. These limited numbers of interests are deemed to be more private than others and consequently meriting greater caution when attempting to gain access to the information they harbour. In Dyment, the Supreme Court identifies three, frequently overlapping, interests that are worthy of protection: personal, territorial, and informational.[16]

Personal privacy interests include mostly interests attached to an individual's physical being. Traditionally, this interest has been perceived as giving rise to the most serious violations of an individual's reasonable expectation of privacy.

Territorial or spatial interests, including most particularly the home, have also been deemed worthy of vigilant protection. Certain examples of what could be included in a territorial or spacial privacy interest are, in an order of diluted expectation: the perimeter space around the home, commercial space, a private car, a school, and at the bottom of the spectrum, a prison.[17]

The third interest recognised by the court is an informational privacy interest. It often overlaps with other interests as a result, notably, of computers and portable telecommunication devices. This right includes the right to store and control information and possibly the right to anonymity.

---

[16] *Supra* note 10 at 428.

[17] Supra note 13 at 444.

An argument could be made that the Supreme Court is moving in the direction of recognising a fourth privacy interest: informational privacy. In recent decisions it seems to suggest that, as a result of the nature and quantity of information they contain, computers and portable phones cannot be considered an extension of the person or place being searched but require special considerations. In *R.* v. *Vu*, the Supreme Court decided that given the access they provide to information about an individual, computers were not to be treated as a cupboard or filing cabinet.[18] It underlined the fact that computers: 1. store immense amounts of information some of which will touch the biographical core of personal information; 2. contain information that is automatically generated often unbeknownst to the user; 3. retain files and dates even after the user thinks they have deleted these; and 4. provide law enforcement agents, in the case of a computer linked to the internet, with access to other devices, documents, and information that are not in any meaningful sense at the location for which the search is authorised.[19] The exception accorded to computers was extended to mobile phones in *R. v. Fearon*.[20] Ironically, it often seems that it is within this informational sphere that individuals appear to behave with the greatest insouciance with respect to their personal information.

3.1.1.3 Abandonment

A particularly interesting feature of the Supreme Court's analysis is the notion that

[18] [2013] 3 S.C.R. 657 at 663.

[19] *Ibid*., at 676.

[20] The minority decision in this case is particularly interesting as it suggests that technology may have a closer connection to the individual's privacy interest than their physical being. Justice Karakatsanis writes that "the incredible and unique power of modern digital communication devices as portals to vast stores of information – and their ability to expose our private lives – means that they can be even more threatening to our privacy than the search of our homes", [2014] S.C.R. 77 (CanLII) at para 134 ("**Fearon**").

privacy is not absolute but can be abandoned if an individual deliberately behaves in such a way as to lead a reasonable person to assume that they have forgone a right to privacy. In Tessling, Justice Binnie states that "a person can have no reasonable expectation of privacy in what he or she knowingly exposes to the public, or to a section of the public, or abandons in a public place".[21] In *R*. v. *Patrick*, he adds that "[a]bandonment is therefore an issue of fact. The question is whether the claimant has acted in relation to the subject matter of his privacy claim in such a manner as to lead a reasonable and independent observer to conclude that his continued assertion of a privacy interest is unreasonable in the totality of the circumstances".[22] Privacy is not an absolute right but a question of what is reasonable under the circumstances.

3.1.2 Interpreting Privacy Breaches by Private Parties

As with the enforcement of a privacy right in search and seizure cases, protecting the individual's right to privacy against a breach by another private party requires first, establishing whether such a right existed and was violated illicitly, and second, whether other considerations might justify the violation. This approach has marked cases dealing notably with the conflict between privacy and freedom of the press such as Aubry[23] and *A.B*. v. *Bragg Communications Inc*[24]. The paragraphs that follow, however, discuss the right to privacy in the context of a workplace where employers' and employees' interest are often at odds as they might be in cases involving Industry Challenges.

---

[21] *Supra* note 13, at 451.
[22] [2009] 1 S.C.R. 579 at 596.
[23] *Supra* note 10.
[24] [2012] 2 S.C.R. 567.

3.1.2.1 Workplace Surveillance

Similar to the analysis developed in Canadian Charter cases, jurisprudence on workplace surveillance reveals neither a purely Common Law nor a purely Civil Law understanding of a right to privacy in the workplace but rather decisions based upon what is reasonable once all the interests have been weighed. This is hardly surprising since the law provides for what sometimes can appear to be competing obligations on employers and employees. For example, art. 2085 of the *Civil Code of Quebec* gives the employer the right to direct and control the employee,[25] but in turn the employer must "take any measures consistent with the nature of the work to protect the health, safety and dignity of the employee".[26] The employee is bound "to act faithfully and honestly and not to use any confidential information he obtains in the performance or in the course of his work".[27] While an employee may have a right to privacy, it is difficult to conceive how an employer can ensure that it is meeting all its obligations without the ability to monitor its employees.

In an employment context arbitration panels and courts seem to balance a perceived right against other considerations. For example, according to Michael Geist, in *Doman Forest Products Ltd* the court applied *R.* v. *Duarte*[28] to the employer-employee context to conclude that a right to privacy was not absolute but must be judged against what was reasonable under the circumstances which in turn depended

[25] S.Q. 1991, c.64 ("**CCQ**").
[26] *Ibid*. at art. 2087.
[27] *Ibid*. at art. 2088.
[28] [1990] 1 SCR 30.

upon the competing interests of the parties.[29] In determining reasonableness the arbitrator pointed to: a). whether it was reasonable to request the surveillance; b) whether surveillance was conducted in a reasonable manner; c) whether there were similar alternatives to surveillance opened to the employer.[30]

Likewise, the Quebec Court of Appeal's controversial decision in *Syndicat des travailleurs(euses) de Bridgestone Firestone de Joliette (csn)* c. *Trudeau*[31], fifteen years ago, but still valid today, seems to have consolidated this weighing of interests. The case addresses an employer's use of videotaped images of an employee on disability leave gardening, collecting his son from daycare, and going about his business in town, to prove that the employee was, in fact, not as disabled as he had claimed.[32] In rendering his decision, Justice LeBel confirmed the Superior Court's finding that while an employer's surveillance of its employee constituted a violation of the latter's right to privacy, this right was not absolute and the surveillance of the employee outside his work could be conducted provided: 1. it was justified by rational motives; 2. it was conducted by reasonable means; 3. it appeared necessary to monitor the behaviour of an employee; and 4. it was conducted in the least intrusive manner possible.[33] Understandably, the decision has been criticised by authors, such as Karen Eltis, for moving Quebec away from a Civil Law understanding of an employee's right to privacy, anchored in the dignity of the employee, to an American

[29] Geist, Michael, "Computer and E-Mail Workplace Surveillance in Canada: The Shift From Reasonable Expectation of Privacy To Reasonable Surveillance" (2003) 82 R. du B. can. 1 at 26-7.

[30] *Ibid*.

[31] 1999 CanLII 13295 (QC CA).

[32] *Ibid*.

[33] *Ibid*.

understanding in which the employee's right is more akin to a property right.[34] Less preoccupied with the preservation of legal systems than Eltis, Geist simply summarizes the case law on workplace surveillance as "surveillance is permitted, but only where a substantial problem has been identified, the surveillance is likely to solve the problem, alternative approaches have been unsuccessfully pursued, and the surveillance is implemented in a fair, even-handed manner".[35] In other words, it must be reasonable! The court's tendency to balance competing rights is an important backdrop against which to read the private sector privacy legislation in effect in Quebec as it provides some guidance with respect to the interpretation and application of these laws.

3.2 PPIPS and PIPEDA

As mentioned briefly in the introduction to this chapter, the two laws that are most relevant to understanding the privacy protection applicable to the Quebec private sector are PPIPS and PIPEDA. An overview of the context form which they emerged, their structure, their purpose, and their provisions that are the most cumbersome to an organization's ability to respond to an Industry Challenge, reveal the areas in which interpretive or legislative changes may be required to accommodate present market practices.

3.2.1 Some Context

According to Eloise Gratton, both PPIPS and PIPEDA reflect the concerns of a third

[34] Eltis, Karen, "La surveillance du courrier électronique en milieu de travail : le Québec succombera-t-il a l'influence de l'approche américaine?", (2006) 51 McGill L.J. 475.

[35] *Supra* note 29 at 28.

wave of privacy protection when the main threat to privacy was perceived to come from electronic data processing and notably the volume of data involved, its storage and retrieval techniques, its transmission over long distances as well as the speed at which these operations could be performed and the high storage capacities of computers.[36] To protect against this, privacy came to mean "control over personal information" and a series of fair information practice ("**FIP**"s) were developed[37] that now form the core of most data protection legislation. These FIPs are reflected in PPIPS and PIPEDA that, regardless of their slightly different purposes, which will be discussed below and in Chapter 5, define "personal information" narrowly and regulate its collection, use, and transfer. Although this restriction does not apply to "personal information which by law is public", in the case of PPIPS[38], or "publicly available", in the case of PIPEDA[39] ("**Public Information**"), the type of information deemed public is either restrictively defined in a regulation, in the case of PIPEDA[40], or it must be identified as such in a statute, in the case of PPIPS.

3.2.2 Structure and Purpose

Whereas both PPIPS and PIPEDA regulate the same activity, that is to say the collection, use, and transmission of personal information, PIPEDA expressly seeks to balance the rights of the individual with that of the organization while PPIPS, as it is

---

[36] Gratton, Eloise, *Understanding Personal Information: Managing Privacy Risks*, Markham, ON, Lexis Nexis Canada Inc., 2013 at 21.

[37] These FIPs attempt to place the individual in control of their personal information by providing them with the right to know the information about them that is being shared, the purpose for which it is collected or communicated and how to have incorrect information corrected or erased. *Ibid*., at 10.

[38] *Supra* note 8 at s.1.

[39] *Supra* note 5 at ss. 7(1)(d), 7(2)(c.1), 7(3)(h.1)

[40] *Regulations Specifying Publicly Available Information* SOR /2001-7.

drafted, seeks exclusively to protect the individual's right not to have his or her privacy invaded as set out in articles 35 to 40 of the CCQ. PPIPS clearly states that its object is to:

> "establish, for the exercise of the rights conferred by articles 35 to 40 of the Civil Code concerning the protection of personal information, particular rules with respect to the personal information relating to other persons which a person collects, holds, uses or communicates to third persons in the course of carrying on an enterprise within the meaning of article 1525 of the Civil Code."[41]

While it would be tempting to argue that PPIPS focuses exclusively on the protection of privacy, and indeed its structure that contains a series of provisions, enforcement and oversight mechanisms and clear penalties for the violation of the law would suggest as much, it is important to recall that during the parliamentary debates at which PPIPS was first introduced the Honourable Laurence Cannon, Minister of Communications, emphasized that while "le Quebec était mur pour une loi qui protégerait les renseignements personnels détenus dans le secteur privé. […] une telle législation ne devait pas freiner la compétitivité des entreprises du Québec".[42] Seemingly, the legislator did not intend the individual's right to privacy to be so absolute as to interfere with other interests such as those of Quebec businesses.

In contrast to PPIPS' apparently singular focus, PIPEDA, as its name and structure suggest, seeks to balance many interests. Its purpose as set out in s. 3 is to establish:

---

[41] *Supra* note 8 at s. 1.

[42] Commission permanente de la culture, Fascicule no 11, 23 février 1993, p 337 at 338.

> "rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances."[43]

PIPEDA's structure appears less focussed than that of PPIPS. It contains six parts[44], only the first two and last of which contain any legislation. Inspired by the Canadian Standards Association's Model Code, a voluntary code of conduct, PIPEDA sets out the principles governing, among others things, the use, collection, storage and communication of information not in the body of the legislation, but rather in a Schedule 1[45]. The voluntary nature of this legislation is further emphasised by s. 5(2) that specifies: "[t]he word "should", when used in Schedule 1, indicates a recommendation and does not impose an obligation", and by the fact that, unlike the Quebec Privacy Commission, the decisions of which are executable by the Superior Court of Quebec, the Federal Privacy Commissioner's report must be brought before the Federal Court for hearing[46]. The Federal Privacy Commission would seem to play an advisory role to industry as it can investigate a complaint,[47] assist in resolving a complaint through various dispute mechanisms,[48] or conduct audits[49]. It cannot levy fines and render enforceable judgements.

---

[43] *Supra* note 5 at s. 3.

[44] Protection of Personal Information in the Private Sector, Electronic Documents, Amendments to the Canada Evidence Act, Amendments to the Statutory Instruments Act, Amendments to the Statute Revision Act, and Coming into Force – and three Schedules – the CSA standards, Acts of Parliament, and Regulations and other instruments.

[45] These principles are: Accountability; Identifying Purposes; Consent; Limiting Collection; Limiting Use, Disclosure, and Retention; Accuracy; Safeguards; Openness; Individual Access; and Challenging Compliance.

[46] *Supra* note 5, at s. 14(1).

[47] *Ibid*., at s. 11(2).

[48] *Ibid*., at s. 12.1(2).

Despite the comment of the former Quebec Privacy Commissioner, Paul-André Comeau, upon reading the Bill that was to become PIPEDA, that PPIPS was aimed at giving effect to privacy rights whereas PIPEDA focussed on the facilitation of commerce[50], as discussed below, with respect to the efficient response to Industry Challenges, neither law plays a particularly facilitating role. The pages that follow, therefore, focus on the provisions of both laws that are most relevant in the context of an Industry Challenge: consent, personal information, collection, use, communication, and exceptions.

3.2.3 The Provisions

The importance of consent as well as the broad definition of Personal Information and the restrictions placed on its collection, use, and transfer can severely impede an organization's response to an Industry Challenge.

3.2.3.1 Consent

A foundational principle of the FIPs, consent is the most obvious restriction PPIPS and PIPEDA place on an organization's ability to respond to an Industry Challenge. Whereas PIPEDA requires "[t]he knowledge and consent of the individual […] for the collection, use, or disclosure of personal information, except where inappropriate"[51], PPIPS only obliges the collector to inform the subject of the object of the file, the use to which the information will be put, the person within the organisation who will have access to it and where the files will be kept and the rights of access and

---

[49] *Ibid*., at s. 18.

[50] Scassa, Teresa and Deturbide, Michael, *Electronic Commerce and Internet Law in Canada*, 2nd. Ed., Toronto, CCH Canada Limited, 2012, at 97.

[51] *Supra* note 5, at Schedule 1, Principle 4.3.

rectification.[52] The individual's consent, however, is required for a use or transmission different from the original stated use or transmission.[53] PPIPS is firm that "[c]onsent to the collection, communication or use of personal information must be manifest, free and enlightened, and must be given for specific purposes. Such consent is valid only for the length of time needed to achieve the purpose for which it was requested".[54]

While PIPEDA requires a subject's consent for the collection, use, and communication of Personal Information, it is more flexible than PPIPS on the nature of this consent. The law allows for consent to be provided in different ways depending on the sensitivity of the information sought. It recognises that "[t]he form of the consent sought by the organization may vary, depending upon the circumstances and the type of information"[55]. It also states that:

> "[t]he way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive"[56].

This approach to information collection was the subject of *Randall* v. *Nubodys Fitness Centres* in which the Federal Court adopted the view of the Privacy Commissioner that information concerning the number of times an employee used a fitness facility on an employer-sponsored plan and communicated this information to the employer, constituted information that was at the lower end of the sensitivity scale and therefore

---

[52] *Supra* note 8, at s. 8.
[53] *Ibid.*, at ss. 12 and 13.
[54] *Ibid.*, at s. 14.
[55] *Supra* note 5 at Schedule 1, Principle 4.3.4.
[56] *Ibid.*, at Schedule 1, Principle 4.3.6.

implied, rather than explicit, consent was appropriate for its collection and transmission.[57] This decision illustrates the court's willingness to balance competing interest so as to reach a decision that is reasonable under the circumstances.

3.2.3.2 Personal Information

PIPPS and PIPEDA provide for excessively inclusive definitions of personal information. According to PPIPS, personal information includes "any information which relates to a natural person and allows that person to be identified",[58] according to PIPEDA, it includes any "information about an identifiable individual"[59] ("**Personal Information**"). Both laws allow exceptions for employee information.[60] The point to retain though is that, as defined in both laws, personal information is much broader in scope than private information. For example, information may be public, such as a telephone number, but still qualify as personal information requiring protection under PPIPS and PIPEDA.

Moreover, as discussed below, although PPIPS and PIPEDA recognise some exceptions to the extremely inclusive definition of Personal Information, these exceptions do not allow for the type of information required by Industry Challenges. As argued in the next chapter, a definition that excludes: 1. data made public by the subject; 2. employee data necessary for the operation of an enterprise; and 3. data

---

[57] 2010 FC 681 (CanLII) at 12.

[58] *Supra* note 8 at s. 2.

[59] *Supra* note 5, at s. 2.

[60] See description of "business contact information in PIPEDA. *Ibid*., at s. 2. Likewise, in "Le marketing direct : les obligations des entreprises", the Commission d'accès à l'information du Québec explains that implicit consent exists between employees and management for the use of nominative lists defined in s. 22(3) of PPIPS to include the name, telephone number, geographic or technological address of the person in question. See www.cai.gouv.qc.ca.

required to participate in programs destined to remedy social inequality, would greatly improve a Quebec company's ability to respond to their client's diversity initiatives.

3.2.3.3 Collection

PPIPS and PIPEDA also restrict the scope of information that an organization is permitted to collect and regulate the methods used to collect it. Both the federal and the provincial laws subject the collection of information to strict content and procedural requirements and prevent an employer from fishing for information on its employees. PPIPS requires a "serious and legitimate reason"[61] for the collection, whereas PIPEDA requires a reasonable purpose[62]. Moreover, PPIPS states that the information collected must be "only the information necessary for the object of the file",[63] and PIPEDA's Limiting Collection Principle suggests an organization collect only that information necessary for the purposes identified by the organization[64].

Both laws require the collection to occur through lawful means. PPIPS forbids an enterprise from not responding to a request for goods, services or employment if an individual fails to provide personal information unless such information was necessary to perform the contract, the collection is authorised by law or there are reasonable grounds to believe the request was not lawful.[65] It confirms that "[i]n case of doubt, personal information is deemed to be non-necessary".[66] Likewise, PIPEDA prevents an organization from making consent to collect, use or disclose information a

[61] *Supra* note 8, at s. 4.
[62] *Supra* note 5, at s. 3.
[63] *Supra* note 8, at s. 5.
[64] *Supra* note 5 at Schedule 1, Principle 4.4.
[65] *Supra* note 8, at s. 9.
[66] *Ibid*.

precondition to the supply of a product or service.[67] The limits placed on collection would, among other things, prevent employers from scouring social media sites for information on their employees since the amount of information available on these sites, and inadvertently collected in the process, would surely exceed that which is necessary for the object of the file.[68]

3.2.3.4 Use

Closely linked to the restrictions placed on the collection of information are the rigid use requirements contained in PPIPS and PIPEDA. According to both laws, the use to which the information may be put must be reasonable or legitimate, it must be expressed to the person whose information is collected and it cannot be changed without the consent of the individual involved. Once the object of the file has been achieved, as stated above, PIPPS prevents the information from being used in another way without the consent of the person and subject to a retention schedule prescribed by law.[69] Likewise, PIPEDA states that "[p]ersonal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law".[70]

The restrictions placed on use prevent an organization from repurposing information which is in the public domain without the consent of the individual concerned. Although information contained in public registries or court reporters is considered to

---

[67] *Supra* note 5, at Principle 4.3.3.

[68] This is an observation made by the Office of the Information and Privacy Commissioner of Alberta in "Guidelines for Social Medial Background Checks", December 2011, at 3.

[69] *Supra* note 8, at s. 12.

[70] *Supra* note 5, at Schedule 1, Principle 4.5.

be publicly available, this information cannot be used for a purpose other than that for which it was used in the registries or reporters without the subject's consent.[71] Also, while PIPEDA regulations consider information that an individual has provided to a "magazine, book or newspaper, in printed or electronic form" to be publicly available, and not subject to consent, if another use is to be made of the information without the owner's consent, the information in question must have been provided by the owner – thus excluding unauthorised biographies – and the subsequent collection, use, and communication of this information subject to what a reasonable person would consider appropriate in the circumstances.[72]

In instances in which organisations respond to several calls for tender daily, some of which contain Industry Challenges, PPIPS' and PIPEDA's provisions on the collection and use of Personal Information create a situation that is both cumbersome and highly inefficient to manage. It would appear that this legislation requires the employee's consent to collect and use its information for each Challenge – as the legislation prevents the repurposing of information or its use in a way other than for that which the original consent was requested. It is difficult to understand how this could be anything but frustrating for an employee who is repeatedly solicited to consent to providing the same information.

3.2.3.5 Communication

As discussed more extensively in Chapter 5, another major obstacle to effective participation in an Industry Challenge is the constraint on communication of personal

[71] *Supra* note 50 at 148-149.
[72] *Ibid*., at 150.

information imposed by PPIPS and PIPEDA. Both PPIPS and PIPEDA require the consent of the person concerned before their personal information can be communicated.[73] PIPPS also imposes obligations on the person communicating the information to ensure that the recipient has safeguards offering the same protection of this information as the original holder.[74] This can present a substantial obstacle in the event that information must be sent abroad notably to the United States, that, as previously described, does not have the same approach as Canada to the protection of personal information.

Furthermore, even if, as noted above, PPIPS s. 23 allows for the communication of nominative lists of clients, members or employees, provided the person concerned has been given the opportunity to refuse consent,[75] the commercial value of these nominative lists remains minimal without the relevant personal information. As evidenced in *Deschesnes* v. *Groupe Jean Coutu (P.J.C.) Inc*[76] in which Groupe Jean Coutu was held to be in violation of PPIPS for transmitting the names and mailing addresses of clients suffering from diabetes to an industry-sponsored event on the illness, the value of the list was not the name and address of the client, but the fact that these were connected to a person suffering from diabetes. The information

[73] *Supra* note 5 at s. 13, and *supra* note 1 at Schedule 1, Principle 4.3.

[74] *Ibid*., at s. 17. With respect to safeguards, s. 10 specifies that "[a] person carrying on an enterprise must take the security measures necessary to ensure the protection of the personal information collected, used, communicated, kept or destroyed and that are reasonable given the sensitivity of the information, the purpose for which it is to be used, the quantity and distribution of the information and the medium on which it is stored." Interestingly, PIPEDA Schedule 1, Principle 4.7 provides greater detail and guidance on appropriate safeguards than PPIPS. While PIPEDA does not appear to require the recipient of information to have in place the same safeguards as the sender, the Office of the Privacy Commissioner recommends informing individuals of the possibility that their information may be sent to another organisation and, if this organisation is outside Canada, of the laws applicable in the recipient jurisdiction, *supra* note 50, at p. 168-169.

[75] *Supra* note 8 at s. 17(2).

[76] [2000] C.A.I., 216.

pertaining to the individual's health, not surprisingly, was deemed by the Quebec Privacy Commissioner to be personal and therefore subject to protection. Without this information, however, it is difficult to see what value the nominative list could provide.

3.2.3.6 Exception

Despite the limits PPIPS and PIPEDA place on the collection, use, and communication of personal information, certain exceptions exist. These can be grouped into two categories. First, the restrictions do not apply to the collection, use and communication of Public Information. Second, they do not apply to activity that falls broadly into three categories: a) journalistic and scholarly purposes; b) information concerning an individual whose consent may not be obtained in time to protect his or her interests (such as health); and c) information required by law or related to law enforcement.[77] It should be noted, however, that according to the Supreme Court in Spencer, "lawful authority" in PEPIDA s. 7(3)(c.1)(ii) does not create a police search and seizure power.[78] A warrant is still required by law enforcement agents requesting information under this provision.

****

Canada's approach to privacy protection reflects a mixture of competing legal influences. Laws such as PPIPS and PIPEDA that are based on the same FIPs as their European counterparts, explicitly recognise privacy as a right by protecting the collection, use, and transmission of Personal Information. When, however, this right

[77] *Supra* note 5, at.7; *supra* note 8, at. 1, 6, 7 and 18.
[78] *Supra* note 12 at para. 71.

conflicts with other rights, such as freedom of the press, workplace surveillance or criminal law, a more tempered protection of privacy is often adopted by the courts. In these cases, privacy is far from an absolute right and even sometimes more of a concept or backdrop against which a conflict is resolved. Moreover, the restrictions these laws place on a company's effective participation in an Industry Challenge fail to acknowledge a present market reality that did not exist as widely at the time they were enacted. Indeed, the broad definition these laws provide of Personal Information as well as the restrictions they place on its collection, use, and transfer without the subject's consent render it practically impossible for an organisation to respond satisfactorily to an Industry Challenge. This, in turn, places Quebec companies at a competitive disadvantage. It could be that existing legislation, having emerged during the third wave of privacy protection referred to above, is no longer adapted to contemporary needs? If so, what can be done to address this? Some possible solutions explored in the next two chapters are: amending or purposefully interpreting certain provisions of PPIPS and PIPEDA (Chapter 4) or, failing this, challenging these laws for their infringement on a company's right to commercial expression (Chapter 5).

Chapter 4.
Purposefully Interpreting Quebec's Privacy Legislation

Although *An Act Respecting the Protection of Personal Information in the Private Sector*[1] and the *Personal Information Protection and Electronic Documents Act*[2] purport to enable individuals to control the information that concerns them, these laws present substantial obstacles to companies wishing to participate in Industry Challenges (as defined in the Introduction). Shifts in business models and market trends require a rethinking not only of the reasons and methods used to protect data but, more concretely, of the measures required of present privacy legislation to accommodate a company's right to express itself commercially.

The present chapter is one of two that explores the interpretive, legislative, and judicial recourses that might be taken to permit a business to respond efficiently and effectively to an Industry Challenge. Focussing on the interpretive and legislative changes that could be brought to PPIPS and PIPEDA, it questions whether it is not time to review certain provisions so as to better align the laws with current commercial realities discussed in the Introduction. It applies the risk analysis developed by Gratton in her purposive approach to interpreting the concept of Personal Information (as defined in Chapter 3), and argues that the notion of Personal Information in PPIPS and PIPEDA should be interpreted or amended to exclude information: 1. made publicly available by the individual; 2. collected by an

[1] Chapter P-39.1 ("**PPIPS**").
[2] S.C. 2000, c. 5 ("**PIPEDA**").

employer and that is necessary for the proper functioning of its enterprise; and 3. required to respond to programs aimed at remedying social inequality.

4.1 A Purposive Approach to PPIPS and PIPEDA

The impediments PPIPS and PIPEDA pose to companies seeking to respond to an Industry Challenge raise many questions not the least of which are what exactly should data protection laws by protecting? Are PPIPS and PIPEDA protecting it? Could changes be brought to these laws that would facilitate private sector participation in Industry Challenges without compromising the individual's right to protect information he or she deems private? The pages that follow review the purpose for data protection laws ("**DLP**"s), examine an alternative method of approaching such protection, and suggest three interpretive / legislative changes to PPIPS and PIPEDA that would accommodate companies responding to Industry Challenges without compromising the individual's right to protect their Personal Information.

4.1.1 What Should DLPs be Protecting?

An answer to this question requires a review of present privacy risks. If Gratton's hypothesis is correct that a fourth wave of privacy concerns is upon us, then DLPs that focus on control of Personal Information - in response to concerns characteristic of the third wave of privacy protection - may not be as relevant as they once were. Increased volumes of information, new types of information collection tools (such as cookies), new identifying methods (such as aggregation and collection of data, data mining, and convergence in technologies), new uses of information (such as law

enforcement, research and development, and targeted advertising), and increased availability of data, challenge not only the notion of an identifiable individual but the very possibility of control.[3] In this new environment, Personal Information, according to Gratton, becomes a concept that is at once over inclusive and under inclusive, riddled with uncertainty and, in some circumstances, even obsolete.[4] At present, providing individuals with absolute control over their Personal Information both disrupts the flow of information that is important to society and prevents collection, use and communication for otherwise legitimate ends.

4.1.2 Alternate Approach to Protecting Privacy

In light of the above, DLPs allowing the individual exclusive control over Personal Information appear inadequate to cope with the challenges of the fourth wave of privacy concerns. But instead of doing away with them, Gratton proposes a purposive interpretation that measures the risks of harm posed to the individual in the event his or her Personal Information were to be mishandled. As this approach will be useful in justifying the three amendments, discussed below, that might be brought to PPIPS and PIPEDA, it warrants some attention.

4.1.2.1 Purposive Interpretation

To address the shortcomings of PPIPS and PIPEDA, Gratton suggests adopting a purposive interpretation of Personal Information in which only information that presents a risk of harm to the individual would be protected. Referring to Aharon

---

[3] Gratton, Eloise, *Understanding Personal Information: Managing Privacy Risks*, Markham, ON, Lexis Nexis Canada Inc., 2013 at 21-55.

[4] *Ibid*., at 91-141.

Barak's work, she explains this approach by stating that: "[e]stablishing the ultimate purpose (and therefore, the relevant legal meaning) depends 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".[5] As the ultimate purpose of data protection legislation is to "protect individuals against a risk of harm that may be triggered by organisations collecting, using and disclosing their personal information", a purposive interpretation of Personal Information takes into consideration the fact that risks are a function:

> "of several variables, such as situation-specific circumstances, the intentions of the parties involved, the kind of information being sought and the way it is processed. Other variables include the historical context, the particular type of technology in question, the political environment, the nature of the information within a given context and the vulnerability of the individual."[6]

Assessing what information poses a risk, and therefore qualifies as Personal Information, requires identifying the activity – collection, use, transmission – which causes the risk as well as the importance and extent of the risk.[7] Gratton divides risk into two categories, subjective and objective, maintaining that data that are collected or disclosed risk causing only subjective harm. She adds that with respect to data that is collected, the risk is triggered only when the data is disclosed and therefore the collection of data generally should not be covered by DLPs.[8] Furthermore, whether disclosed information poses a risk of harm will depend on its level of identifiability, intimacy, and availability: the higher the

[5] *Ibid.,* at 157.
[6] *Ibid*., at 157-8.
[7] *Ibid*., at 180.
[8] *Ibid*., at 224.

degree of identifiability and intimacy and the lower the level of availability, the greater the risk of harm.[9] The use of information, on the other hand, risks causing objective harm such as discrimination, financial or physical harm.[10] Consequently, if the use of particular data risks causing objective harm, it should qualify as Personal Information and be kept accurate and relevant.[11] If its use does not have the potential to cause this harm it should not qualify as Personal Information.[12]

4.2 Applying a Purposive Approach

Gratton's purposive approach, and especially, the risk analysis it contains, will be applied in the pages that follow to demonstrate how three changes to PPIPS and PIPEDA would greatly improve a company's ability to respond to Industry Challenges while at the same time minimising individual privacy risks. All three require interpreting Personal Information to exclude: 1. data made publicly available by the individual; 2. employee data necessary for the operation of an enterprise; and 3. data required by programs intended to remedy social inequalities.

4.2.1 Data Made Publicly Available by the Individual

Adapting the definition of Personal Information in PPIPS and PIPEDA to exclude information that has been deliberately disclosed by its owner, for example over social media, poses neither an objective nor a subjective risk of

[9] *Ibid*.
[10] *Ibid*., at 225.
[11] *Ibid*.
[12] *Ibid*.

harm to the individual but provides the company with access to and use of the information it requires to respond to an Industry Challenge. Indeed, the blanket protection of Personal Information PPIPS and PIPEDA provide seems unjustifiable in an era of social media when individuals are at liberty to, and do, share varying degrees of intimate information with 400 of their "closest" friends. Does this shared information, for all intents and purposes, not become public? And if so, why should employers be prevented from using it - especially if it poses little or no risk of harm to the individual?

The following three examples, all involving social media, illustrate how PPIPS and PIPEDA are overly restrictive on the information businesses seek to collect, use, and communicate without in fact offering protection to individuals who have chosen to disclose the information.

4.2.1.1 Facebook

Although employers are discouraged from scouring Facebook accounts to collect information on their employees, this same information, depending on the Facebook account settings, may be admissible evidence in the context of a trial. In fact, in *Campeau et Services alimentaires Delta Dailyfood Canada*, Québec's Commission des Lésions Professionnelles states that this evidence "si elle a été obtenue légalement, ne constitue pas une atteinte à la vie privée. Facebook fait partie de la vie publique et ceci même si la personne a mis des paramètres privés pour la protéger".[13] If a subject has chosen to share

[13] 2012 QCCLP 7666 at para. 37.

information with what in the court's eyes, constitutes the public, why should this information not be considered Public Information (as defined in Chapter 3) for the purposes of PPIPS and PIPEDA?

4.2.1.2 LinkedIn

An even greater incongruity exists with respect to LinkedIn since the subject is allowed to use their job title and their employer's name to market themselves but the employer must obtain consent before using the same information to market its goods or services. LinkedIn usually provides preliminary information such as a subject's photo, their professional title, the company that employs them and often their education to people who are not even "linked" to the subject in question. The photo, in and of itself, usually testifies to the gender – male or female[14] -, frequently to ethnicity and sometimes to religious affiliation in the cases of religions that adhere to certain dress codes. If this information is readily accessible to anyone who types a name into a search engine, has it not acquired a public character?

4.2.1.3 Blogging

Finally, what about the information a blogger shares when blogging on matters deemed private? Should a person who blogs or publishes regularly about matters concerning aspects of their biographical core of information have the right to pursue their employer for collecting, using or communicating this information? Certainly this was the argument invoked by Lacoursière J. in

[14] Homosexual, transgender and bi-sexual may not be as easy to ascertain.

Blanc v. *Éditions Bang Bang* to reject the plaintiff's claim that the photo she used to identify her blog had been reproduced without her consent by another editor thereby violating her right to her image.[15] The court held that as the photo that had been used was the one that appeared on her blog as well as on her Facebook and Twitter accounts, it belonged to the public domain.

The three examples above illustrate deliberate decisions on the part of the subject to render certain items of their Personal Information public. Applying Gratton's risk of harm test to this information suggests that the potential harm from the collection and disclosure of information is non-existent as the individual provided the information. Likewise, the potential objective harm stemming from its use by the employer is difficult to conceive as the latter would be using it to help end discrimination. As an aside, it is interesting to note the similarities between the case of information made publicly available by the individual and the test used to establish abandonment in criminal cases involving s. 8 of the *Canadian Charter of Rights and Freedoms*[16]. This test also involves balancing objective and subjective criteria to determine whether a reasonable expectation of privacy existed and if so, whether it was violated by law enforcement officials.[17]

---

[15] [2011] QCCS 2624.

[16] *Constitution Act*, 1982 R.S.C., 1985, App.II, no 44. ("**Canadian Charter**").

[17] As discussed in Chapter 3, in *R.* v. *Tessling* [2004] 3 S.C.R. 431, and then again in *R.* v. *Patrick* [2009] 1 S.C.R. 579 ("**Patrick**"), the Supreme Court elaborated a two-step test that seeks to establish first, whether the subject has a reasonable expectation of privacy – from both a subjective and objective perspective - and second, if such is the case, whether it was it violated. This test can be easily adapted to instances involving potential breaches of informational privacy to become:

1. Did the subject have a reasonable expectation of privacy?

A more certain approach might be to amend PPIPS and PIPEDA so that the category of "data made public by the individual" is included in section 1 of the former or subsections 7(1); 7(2) and 7(3) of the latter. Such an amendment would not be out of keeping with other data protection regimes such as art. 8(2)(e) of EU Directive 95/46/EC that specifically exempts from the prohibition against the processing of certain types of sensitive data "data which are manifestly made public by the data subject".[18]

4.2.2 Employee Data Necessary for the Operation of an Enterprise

A second category of data that should be excluded from the definition of Personal Information is information necessary for the proper operation of an enterprise. This could be accomplished by adopting a purposive understanding

---

A. What is the subject matter of the information collected / used / communicated?
B. Did the subject have a direct interest in the contents?
C. Did the subject have a subjective expectation of privacy in the information collected / used / communicated?
D. If so, was the expectation objectively reasonable considering the following:
    a. Place where the collection / use / communication occurred? Was there a trespass involved?
    b. Was the informational content of the subject matter in public view?
    c. Whether the information content of the subject matter had been abandoned?
    d. Whether such information was already in the hands of third parties; if so, was it subject to an obligation of confidentiality?
    e. Whether the organization's technique was intrusive in relation to the privacy interest.
    f. Whether the use of surveillance technology / evidence gathering technique was itself objectively unreasonable.
    g. Whether the informational content exposed any intimate details of the subject's lifestyle, or information of a biographical nature.

2. If a reasonable expectation of privacy existed, was it violated?

When the above test is applied to the three social media examples, a conclusion similar to the one reached when applying Gratton's analysis can be drawn. Indeed, it appears that while a subjective expectation of privacy may well exist, the subject's behaviour negates any possible objective expectation thereby rendering the information public.

[18] Directive 95/46/EC *on the protection of individuals with regard to the processing of personal data and of the free movement of such data*, http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.

of "necessary" in s. 5 of PPIPS or even broadening the meaning of PIPEDA's s. 4.01: "in relation to their employment, business or profession"[19]. This interpretation is not out of keeping with a certain branch of jurisprudence on the information a Quebec employer is allowed to collect. PIPPS limits employers to collecting only information that is "necessary for the object of the file". Lukasz Granosik, in his review of case law on the concept of "necessary" in the privacy context, concludes that Quebec case law remains divided between a narrow, literal reading of the word "necessary" and a much broader interpretation in which a test similar to the Oakes test has been applied.[20] Among the cases in this second category is that of *Dubé* c. *Le Secretariat de L'action catholique de Joliette* in which the tribunal, in assessing what information was necessary to collect in an employment context, listed three items: 1. the fulfilment of the employee's duties; 2. the functioning of the enterprise; and 3. the performance of the employment contract.[21]

Although the risk of subjective harm from disclosure of data necessary for the operation of an enterprise may be greater than with information deliberately made available by the individual, this risk can be reduced to render the possibility of its occurrence negligible. An employer can protect against the harm linked to disclosure by ensuring the information, when legitimately disclosed, is disclosed in such a way as to render its owner non-identifiable. It

[19] This section was added in 2015 along with the definition of "business contact information" in s. 2

[20] Granosik, Lukasz, "Le critère de nécessité: son évolution, son importance, son impact et son application», *Les 20 ans de la Loi sur la protection des renseignements personnels dans le secteur privé* (2014), Cowansville : Y. Blais, 2014.

[21] 2004 CanLII 73641 (QC SAT) at 64.

can also ensure that it has sufficiently solid data protection mechanisms in place to reduce the risk of a leak or illegitimate disclosure. With respect to the use of this information, the risk seems inconceivable as the reason for which the information is used is to combat discrimination against individuals to whom the information pertains.

An alternative to a purposive interpretation of "necessary" or "in relation to their employment, business of profession" that would avoid the potential for legal uncertainty, cited by Gratton as one of the two limits of the purposive approach,[22] would be to amend PPIPS and PIPEDA to include a limited-use employee information collection provision enabling employers to collect, use, and communicate information that is necessary for the operation of the employer's enterprise. Such a change could be made by adopting a section similar to Alberta's *Personal Information Protection Act*, s.15(1)[23] and adding a subsection 15(1)(a)(iii) that would read "ensuring the proper functioning of the enterprise". This amendment goes slightly beyond Gratton's recommendation

[22] The other being the lack of a balance test to weigh competing values. *Supra* note 3 at 159.

[23] S.A. Chapter P-6-5 ("**Alberta PIPA**"). Alberta PIPA's employee collection provision goes further than British Columbia's Personal Information Protection Act, SBC 2003 Chapter 23 ("**BC PIPA**") or PIPEDA. Section 15(1) reads:

An organization may collect personal employee information about an individual without the consent of the individual if

(a) the information is collected solely for the purposes of

(i) establishing, managing or terminating an employment or volunteer-work relationship, or

(ii) managing a post-employment or post-volunteer-work relationship

(b) it is reasonable to collect the information for the particular purpose for which it is being collected, and

(c) in the case of an individual who is a current employee of the organization, the organization has, before collecting the information, provided the individual with reasonable notification that personal employee information about the individual is going to be collected and of the purposes for which the information is going to be collected.

to the Commission d'accès à l'information that PPIPS should be brought in line with PIPEDA, Alberta PIPA and BC PIPA by enabling an employer to collect employee information to better manage the employee provided the employer notifies the latter of the type of information it may collect, how the information will be used and that both the collection and notice are reasonable.[24]

4.2.3 Data Required by Programs Intended to Remedy Social Inequalities

A third exclusion to the definition of Personal Information in PPIPS and PIPEDA that would enable businesses to participate in Industry Challenges would be information required by programs intended to remedy social inequalities. Again, in an employment context, such exclusion would not run counter to Quebec law. Although the type of information required for the purposes of an Industry Challenge are protected by s. 10 of the Quebec Charter of Rights and Freedoms.[25] Section 18.1 of the Quebec Charter states that:

> "[n]o one may, in an employment application form or employment interview, require a person to give information regarding any ground mentioned in section 10 unless the information is useful for the application of section 20 or the implementation of an affirmative action program in existence at the time of the application."[26]

Section 20 states that:

---

[24] Gratton, Eloise, "Updating Quebec Private Sector Privacy Law – Part 2 of 2" http://www.eloisegratton.com/blog/2015/12/11/updating-quebec-private-sector-privacy-law-part-2-of-2/

[25] Every person has a right to full and equal recognition and exercise of his human rights and freedoms, without distinction, exclusion or preference based on race, colour, sex, pregnancy, sexual orientation, civil status, age except as provided by law, religion, political convictions, language, ethnic or national origin, social condition, a handicap or the use of any means to palliate a handicap", *Quebec Charter of Human rights and Freedoms*, CQLR, c. C-12 ("**Quebec Charter**").

[26] *Ibid*.

> "[a] distinction, exclusion or preference based on the aptitudes or qualifications required for an employment, or justified by the charitable, philanthropic, religious, political or educational nature of a non-profit institution or of an institution devoted exclusively to the well-being of an ethnic group, is deemed non-discriminatory."[27]

The right of an employer to collect such information was confirmed in *X* c. *Residence l'Oasis Fort Saint-Louis* in which the plaintiff complained that the type of information that was asked of her in an employment interview was excessive.[28]

Similar to data necessary for the operation of an enterprise, the risk of subjective harm from disclosure of information required by a program intended to remedy social inequalities, while real, may be mitigated through the same type of measures as above: anonymized disclosure and solid data protection mechanisms. As with the other two categories of information, the potential for objective harm appears minimal since the intended use of the information is to end discrimination.

Again, like with information necessary for the operation of an enterprise, to avoid uncertainty, PPIPS and PIPEDA might be better amended to exclude from protection, information required by programs intended to remedy social inequality. This information would form an exception similar to the exceptions for information collected, used, and communicated for journalistic, scholarly or research purposes. Interestingly, BC PIPA, in sections 12(f), 15(f), and 18(f),[29] and Alberta PIPA, in sections 14 (f), 17 (f), and 20(l),[30] allow for the collection, use, and communication of personal information without the individual's consent to determine their suitability "to

[27] *Ibid*.
[28] [1995] no AZ-95151507 (C.A.I).
[29] *Supra* note 23.
[30] *Supra* note 22.

receive an honour, award or similar benefit". Presuming the type of data required for the honor or award may be much the same as the information required to respond to an Industry Challenge, it is not inconceivable that PPIPS and PIPEDA should include an exception for data required by a program intended to remedy social inequalities.

****

A purposive approach to the interpretation of PPIPS and PIPEDA grounded in a risk assessment of the harm to individuals in the event of a breach, is helpful in understanding what amendments, interpretative as well as legislative, could be made to PPIPS and PIPEDA to enable greater flexibility with respect to the Personal Information a business can collect, use, and disclose in the context of an Industry Challenge without noticeably increasing the risk of harm to the individual. These changes, among others, could include interpreting Personal Information to exclude data made publicly available by the individual, employee data necessary for the operation of an enterprise, and data required by programs intended to remedy social inequalities.

The advantage of purposefully interpreting Quebec's private sector privacy legislation is the leeway it provides a company to exercise its right to express itself in response to ever changing market demands. One of its drawbacks, however, remains the potential for legal uncertainty. Certainty, however, may only be achievable through legislative change and perhaps, as discussed in the next chapter, through judicial review.

Chapter 5.
Challenging Quebec's Private Sector Privacy Legislation

The fact that, in Canada, rights are not absolute is clearly set out in s.1 of the *Canadian Charter of Rights and Freedoms* that states: "[t]he *Canadian Charter of Rights and Freedoms* guarantees the rights and freedoms set out in it subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society".[1] Privacy, therefore, frequently requires balancing against other competing rights and interests. As discussed in the Introduction, this was reiterated in 2013 by the Supreme Court of Canada ("**Supreme Court**"), in *Alberta (Information and Privacy Commissioner)* v. *United Food and Commercial Workers, Local 401*[2], that held Alberta's *Personal Information Protection Act*[3] to be unconstitutional for violating a union's right to express itself as per s. 2(b) of the Canadian Charter. The U.F.C.W. decision is particularly interesting as it provides some indication of the approach a court might take in interpreting a conflict between the right to privacy and a company's use of workforce demographics to market itself – in so far as this practice constitutes a form of commercial expression.

In light of the U.F.C.W. decision then, this chapter considers the possible Canadian Charter challenges a company could bring against *An Act Respecting the Protection of Personal Information in the Private Sector*[4] and the *Personal Information Protection and Electronic Documents Act*[5] in the event the enforcement of this legislation

---

[1] *Constitution Act*, 1982 R.S.C., 1985, App.II, no 44 ("**Canadian Charter**").
[2] [2013] 3 S.C.R. 733 ("**U.F.C.W.**").
[3] S.A. 2003, Chapter P-6.5 ("**Alberta PIPA**").
[4] Chapter P-39.1 ("**PPIPS**")
[5] S.C. 2000 c. 5 ("**PIPEDA**").

prevented the company from responding to an Industry Challenge (as defined in Chapter 4). In essence, this chapter sets out the arguments a company might invoke were it to be pursued for having violated PPIPS and / or PIPEDA in responding to an Industry Challenge. If, as described in the Introduction, Industry Challenges are a form of commercial expression, a company defending against a privacy violation claim could argue, much as the union did in U.F.C.W. that, as drafted, existing privacy legislation violates its right to express itself under s. 2(b) of the Canadian Charter.

The pages that follow begin by presenting the reasoning adopted by courts in instances of judicial review. They then apply this reasoning to a hypothetical challenge of PPIPS and PIPEDA. While it could be argued that both these laws violate a company's right to express itself commercially, their vulnerability in the instance of a judicial review is not the same. Although a court would probably hold PPIPS' and PIPEDA's respective objectives to be justifiable, in the case of PIPEDA, the methods used to meet these objectives appear to cause more than a minimal impairment to an organisation. In the case of both PPIPS and PIPEDA, the objectives are disproportionate to the benefits the laws purport to confer.

5.1 Judicial Review

A constitutional challenge to any law requires a two-part analysis in which the court must first, determine whether the law in question breaches a Canadian Charter right and second, whether such breach is justifiable in a free and democratic society.

5.1.1 Proving the Violation

To prove a violation, the plaintiff must demonstrate, according to civil standards, that

the law violates a right protected by the Canadian Charter.[6] Once this is accomplished, the burden of proof shifts to the legislator to justify its law.[7] Peter Hogg notes that in assessing whether a right has been violated, it is essential to define the right as one that is worth protecting. He states that "[e]ach right should be so interpreted as not to reach behaviour that is outside the purpose of the right – behaviour that is not worthy of constitutional protection".[8] A purposive rather than a generous interpretation is, therefore, preferable.

5.1.2 Justifying the Violation: the Oakes Test

The second step in the judicial review of legislation is set out in the case of *R.* v. *Oakes* in which the Supreme Court, to determine whether the law in question was justifiable in a free and democratic society, examined two issues: 1. whether "the objective which the measures responsible for a limit on a Charter right or freedom are designed to serve, [were] of 'sufficient importance to warrant overriding a constitutionally protected right or freedom"; and 2. once the sufficiently significant objective was recognized, whether "the means chosen [were] reasonable and demonstrably justified".[9] To determine whether the means chosen were reasonable, the court examined three further questions: 1. whether "measures adopted [were] carefully designed to achieve the objective in question"; 2. whether the means "impair[ed], 'as little as possible' the right or freedom in question and; 3. whether there was a "proportionality between the effects of the measures which [were] responsible

[6] Hogg, Peter, *Constitutional Law of Canada*, 5th ed., vol. 2 Toronto: Carswell, 2014 at 38-8.
[7] *Ibid*., at 38-7.
[8] *Ibid*., at 38-6.
[9] [1986] S.C.R. 103 at 138-139 ("**Oakes**").

for limiting the Charter right or freedom, and the objective which [had] been identified as of 'sufficient importance'".[10] Hogg summarises the effects of the Oakes test as follows:

> "it is step 3 – least drastic means – that is the centre of the inquiry into s. 1 justification. Only in a rare case will a court reject the legislative judgement that the objective of the law is sufficiently important to justify limiting a Charter right (step 1). It is an even rarer case where the law is not rationally connected to the objective (step 2). And the inquiry into disproportionate effect (step 4) is normally, if not always, precluded by the judgement that the law's objective is sufficiently important to justify the impact on the Charter right (step 1)."[11]

Each of these steps, however, warrants greater explanation.

5.1.2.1 Sufficiently Important Objective

Although rare that a court will invalidate a law because of its objective, the definition of this objective is essential to determining the direction the judicial review will take. Hogg explains that the higher the level of generality at which the legislative objective is framed, the more desirable the objective will appear.[12] The review of a law with broadly framed objectives will thus focus on the second part of the Oakes analysis, that is to say, the proportionality and the means used to accomplish the objectives.[13] If, on the other hand, the objectives are narrowly defined, it will be difficult to conceive of alternative and less onerous means of fulfilling these.[14] Hogg concludes that "[t]he statement of the objective should therefore be related to the infringement of the Charter, rather than to other goals. In other words, the statement of the objective

---

[10] *Ibid*.
[11] *Supra* note 6 at 38-18.
[12] *Ibid*., at 38-19.
[13] *Ibid*.
[14] *Ibid*.

should supply a reason for infringing the Charter right".[15] He also explains that the objectives of a law cannot be justified under s.1 if they are incompatible with the values embodied in the Canadian Charter or if they are *ultra vires* the enacting legislative body on federal distribution of power grounds.[16] Likewise, the objective of the legislation cannot shift over time to reflect changing social conditions.[17] This last restriction may prove increasingly fatal to PPIPS and PEPIDA that reflect concerns of the third wave of privacy protection, described in the Introduction, but that are becoming ill-adapted to privacy concerns of the fourth wave.

5.1.2.2 Rational Connection

In analysing the rational connection, the court must determine whether the law, as it is drafted, fulfils the objectives it set out to accomplish. In *R*. v. *Edwards Books and Art*, the court explained that "[t]he requirement of rational connection calls for an assessment of how well the legislative garment has been tailored to suit its purpose".[18] Ironically, Oakes is an example in which the law was struck down on the rational connection test as the court found that there was no rational connection between possession of a narcotic and the intent to traffic.

5.1.2.3 Minimum Impairment

Referred to by Hogg as the "heart and soul of s. 1 justification", the minimum impairment analysis seeks to establish whether the law under review pursues its

[15] *Ibid*., at 38-20.
[16] *Ibid.*, at 38-26.
[17] *Ibid.*
[18] [1986] 2 S.C.R. 713, at 770.

objective by the least drastic means possible. [19] In so doing, however, it will allow the legislator a margin of appreciation, especially when the following matters are involved: protection of a vulnerable group (such as children), complex social-science evidence necessary to make the case; complex social issues; competing interest groups, and allocation of scarce resources.[20] As a result, Hogg argues, the jurisprudence on this second step tends to be unpredictable.[21]

5.1.2.4 Proportionate Effect

The third and final step of the second part of the Oakes test has not been used to invalidate legislation in Canada. Although Hogg explains this by qualifying it as redundant,[22] the step merits some scrutiny as it might indeed prove relevant to a judicial review of PPIPS and PIPEDA. The proportionate effect step assesses whether the law, despite the rational connection between its objective and means, and regardless of having used the least drastic means possible, is still too high a price for violating a right protected by the Canadian Charter. The value of this last step is well described by Aharon Barak who explains that "[p]roportionality examines the relationship between the object and the means of reaching it".[23] He argues that in certain circumstances advancing the general interest might not justify the limitation to the human right.[24] Consequently, according to Barak:

---

[19] *Supra* note 6 at 38-36.
[20] *Ibid*., at 38-43.
[21] *Ibid*.
[22] *Ibid*., at 38-44.
[23] "Proportionality Effect: The Israeli Experience", (2007), 57 *University of Toronto Law Journal* 369, at 371.
[24] *Ibid*.

> "[t]his test examines the proper correlation between the benefit stemming from attainment of the proper object and the extent of its effect upon the constitutional right. It focuses upon the results of the statute. It examines the proper ratio between the benefit stemming from attainment of the object and the deleterious effect upon the human right. Whereas the rational connection test and the least harmful measure test are essentially determined against the background of the proper objective, and are derived from the need to realize it, the test of proportionality (*stricto sensu*) examines whether the realization of this proper objective is commensurate with the deleterious effect upon the human right. It is a principle of balancing. It requires placing colliding values and interests side by side and balancing them according to their weight."[25]

This last paragraph also appears in Chief Justice McLachlin's majority decision in *Alberta* v. *Hutterian Brethren of Wilson Colony*.[26] Chief Justice McLachlin explains that "[t]he final stage of Oakes allows for a broader assessment of whether the benefits of the impugned law are worth the cost of the rights limitation".[27] In other words "are the overall effects of the law on the claimant disproportionate to the government's objectives".[28] In order to assess this, McLachlin sets out a three-step analysis to determine: 1. the salutary effects of the law; 2. its deleterious effects; and 3. the outcome once these are weighed against each other.[29] Each of these steps will be applied below to review the constitutionality of PPIPS and PIPEDA.

5.2 Judicially Reviewing PPIPS and PIPEDA

While the success of a challenge to PPIPS' and PIPEDA's objectives would appear slim, as it requires convincing a court that the fourth wave of privacy challenges that now affect us has rendered legislation developed during the third wave irrelevant, in

---

[25] *Ibid*., at *374*.

[26] [2009] 2 S.C.R. 567 at 606-7 ("**Hutterian Brethren**").

[27] *Ibid*. at 605.

[28] *Ibid*. at 604.

[29] *Ibid*. at pp. 607-615.

the case of an Industry Challenge, the means used by PIPEDA to realise its objectives present more than a minimal impairment of an organisation's right. Serious consideration should also be given to the disproportionate effect PPIPS and PIPEDA have on an organization's freedom to express itself commercially.

5.2.1 Violation of the Right to Commercial Expression

In the same way the United Food and Commercial Workers Local 401, in U.F.C.W., challenged Alberta PIPA by arguing that it violated the union's right to express itself, an organisation could challenge PPIPS and PIPEDA for impeding its right to respond to an Industry Challenge and, by extension, to express itself commercially. Since the Introduction and Chapter 3 describe how Industry Challenges are a form of commercial expression and the ways in which PPIPS and PIPEDA prevent companies from effectively responding to these Challenges, the paragraphs that follow will not revisit these arguments. They will start from the premise that Quebec's private sector privacy legislation violates a company's right to express itself commercially and proceed directly to an analysis of this violation according to the Oakes test.

5.2.2 Privacy: A Sufficiently Important Objective

Challenging PPIPS' and PIPEDA's objectives may not prove the most successful tactic as its depends on an acknowledgement, of which there is little evidence to date, that legislation developed during the third wave of privacy concerns is not adapted to address those of the fourth wave. At present, although slightly different, PPIPS' and PIPEDA's objectives, in that they intend to provide the individual with control over

their information and to implement fair information practices ("**FIP**"s), are unlikely to be judged insufficiently important to justify their respective legislation. To reiterate what was discussed in Chapter 3, PPIPS' express objective is to establish rules regarding the collection, use, and communication of information that respect the rights set out in articles 35 to 40 of the *Civil Code of Quebec*[30]. PIPEDA, however, seeks to regulate the collection, use, and communication of this same information but in such a way as to respect the privacy right of the individual and the needs of organizations. While PPIPS' and PIPEDA's slightly differing objectives will influence a challenge to these respective laws, they are unlikely to be considered sufficiently un-important to justify striking down either piece of legislation at this step of the judicial review.

The only conceivable justification for a court to find PPIPS' and PIPEDA's objectives to be unimportant would be if the court were to find them no longer relevant. Such an argument would require demonstrating that the control over personal information model upon which both laws are based is, as Gratton argues, increasingly ineffective in an age of every increasing volumes of technology, new types of information collection tools, new identifying methods, new uses of information and increased availability of data.[31] While threats to privacy may be shifting, the threats that characterise the third wave have yet to disappear. PPIPS and PIPEDA therefore remain relevant.

[30] S.Q. 1991, c.64.

[31] Gratton, Eloise, *Understanding Personal Information: Managing Privacy Risks*, Markham, ON, Lexis Nexis Canada Inc., 2013 at 21-56.

Moreover, the cases that are frequently cited as authoritative in matters concerning privacy, display reasoning typical of the third privacy wave. In *R*. v. *Dyment*, LaForest J. refers to Alan Westin to acknowledge that "[g]rounded in man's physical and moral autonomy, privacy is essential for the well-being of the individual".[32] Similar links among privacy, dignity, and autonomy can be found in civil cases such as *Godbout* v. *Longueil*[33] or *Aubry* v. *Les Éditions Vice-Versa Inc*[34]. Even the U.F.C.W. case provides a striking example of the courts' defense of privacy as control over personal information.[35] At this stage the courts appear unlikely to view PPIPS' and PIPEDA's objectives as un-important.

5.2.3 Rational Connection

So long as individual control of personal information is recognised as a sufficiently important objective, PPIPS and PIPEDA will probably not be found unconstitutional for lack of a rational connection between their objectives and the legislative measures proposed to achieve them. This is hardly surprising as both their provisions reflect the FIPs that developed internationally during the third wave of privacy protection and seem to be generally accepted as adequate. PPIPS' sole objective of allowing

---

[32] [1988] 2. S.C.R. 417 at 427.

[33] [1997] 3 S.C.R. 844 at para. 65.

[34] [1998] 1 S.C.R, 591.

[35] The court justifies the quasi-constitutional status it attributes to Alberta PIPA by pointing to the legislation's purpose as providing individuals with some measure of control over their personal information, control that is intimately connected to personal autonomy, dignity, and privacy. The Supreme Court explains that "PIPA's objective is increasingly significant in the modern context, where new technologies give organizations an almost unlimited capacity to collect personal information, analyse it, use it and communicate it to others for their own purposes". It identifies the three objectives the law seeks to advance as those of: 1. enabling the individual control over their personal information by "restricting who can collect, use and disclose personal information without the individual's consent and the scope of such collection, use and disclosure"; 2. avoiding potential harm flowing from "permanent storage or unlimited dissemination of personal information through the Internet or other forms of technology without an individual's consent"; and 3. reinforcing social values of individual autonomy, dignity and privacy by providing them with some measure of control over their personal information. *Supra* note 2 at 747-749.

individuals to determine how their information will be collected, used, and communicated with very little left to the discretion of the organisation, except the initial collection that is subject to the requirement that the information be necessary[36], places the control of personal information almost exclusively in the hands of the person to whom the information relates. The legislation imposes a necessity based collection provision for initial collection of information and subjects subsequent and different uses and communication to the individual's consent. It provides mechanisms whereby an individual can have access to and correct any inaccurate information.

Likewise, PIPEDA, the objective of which is to balance the competing rights of the individual to control the collection, use, and communication of personal information against those of the organisation with respect to the same information, appears drafted to at least attempt to reconcile these somewhat divergent interests. PIPEDA's tone is more suggestive than coercive and the Principles it seeks to impose are based on the Canadian Standards Association Model Code that is drafted for industry. They reflect standard FIPs requiring consent for the collection, use, and communication of information and providing the individual with mechanisms to verify and correct inaccurate information as explained in Chapter 3.

PIPEDA differs from PPIPS, however, on the matter of consent. While the individual's consent is required for the collection, use, and communication of personal information, the explicitness of this consent may vary depending upon the sensitivity of the information involved. Collection is also subject to a reasonableness standard

[36] *Supra* note 4 at s.5.

that Lawson and O'Donoghue argue leads to an "uneasy 'balancing test'" between the rights of the organisation and those of the individual.[37] It is this uneasy balance that contributes to PIPEDA's vulnerability in the event of judicial review.

5.2.4 PIPEDA and Minimal Impairment

In contrast to PPIPS' singular and narrowly defined objective that certainly protects it from charges of unnecessary impairment[38], the balance PIPEDA's objective purports to maintain between the seemingly competing interest of the individual, who wishes to retain control over their personal information, and the organisation, that seeks to use it, especially in the context of an Industry Challenge, renders the law vulnerable to judicial challenge on the grounds of impairment. The importance of this equilibrium is frequently referred to by the courts in cases such as *Englander* v. *Telus Communication* in which the Federal Court of Appeal explains that:

> "even though Part I and Schedule I of the Act purport to protect the right of privacy, they also purport to facilitate the collection, use and disclosure of personal information by the private sector. In interpreting this legislation, the Court must strike a balance between two competing interests. […]"[39].

In light of the Supreme Court's tendency to find reasonable solutions to cases involving conflicting rights – as discussed in Chapter 3 - and of its finding in U.F.C.W. that "[t]he price PIPA exacts, […], is disproportionate to the benefits it promotes"[40], an organization would be justified in requesting a judicial review of PIPEDA. The

---

[37] Lawson, Philippa and O'Donoghue, Mary, "Approaches to Consent in Canadian Data Protection Law", in Kerr, Lucock and Steeves, eds. *On the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, Oxford: UP, 2009, 23-42 at 33.

[38] It is difficult to conceive of a less restrictive means of giving the individual absolute control over the information an enterprise collects, uses, and communicates on them than by requiring prior consent to all these activities.

[39] 2004 FCA 387 (CanLII) para. 46.

[40] *Supra* note 2 at 749.

organization should argue that with respect to Industry Challenges, the law disproportionately impairs its right to commercially express itself. It should demonstrate that while employee consent to the collection, use, and communication of his or her information may correspond to the control of personal information model upon which PIPEDA is based, in an employment setting, it is excessive given the damper it places on the employer's ability to promote its goods or services. As previously discussed, conveying information on workforce demographics to a marketplace that is increasingly concerned with the social engagement of its vendors – notably its promotion of Target Groups (as defined in the Introduction) - is essential for a business to remain competitive.

PIPEDA's impairment of an organisation appears all the more disproportionate when compared to the risk of either subjective or objective harm to the individual. The way information is communicated in response to an Industry Challenge, while precise, does not render the individual identifiable *per se*. A person who wishes, for example, to keep their sexuality secret will be little more exposed by disclosing this information to a Human Resources representative who is bound to keep the information confidential and only to use it in responding to an Industry Challenge, than if they said nothing at all. This employee will simply be added to the others who come forward as belonging to the same Target Group. A person who wishes to keep their sexuality confidential is not automatically "outed" because he or she happens to be one of 5 LGBT[41] employees disclosed by the organization. An opposite case might be made in instances in which an employee's biography is forwarded to justify their inclusion in a

[41] Lesbian, Gay, Bisexual, Transgender.

client team. In that a biography contains a name and is transmitted to correspond to a category required by the client, it is clearly more sensitive – especially in instances in which a photograph is included or a category that is not outwardly visible is in question such as one's sexuality.

Likewise, why should an organization be prevented from repurposing personal information about its employees that these employees have made public through a blog, a Facebook posting or a photo on LinkedIn? Would using this information not, in essence, be similar to the union's use of photos of its members in public places in U.C.F.W.? The court found the location in which the photos were taken militated against any argument that what was being captured was purely personal information because the photograph could have been taken and used by any news media for journalistic purposes.[42] It is unclear what PIPEDA is protecting by forbidding organizations from repurposing information which individuals have deliberately made public to respond to an Industry Challenge.

The organization might also argue that the fact that, as discussed in the previous chapter, three amendments could be made to PIPEDA, to recognise the needs of the organisations to collect, use, and communicate personal information without for as much increasing the risk to the individual that this information will be misused, creates more than minimal impairment. To recap, these amendments are: 1. data that has been deliberately made public by the individual should be considered Public Information; 2. an employee information collection, use, and communication principle

[42] *Ibid*.

should be included in PIPEDA to allow employers to collect information that is necessary to the operation of the enterprise; and 3. PIPEDA should exempt activity related to the remedying of social inequality from activity included within the scope of its application.

5.2.5 PPIPS, PIPEDA and Proportionality

While it would appear difficult to challenge PPIPS for an insufficiently important objective, a lack of rational connection or minimum impairment, the legislation is certainly worthy of scrutiny, as is PIPEDA, for the disproportionate harm they cause organisations and potentially the communities in which they operate. An analysis of these laws according to the steps set out in Hutterian Brethren reveals that in the context of an Industry Challenge, the restrictions Quebec private sector privacy legislation places on an organisation's ability to express itself commercially, arguably outweigh the risk of harm suffered by the employee in the event their personal information is handled in violation of existing privacy legislation. Indeed, a strict application of PPIPS and PIPEDA could deprive the public of information it requires to make informed decisions, potentially limit the competitiveness of Quebec business abroad, and discourage private sector engagement in affirmative action programs.

5.2.5.1 Salutary Effect

The transition from a third to a fourth wave of privacy concerns arguably diminishes PPIPS' and PIPEDA's salutary effects, without for as much rendering it obsolete. Although these laws may protect individuals against a risk of harm triggered by organisations collecting, using, and disclosing their personal information, this harm

may not be the greatest threat to privacy. In fact, the dignity, autonomy, and self-worth associated with privacy are perhaps now threatened, as Gratton points out, by new information collection tools, new identifying methods, new uses of information, and increased availability of data, all of which render the possibility of control illusory and challenge what it means to identify an individual.[43] So while laws that still focus on enabling an individual to control their personal information may have some salutary effect, this effect is greatly diminished given that the ill it was intended to remedy is changing. Their deleterious effects, however, are substantial.

5.2.5.2 Deleterious Effect

Many deleterious effects stem from preventing an organization from expressing itself commercially. Most notably, it prevents individuals from making "informed economic choices, an important aspect of individual self-fulfilment and personal autonomy".[44] By preventing an organization from collecting, using, and communicating information on its workforce demographics, PPIPS and PIPEDA prevent a company from acquiring and disclosing details about its goods and services that are becoming increasingly important to consumers. As discussed in the Introduction, as consumer activism increases, the type of information that is required to respond to Industry Challenges is as vital to consumers as price and quality in shaping their choice. Preventing a company from communicating this is not only a violation of its freedom of expression, it is, perhaps more importantly, depriving the public of their right to know what they are purchasing and from whom they are purchasing it.

---

[43] *Supra* note 31.

[44] *Ford* v. *Quebec,* [1988] 2 S.C.R. 712 at 767.

A secondary consideration, but one that merits exploring, is the rendering of Quebec businesses less competitive than their American counterparts. Although neither the Canadian Charter nor the Quebec *Charter of Human Rights and Freedoms*[45] protects economic rights, it is nevertheless important, when weighing PPIPS' and PIPEDA's deleterious effects, to note their potential to weaken the economic competitiveness of Quebec businesses. If companies cannot respond to questions concerning their employees' personal information with the same degree of precision as that of their American counterparts, they risk losing contracts, laying off staff, and potentially closing down – all effects that are deleterious to the Quebec economy. It should be recalled that the legislator never intended Quebec privacy legislation to place a damper on business.[46]

A third consideration that is broadly linked to the impediment to commercial expression is discouraging industry from contributing to the rectification of social injustices by preventing it from participating and communicating its participation in affirmative action programs. Noting that "affirmative action arose in the United States in response to racial discrimination which was structurally ingrained, and could be ameliorated only through bold, systemic measures", Drumbl and Craig attempt to justify the awkward relationship the Canadian courts have had to interpreting the affirmative action provisions in the Canadian Charter.[47] They explain that problems "arise where the state intervenes directly in the allocation of social benefits, and

[45] CQLR, c. C-12.

[46] See the honourable L. Canon's remarks quoted at note 42 Chapter 3.

[47] Drumbl, Mark A. and Craig, John D.R., "Affirmative Action in Question: A Coherent Theory for Section 15(2)", Vol. IV, No.1 (1997) *Review of Constitutional Studies*, 80 at 86.

prescribes an allocation based on personal characteristics which are irrelevant to the issue of whether individuals want or need the social benefit".[48] If the State is perhaps not the appropriate organ to remedy these inequalities, then should the private sector not be given some flexibility to assist in rectifying structurally ingrained inequality? If so, then discouraging participation in Industry Challenges through laws like PPIPS and PIPEDA seems counterproductive.

In addition to being a form or marketing, responding to Industry Challenges and publishing workforce demographics on internet pages or promotional materials, fulfills a social justice function. It is a way for industry to inform the public about the lower than average participation of certain members of a Target Group in a given industry and the measures it is taking to help remedy this. It also serves to inform members of the Target Group that the company is a welcoming or "equal opportunity employer". It may challenge competing companies in the same sector to better their statics thereby using competition and the marketplace to affect social change. It may raise public awareness to the systematic discrimination encountered by members of a Target Group as well as help fight negative stereotyping of the group in question. Arguably, preventing an organisation from collecting, using, and communicating employee information to promote social change constitutes a deleterious effect that outweighs the salutary effects of PPIPS and PIPEDA.

5.2.5.3 Weighing the Salutary and the Deleterious Effects of PPIPS and PIPEDA

A weighing of the salutary and deleterious effects of PPIPS' and PIPEDA's

[48] *Ibid*., at 88.

impairment of a company's right to express itself commercially, especially within the context of an Industry Challenge, should encourage the legislator to reconsider the effect of these laws. While the ability to control one's Personal Information, and thereby retain some dignity and autonomy in the workplace, is important, as discussed in Chapter 4, a risk analysis of the real damage that might be caused to the employee in this context reveals a low potential for harm – especially given the security measures enumerated above that can be put in place to prevent a misuse of personal information. Continuing to prevent the repurposing and communication of this information, however, deprives the consumer of important information they require to make an informed choice about the goods or services they are purchasing, risks diminishing the competitiveness of Quebec business, and discourages the private sector from engaging in initiatives aimed at remedying social inequalities.

****

The U.F.C.W. case that forced change to Alberta PIPA and recognised a union's right to express itself, is a recent reminder that rights, even Canadian Charter protected ones, are not absolute but require balancing and defining according to what is reasonable in the circumstances. In light of this case, it is not inconceivable that an organisation challenge PPIPS and PIPEDA for preventing it from expressing itself commercially by restricting its ability to collect, use, and communicate Personal Information on employees without their consent in response to an Industry Challenge. Applying the analysis set out in Oakes, a company might argue that while PPIPS' and PIPEDA's objectives may still seem worthy and the legislation rationally connected to

these, the impairment PIPEDA inflicts is more than minimal. Additionally, in that both laws limit a form of commercial expression, and therefore risk depriving consumers of information necessary to make informed decisions, threatening the competitiveness of Quebec businesses, and discouraging private sector participation in affirmative action type programs, their overall impediment, in the case of an Industry Challenge, outweighs their benefit.

Chapter 6.
Conclusion: Pining Down Proteus

In *R*. v. *Tessling*, Binnie J describes privacy as a protean concept.[1] Jean-Louis Halpérin, referred to in the introduction to this essay, also believes privacy to be a concept best represented as a shifting border between many, often conflicting, interests.[2] The challenge in any given situation is to establish where the border should be drawn. The present essay uses the example of Industry Challenges (as defined in the Introduction) to explore where, in Quebec, the limit might be traced between a company's need to use workforce demographics to advertise its goods and services – a form of commercial expression - and its employees' right to keep Personal Information (as defined in Chapter 3) confidential. At present, the latter's rights are protected both provincially, by an *Act Respecting the Protection of Personal Information In the Private Sector*[3] and federally, by the *Personal Information Protection and Electronic Documents Act*[4].

This essay briefly reviews privacy protection in jurisdictions with the greatest legal influence on Quebec and Canada: the European Union, the United States and the United Kingdom (Chapter 2). It demonstrates how a blend of these influences is reflected in the Quebec and Canadian approaches to privacy and how existing privacy legislation might prevent a company from effectively and efficiently responding to Industry Challenges (Chapter 3). Finally, the last two chapters

---

[1] *R. v. Tessling,* [2004] 3 S.C.R. 431 at 445.

[2] Halpérin, Jean-Louis, "L'essor de la 'privacy' et l'usage des concepts juridiques", *Droit et Société* 61/2005, 765 at 775.

[3] Chapter P-39.1 ("**PPIPS**").

[4] S.C. 2000, c. 5 ("**PIPEDA**").

respectively explore the interpretive and legislative amendments that could be made to PPIPS and PIPEDA to enable companies to respond to Industry Challenges (Chapter 4) as well as the possible legal action a company could take on the ground that Quebec's privacy legislation violates its right to express itself commercially under s. 2(b) of the *Canadian Charter of Rights and Freedoms*[5] (Chapter 5). This study leads to the following concluding observations.

6.1 Growing Pains?

The evident tension between legislation such as PPIPS and PIPEDA and Industry Challenges may simply be a symptom of growing pains in the transition from the third to the fourth wave of privacy concerns and protection. While the third wave's concerns are still relevant, new market trends and demands, not to mention the technology and the new uses of information it generates, raise many new privacy questions characteristic of the fourth wave.

Responding to these requires more than ascertaining whether privacy is a right or a concept and, if a right, what type of right. These inquiries are ultimately sterile especially if as discussed in Chapters 2 and 3, in the United Kingdom, privacy may not be recognized as a right *per se* but still be protected, whereas in Canada, it may be recognized as a right but may have to cede or adapt itself to other equally important rights and societal concerns. Aharon Barak captures this subtlety and the judge's role in preserving it in what he terms the: "the constitutional dialectic", explaining that:

[5] *Constitution Act*, 1982 R.S.C., 1985, App.II, no 44..

> "human rights and the limitations on them derive from the same source. They reflect the same values. Human rights can be limited, but there are limits to the limitations. The role of the judge in a democracy is to preserve both of these limitations. Judges must ensure the security and existence of the state as well as the realization of human rights; they must determine and protect the integrity of the proper balance."[6]

Ultimately a less theoretical a more practical approach may be necessary.

6.2 A Pragmatic Approach

Until the transition from the third wave to the fourth is complete and the extent of the real privacy concerns characteristic of the fourth wave can be ascertained, at least in the case of Industry Challenges, existing tools can conceivably be leveraged to meet the needs of industry while respecting individual privacy. As suggested by Gratton in Chapter 4, a purposive interpretation of PPIPS and PIPEDA, grounded in a risk assessment of the actual harm suffered by an individual in the event of a breach, may be adapted to understand what amendments, interpretive as well as legislative, could be made to this legislation to provide business with the information it requires to respond to an Industry Challenge without noticeably increasing the risk of harm to the individual.

Another approach would be to leverage existing fair information practices ("**FIP**"s) differently to respond to the privacy concerns Industry Challenges present. This last point is made by Tene and Polonetsky albeit in response to privacy challenges posed by Big Data.[7] For example, if consent poses an obstacle to industry, perhaps the

[6] Barak, Aharon, "Proportionality Effect: The Israeli Experience", (2007), 57 University of Toronto Law Journal 369 at 382.

[7] Tene, Omer and Polonetsky, Jules, "Big Data for All: Privacy and User Control in the Age of Analytics, 11 *Northwestern Journal of Technology and Intellectual Property* (2013) at 3.

consent requirements could be reduced while ensuring the same or a better level of protection for the individual by emphasizing data integrity and enforcement.

A second approach suggested by Tene and Polonetsky would be to shift the focus of privacy legislation away from users to business.[8] Data protection would thus become a governance issue just like, and perhaps at par with, diversity and environmental sustainability. Tene and Polonetsky note that this approach:

> "signifies a paradigm shift from privacy law to data protection regulation, which, while concerned with privacy, has other goals, such as setting standards for the quality of personal information and ensuring that individuals and businesses are able to process information about others for various legitimate ends." [9]

They demonstrate how making privacy a governance issue is more effective than legislating by quoting a comparative study by Mullingan and Bamberger that proves how by making privacy a governance issue and appointing privacy officers, United States businesses "have seen privacy grow from the ground up, whereas European businesses often settle for privacy 'on the books'".[10] Moreover, there are advantages of working with existing tools.

[8] Tene, Omer and Polonetsky, Jules, "To Track or 'Do Not Track" Advancing Transparency and Individual Control in Online Behavioral Advertising", 2012, *Minnesota Journal of Law, Science & Technology*, Vol. 13.1. at 48.

[9] *Ibid*.

[10] *Ibid.*, at 49.

6.3 Advantages

At least two arguments militate in favor of working with existing tools. These are: 1. the global nature of the privacy challenge, and 2. the course already being charted by Canadian courts.

6.3.1 Privacy in a Global Context

The global presence of American companies in jurisdictions that, similar to Quebec, have strong privacy protection legislation, suggests that Quebec companies are not alone in dealing with local legislation that hinders their commercial interests. Charting a course that is starkly different for other jurisdictions will affect global integration. Indeed, since the data protection laws ("**DLP**"s) and FIPs that emerged around the world during the third wave of privacy protection are very similar and mutually integrated, a radical change in course through drastically new legislation would cause tremendous disruption. Gratton explains this disruption in reference to the definition of Personal Information by noting that providing for an interpretation instead of proposing a new wording of the definition may avoid having to completely reopen the 'control' conception of privacy, which is the basis of DPLs adopted all over the world."[11] She further argues that "[i]t is always less problematic to provide a solution that will be incorporated within the current legal framework […], such as a proposed interpretation, than to propose something completely new."[12] Although less certain than a legislative amendment, working with present tools will make efforts easier to coordinate internationally.

---

[11] Gratton, Eloise, *Understanding Personal Information: Managing Privacy Risks*, Markham, ON, Lexis Nexis Canada Inc., 2013 at 147.

[12] *Ibid*., at 152.

6.3.2 Jurisprudential Consistency

A second reason for not drastically changing existing privacy legislation and opting instead for a more informal means of protecting privacy is the flexibility it offers the courts to decide, case by case, where to erect the border between privacy and other interests. It is also in keeping with the course the courts have charted in decisions such as *Englander* v. *Telus Communication*.[13] In reference to the balance PIPEDA must maintain between the individual's right to privacy and the organisation's right to collect, use, and communicate Personal Information, the Federal Court advocates "flexibility, common sense and pragmatism"[14]. Likewise, in *Alberta (Information and Privacy Commissioner)* v. *United Food and Commercial Workers, Local 401* the Supreme Court of Canada chastises the legislator for a law that restricts a union's right to use Personal Information "without regard for the nature of the personal information, the purpose for which it is collected, used or disclosed, and the situational context for that information".[15] It would appear, therefore, that the courts have already adopted a purposive approach to weed out the aspects of PPIPS and PIPEDA that are perhaps dated or inappropriate in a given circumstance without calling for a complete overhaul of the privacy legislation in question.

****

To return, then, to the question posed at the beginning of this essay: "what is privacy?" perhaps the best answer is not a legal definition at all but rather an image.

[13] 2004 FCA 387 (CanLII).
[14] *Ibid*., at para. 46.
[15] [2013] 3. S.C.R. 733 at 749.

That image is the one used by Justice Binnie: the image of Proteus. As societies transition into the fourth wave, privacy resembles, more than ever the water god, who can foretell the future, but who will change shapes to avoid having to do so. Instead of trying in vain to pin it down, once and for all, privacy may be best left to define on a case by case basis and in consideration of the applicable legislation and jurisprudence. Although less certain than a legislative definition of the concept, judicial interpretation may prove the only mechanism sufficiently flexible to truly protect a concept like privacy that, while illusive, is not dead, and indeed fundamentally important to human, social, economic, and political development.

BIBLIOGRAPHY

Legislation

An Act Respecting the Protection of Personal Information In the Private Sector Chapter P-39.1.

Bank Act, S.C. 1991, c.46.

Canada Post Act, R.S.C., 1985, c.C-10.

Canadian Charter of Rights and Freedoms, *Constitution Act*, 1982 R.S.C., 1985, App.II, no 44.

Civil Code of Quebec, S.Q. 1991, c.64.

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, http://www.conventions.coe.int/Treaty/en/Treaties/Html/108.htm.

Data Protection Act, 1998 c. 29.

Directive 95/46/EC *on the protection of individuals with regard to the processing of personal data and of the free movement of such data*, http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.

Directive 97/66/EC *concerning the processing of personal data and the protection of privacy in the telecommunications sector, http://www.aip-bg.org/lichnidanni/pdf/directive_97_66.pdf.*

European Union Charter of Fundamental Rights, http://ec.europa.eu/justice/fundamental-rights/charter/index_en.htm.

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

Personal Information Protection Act, S.A. 2003 Chapter P-6-5.

Personal Information Protection Act, SBC 2003 Chapter 23.

Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5.

Quebec Charter of Human Rights and Freedoms, CQLR, c. C-12.

Radio Communications Act, R.S.C., 1985, c.R-2.

Règlement 58-101 sur l'information concernant les pratiques en matière de gouvernance, http://www.lautorite.qc.ca/files/pdf/reglementation/valeurs-mobilieres/58-101/2015-11-17/2015nov17-58-101-vofficielle-fr.pdf.

Regulations Specifying Publicly Available Information SOR /2001-7.

Restatement (Second) of the Law of Torts, § 652A (1997).

Telecommunications Act, S.C. 1993, c.38.

The International Covenant on Civil and Political Rights, http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx.

The Privacy Act, RSBC 1996, c 373.

The Privacy Act, CCSM c P125.

The Privacy Act, RSS 1978, Chapter P-24.

The Privacy Act, RSNL 1990, Chapter P-22.

United Nations' Universal Declaration of Human Rights, http://www.un.org/en/documents/udhr/.

Jurisprudence

A.B. v. *Bragg Communications Inc,* [2012] 2 S.C.R. 567.

Alberta v. *Hutterian Brethren of Wilson Colony*, [2009] 2 S.C.R. 567.

Alberta (Information and Privacy Commissioner) v. *United Food and Commercial Workers, Local 401,* [2013] 3. S.C.R. 733.

Aubry v. Les Éditions Vice-Versa Inc. [1988] 1 S.C.R. 591.

Blanc v. *Éditions Bang Bang,* [2011] QCCS 2624.

Campbell v. *MGN Limited,* [2004] UKHL.

Campeau et Services alimentaires Delta Dailyfood Canada, 2012 QCCLP 7666.

Carmie Watkins, Plaintiff-appellant, v. *L.M. Berry & Company, et al., Defendants-appellees*, 704 F.2d 577 (11th Cir. 1983).

Cass. Soc., 2 octobre 2001, Société Nikon France SA, Bull.Civ. 2001.

Deschesnes v. *Groupe Jean Coutu (P.J.C.) Inc*, [2000] C.A.I., 216.

Dubé c. *Le Secretariat de L'action catholique de Joliette*, 2004 CanLII 73641 (QC SAT).

Englander v. *Telus Communication*, 2004 FCA 387 (CanLII).

Ford v. *Quebec,* [1988] 2 S.C.R. 712.

Godbout v. *Longueil*, [1997] 3 S.C.R. 844.

Jane Doe 464533 v. *ND* [2016] O.J. No. 382, 2016 ONSC 541.

Jones v. *Tsige*, 2012, ONCA, 32.

Randall v. *Nubodys Fitness Centres*, 2010 FC 681.

R. v. *Cole,* [2012] 3 S.C.R. 34.

R. v. *Duarte* [1990]1 SCR 30.

R. v. *Dyment,* [1988] 2 S.C.R. 417.

R. v. *Edwards Books and Art,* [1986] 2 S.C.R. 713.

R. v. *Fearon,* 2014 S.C.R. 77.

R. v. *Oakes,* [1986] S.C.R. 103.

R. v. *Patrick,* [2009] 1 S.C.R. 579.

R. v. *Plant* [1993] 3 S.C.R. 281.

R. v. *Spencer,* 2014 SCC 43.

R. v. *Tessling,* [2004] 3 S.C.R. 431.

R. v. *Vu,* [2013] 3 S.C.R. 657.

Smyth v. *Pillsburry Co*., 914. Supp. 97 (E.D. Pa. 1996).

Syndicat des travailleurs(euses) de Bridgestone Firestone de Joliette (csn) c. *Trudeau*, 1999 CanLII 13295 (QC CA).

Wainright v. *Home Office,* [2003] UKHL 53.

X c. *Residence l'Oasis Fort Saint-Louis,* [1995] no AZ-95151507 (C.A.I).

Secondary Sources

Barak, Aharon, “Proportionality Effect: The Israeli Experience”, (2007), 57 *University of Toronto Law Journal* 369.

Calo, Ryan, “Privacy and Markets: A Love Story”, *Legal Studies Research Paper* No. 2015-26.

Commission d’accès à l’information du Québec, “Le marketing direct : les obligations des entreprises”, www.cai.gouv.qc.ca.

Commission permanente de la culture, Fascicule no 11, 23 février 1993.

Cummins, http://sustainability.cummins.com/social/diversity/diversity-procurement.

Drumbl, Mark A. and Craig, John D.R., “Affirmative Action in Question: A Coherent Theory for Section 15(2)”, Vol. IV, No.1 (1997) *Review of Constitutional Studies*, 80.

Eltis, Karen, “La surveillance du courrier électronique en milieu de travail : le Québec succombera-t-il à l’influence de l’approche américaine? ”, (2006) 51 McGill L.J. 475.

Geist, Michael, “Computer and E-Mail Workplace Surveillance in Canada: The Shift From Reasonable Expectation of Privacy To Reasonable Surveillance” (2003) 82 R. du B. Can. 1.

Gratton, Eloise, *Understanding Personal Information: Managing Privacy Risks*, Markham, ON, Lexis Nexis Canada Inc., 2013.

Gratton, Eloise, “Updating Quebec Private Sector Privacy Law – Part 2 of 2” http://www.eloisegratton.com/blog/2015/12/11/updating-quebec-private-sector-privacy-law-part-2-of-2/.

Granosik, Lukasz, “Le critère de nécessité: son évolution, son importance, son impact et son application», *Les 20 ans de la Loi sur la protection des renseignements personnels dans le secteur privé* (2014), Cowansville : Y. Blais, 2014.

Halpérin, Jean-Louis, “L’essor de la ‘privacy’ et l’usage des concepts juridiques”, *Droit et Société* 61/2005, 765.

Hogg, Peter, *Constitutional Law of Canada*, 5th ed., vol. 2 Toronto: Carswell, 2014.

Hunt, Chris D.L., “Conceptualizing Privacy and Elucidating its Importance: Foundational Considerations for the Development of Canada’s Fledgling Privacy Tort”, (2011) 37 Queen’s L.J. 167.

Hunt, Murray, *Using Human Rights Law in English Courts*, Oxford, Hart Publishing, 1997.

Klein, Naomi, *No Logo*, London, Flamingo, 2000.

Lawson, Philippa and O'Donoghue, Mary, "Approaches to Consent in Canadian Data Protection Law", in Kerr, Lucock and Steeves, eds. On the Identity Trail: Anonymity, Privacy and Identity in a Networked Society, Oxford: UP, 2009, 23-42.

Morgan, Charles, "Employer Monitoring of Employee Electronic Mail and Internet Use", (1999) 44 McGill L.J. 849.

Newman, Daniel E., "European Union and United States Personal Information Privacy, and Human Rights Philosophy – Is There a Match?", (2008) 22 Temp. Int'l & Comp. L.J. 307.

Office of the Information and Privacy Commissioner of Alberta, "Guidelines for Social Medial Background Checks", December 2011.

Philipson, Gavin, "Transforming Breach of Confidence? Towards a Common Law Right of Privacy under the Human Rights Act", MLR 66:5, September 2003, 726.

RIA Canada, https://riacanada.ca/trendsreport/.

Scassa, Teresa and Deturbide, Michael, *Electronic Commerce and Internet Law in Canada*, 2nd. Ed., Toronto, CCH Canada Limited, 2012.

Tene, Omer and Polonetsky, Jules, "Big Data for All: Privacy and User Control in the Age of Analytics, 11 *Northwestern Journal of Technology and Intellectual Property* (2013) 239.

Tene, Omer and Polonetsky, Jules, "To Track or 'Do Not Track" Advancing Transparency and Individual Control in Online Behavioral Advertising", 2012, *Minnesota Journal of Law, Science & Technology*, Vol. 13.1.

United Nations-Supported Principles for Responsible Investing, https://www.unpri.org/about/the-six-principles.

Warren, Samuel D. and Brandeis, Louis D., "The Right to Privacy", Harvard Law Review, V.IV, No.5, December 1890.

Westin, Alan, *Privacy and Freedom*, NY, IG Publishing, 1967.

Whitman, James, "The Two Western Cultures of Privacy", (2003-2004) 113 Yale L.J. 1151.