Université de Montréal

The Legal Implications of Internet Marketing :
Exploiting the Digital Marketplace Within the Boundaries of the Law

par
Sarit Mizrahi

Faculté de droit

Mémoire présenté à la Faculté des études supérieures
en vue de l'obtention du grade de maîtrise en droit (LL.M.)
option Droit des technologies de l'information

décembre 2012

Université de Montréal
Faculté des études supérieures et postdoctorales

Ce mémoire intitulé :

The Legal Implications of Internet Marketing : Exploiting the Digital Marketplace Within the Boundaries of the Law

Présenté par :
Sarit Mizrahi

a été évalué par un jury composé des personnes suivantes :

Professeur Karim Benyekhlef, président-rapporteur
Professeur Nicolas Vermeys, directeur de recherche
Professeur Pierre Trudel, membre du jury

RÉSUMÉ

Au cours des dernières années, le domaine de la consommation a grandement évolué. Les agents de marketing ont commencé à utiliser l'Internet pour influencer les consommateurs en employant des tactiques originales et imaginatives qui ont rendus possible l'atteinte d'un niveau de communication interpersonnelle qui avait précédemment été insondable. Leurs interactions avec les consommateurs, en utilisant la technologie moderne, se manifeste sous plusieurs formes différentes qui sont toutes accompagnés de leur propre assortiment de problèmes juridiques. D'abord, il n'est pas rare pour les agents de marketing d'utiliser des outils qui leur permettent de suivre les actions des consommateurs dans le monde virtuel ainsi que dans le monde physique. Les renseignements personnels recueillis d'une telle manière sont souvent utilisés à des fins de publicité comportementale en ligne – une utilisation qui ne respecte pas toujours les limites du droit à la vie privée. Il est également devenu assez commun pour les agents de marketing d'utiliser les médias sociaux afin de converser avec les consommateurs. Ces forums ont aussi servi à la commission d'actes anticoncurrentiels, ainsi qu'à la diffusion de publicités fausses et trompeuses – deux pratiques qui sont interdites tant par la loi sur la concurrence que la loi sur la protection des consommateurs. Enfin, les agents de marketing utilisent diverses tactiques afin de joindre les consommateurs plus efficacement en utilisant diverses tactiques qui les rendent plus visible dans les moteurs de recherche sur Internet, dont certaines sont considérés comme malhonnêtes et pourraient présenter des problèmes dans les domaines du droit de la concurrence et du droit des marques de commerce. Ce mémoire offre une description détaillée des outils utilisés à des fins de marketing sur Internet, ainsi que de la manière dont ils sont utilisés. Il illustre par ailleurs les problèmes juridiques qui peuvent survenir à la suite de leur utilisation et définit le cadre législatif régissant l'utilisation de ces outils par les agents de marketing, pour enfin démontrer que les lois qui entrent en jeu dans de telles circonstances peuvent, en effet, se révéler bénéfiques pour ces derniers d'un point de vue économique.

Mots-clés : publicité comportementale en ligne, vie privée, médias sociaux, protection du consommateur, optimisation pour les moteurs de recherche, chapeaux noirs, hackers, AdWords, concurrence déloyale, marques de commerce

ABSTRACT

The evolution of consumerism in recent years has been nothing short of remarkable. The unprecedented use of the Internet by marketers to influence consumers in original and imaginative ways has rendered possible a level of communicative efficiency that had previously been unfathomable. Their interaction with consumers using modern technology manifests itself in several different forms – all of which are accompanied by their own assortment of legal issues. To begin with, it is not unheard of for marketers to use tools meant to track the behaviour of individuals throughout both the virtual and physical worlds. The personal information collected in such a manner is often utilized for Online Behavioural Advertising purposes – a use which does not always respect the boundaries of privacy law. It has also become rather common for marketers to utilize online social media to promote conversations with consumers. It has occurred, however, that these forums have also been utilized to further the anti-competitive ambitions of companies while also serving as an outlet for false advertising – two eventualities that are prohibited by both competition laws and consumer protection laws. Finally, marketers utilize various tactics in order to more successfully reach consumers through online search engines – a practice known as Search Engine Marketing – some of which are considered to be dishonest and could present issues from both competition law and trademark law perspectives. This thesis essentially provides a detailed description of these tools and the manners in which they are utilized and then proceeds to illustrate the legal issues that may arise as a result of their use. In doing so, it outlines the legal boundaries within which marketers must use these tools so as to ultimately demonstrate that the laws that come into play under such circumstances may, in fact, prove to be beneficial to marketers from an economic perspective.

Keywords : Online Behavioural Advertising, Privacy, Social Media Marketing, Consumer Protection, Search Engine Marketing, Black hat, Keyword advertising, Unfair Competition, Trademarks

TABLE OF CONTENTS

LIST OF ACRONYMS AND ABBREVIATIONS

AELFIT	An Act to establish the Legal framework for information technology
AIPLA Quarterly Journal	American Intellectual Property Law Association Quarterly Journal
Alb. L.J. Sci. & Tech.	Albany Law Journal of Science and Technology
All E.R.	All England Law Reports
ARPPIPS	An Act Respecting the Protection of Personal Information in the Private Sector
B.C. L. Rev.	Boston College Law Review
B.E.	Banque Express
B.R.	Quebec Judicial Reports; Court of the Queen's Bench (in appeal)
B.U. J. Sci. & Tech. L.	Boston University Journal of Science and Technology Law
BCSC	British Columbia Supreme Court
Berkeley Tech. L.J.	Berkeley Technology Law Journal
Bus. Law.	The Business Lawyer
C. de D.	Les Cahiers de droit
C.A.	Cour d'appel/Court of Appeal
C.A.I.	Commission d'accès à l'information
C.C.	Criminal Code
C.C.C.	Canadian Criminal Cases
C.C.Q.	Civil Code of Quebec
C.J.L.T.	Canadian Journal of Law and Technology
C.P.R.	Canadian Patent Reporter
C.Q.	Court of Quebec
C.R.R.	Canadian Rights Reporter

C.S.	Cour supérieure/Superior Court
CAI	Commission d'accès à l'information/Access to Information Commission
Cal. Rptr.	California Reporter
Can. Bus. L.J.	Canadian Business Law Journal
Can.-U.S. L.J.	Canada United States Law Journal
Cir. Cal.	Circuit Court of Appeals
Cleveland St. L. Rev.	Cleveland State Law Review
Competition Act	CA
Conn. L. Rev.	Connecticut Law Review
Consumer Protection Act	CPA
Ct. App. 2nd Cir.	Court of Appeals, Second Circuit
D.L.R.	Dominion Law Reports
Deep Packet Inspection	DPI
Def. Counsel J.	Defense Counsel Journal
DePaul-LCA J. Art & Ent. L.	DePaul-LCA Journal of Art and Entertainment Law
Dist. Ct. Texas	District Court of Texas
E.D. Va.	Eastern District Court of Virginia
EYB	Éditions Yvon Blais
F. Supp.	Federal Supplement
F.C.	Canada Federal Court Reports
F.C.A.	Federal Court of Appeal
F.C.J.	Federal Court Judgments
F.C.T.D.	Federal Court Trial Division
FC	Federal Court
GPS	Global Positioning Device
Ga. L. Rev.	Georgia Law Review
Harv. J. L. & Tech.	Harvard Journal of Law and Technology

Hastings Comm. & Ent. L.J.	Hastings Communication and Entertainment Law Journal
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
I.D.E.A.	IDEA: The Intellectual Property Law Review
Ind. L. Rev.	Indiana Law Review
Int'l Bus. L.J.	International Business Law Journal
Intell. Prop. L. Bull.	Intellectual Property Law Bulletin
Internet Service Provider	ISP
IP Address	Internet Protocol Address
J. Legal Stud.	Journal of Legal Studies
J. Telecomm. & High Tech L.	Journal on Telecommunications & High Technoloy Law
J.E.	Jurisprudence expresse
J.L.	Jurisprudence logement
J.Q.	Jugements du Québec/Quebec Judgments
L.C.	Laws of Canada
L.Q.	Laws of Quebec
L.R.Q.	Lois refondues du Québec/Revised Statutes of Quebec
Location-based Social Network	LBSN
Loy. U. Chi. L.J.	Loyola University Chicago Law Journal
M.D. Fla.	United States District Court for the Middle District of Florida
MAC Address	Media Access Control Address
MIS Quarterly	Management Information Systems Quarterly
Mich. L Rev.	Michigan Law Review
N.D. Cal.	United States District Court, Northern District of California
N.D. Ill.	Northern District Court of Illinois

N.R.	National Reporter
O.A.C.	Ontario Appeal Cases
O.J.	Ontario Judgments
ONCA	Ontario Court of Appeal
P.C.C.	Privacy Commissioner of Canada
Penn. St. Int'l L. Rev.	Penn State International Law Review
PIPEDA	Personal Information Protection and Electronic Documents Act
QC C.S.	Cour supérieure du Québec/Quebec Superior Court
QCCA	Cour d'appel du Québec/Quebec Court of Appeal
QCCQ	Cour du Québec/Court of Quebec
QCCS	Cour supérieure du Québec/Quebec Superior Court
R. de. J.	Revue de jurisprudence
R.G.D.	Revue générale de droit
R.G.D.	Revue générale de droit
R.J.E.U.L.	Revue juridique des étudiants de l'Université Laval
R.J.Q.	Recueil de jurisprudence du Québec
R.J.T.	Revue Juridique Thémis
R.L.	Revue légale
R.L.n.s.	Revue légale - Nouvelle série
R.R.A.	Recueil en responsabilité et assurance
R.S.C.	Revised Statutes of Canada
R.S.Q.	Revised Statutes of Quebec
REJB	Répertoire électronique de jurisprudence du Barreau
S. C. L. Rev.	South Carolina Law Review
S. Cal. Interdisc. L.J.	Southern California Interdisciplinary Law Journal
S.C.	Statutes of Canada
S.C.R.	Supreme Court Rulings
S.D.N.Y.	Southern District of New York

S.O.Q.U.I.J.	Société québécoise d'information juridique
Santa Clara L. Rev.	Santa Clara Law Review
SCC	Supreme Court of Canada
Search Engine Marketing	SEM
Shidler J.L. Com. & Tech.	Shidler Journal of Law, Commerce and Technology
Social Media Marketing	SMM
Social Network Website	SNW
Trade-marks Act	TMA
Trademark Rep.	The Trademark Reporter
U. Toronto Fac. L. Rev.	University of Toronto Faculty of Law Review
U.B.C.L. Rev.	University of British Columbia Law Review
URL	Uniform Resource Locator

To my parents, who provided me with the faith, confidence and courage to chase my dreams; to my sisters who have never failed to give me the strength that got me through all the milestones in my life; to my nieces and nephews who have always managed to make me smile along the way; and to Aylon, without whose solid shoulder and undying support I would never have been able to complete this thesis.

ACKNOWLEDGMENTS

I would like to take this opportunity to express my gratitude to my thesis advisor, Professor Nicolas Vermeys, to whom I am eternally grateful for being there every step of the way to provide me with the guidance I required to complete this thesis. Your unwavering dedication and support is heartfelt and very much valued and appreciated.

INTRODUCTION

The evolution of consumerism in recent years has been nothing short of remarkable. The unprecedented use of the Internet by marketers to influence consumers in original and imaginative ways has rendered possible a level of communicative efficiency that had previously been unfathomable. Not only does the Internet provide an innovative means of presenting consumers with all the possibilities that the market has to offer them, but it also endows marketers with an increased ability to satisfy those consumer desires which may not necessarily be mainstream.

Internet marketing makes use of the World Wide Web to promote and facilitate the exchange of goods and services from merchants to consumers, ultimately providing consumers with what they need and want[1]. The significance of Internet marketing, however, lies not only in the new medium itself, but also in the possibilities it presents. Contrary to the physical world, the World Wide Web possesses no boundaries. Consequently, while the physical world is adept at fulfilling solely those desires which are mainstream, the virtual world is capable of satisfying *all* consumer desires, no matter how precise and rare they may be.

This phenomenon can be explained by a theory coined by economist Chris Anderson and known as the "Long Tail theory"[2]. The Long Tail theory outlines the insufficiency of the physical world in today's market, and the manner in which the Internet provides incredible possibilities for the exploitation of this gap. On account of its spatial limitation, the physical world is only able to provide what can be sold in sufficient quantity to ensure profitability. As a result, brick and mortar establishments tend to limit themselves to the provision of mainstream products that will attract a significant number of consumers, while ignoring the more pointed tastes, referred to as niche products, of a

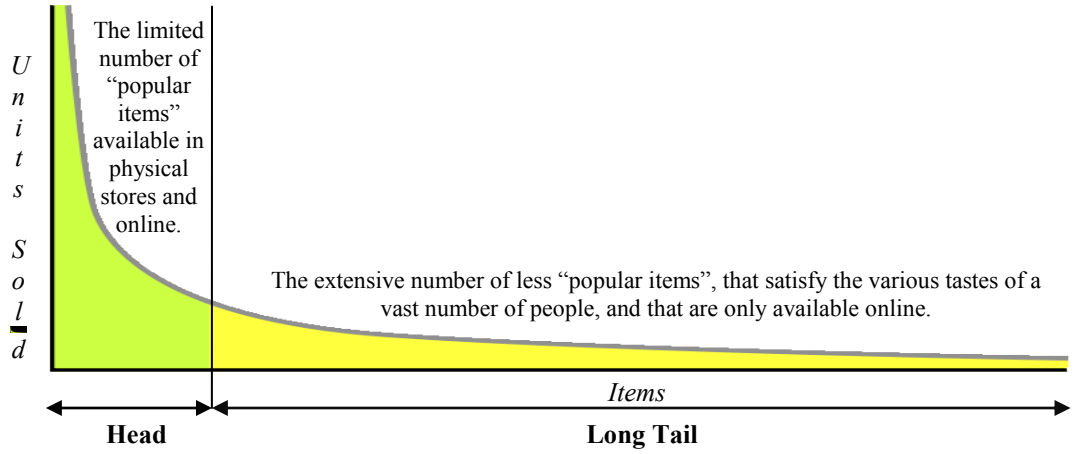
---

[1]Kent A. GRAYSON, Jonathan D. HIBBARD and Philip KOTLER, "Marketing", in *Encyclopædia Britannica Online Academic Edition*, 2011, online: <http://www.britannica.com/EBchecked/topic/365730/marketing> (site consulted on November 19, 2011).

smaller percentage of the population. This is due to the fact that niche products are so numerous and fulfill such a vast assortment of tastes for various people, that it would not be economically sound for a physical establishment, afflicted with a limitation on space, to carry all of these different items so as to satisfy such diverse desires. The lack of benefit for carrying niche products in a brick and mortar establishment results directly from the inability to sell each of these items in sufficient quantity that would justify the cost of their occupation of shelf space[3].

In a world where shelf space is not an issue, however, the profit that could be incurred through the sale of niche products is significant as the number of niche markets is never-ending. This reality is depicted by Chris Anderson as a power law distribution graph, where the "head" of the graph represents the mainstream products that are sold in large quantities, and the "tail" of the graph, which extends infinitesimally never quite reaching zero, represents the niche products (see Image 1). This graph essentially illustrates the fact that, while "[…] individually, none of these [niche products are] popular, [...] there are just so *many* of them that collectively they represent a substantial market"[4].

Image 1: The Head and the Long Tail[5]



---

[2] Chris ANDERSON, *The Long Tail: Why the Future of Business is Selling Less of More*, New York, Hyperion, 2006.
[3] *See: Id.*, p. 15-26.
[4] *Id.*, p. 21-22.

This is where the Internet provides all of its possibilities. Unlike brick and mortar establishments, the Web is not limited with respect to the number of products it can provide. It is thus possible for online retailers to satisfy the niche desires in a manner that would never be feasible for physical ones, ultimately serving to create a seemingly endless market for online vendors[6]. The Internet has therefore opened up a world of unlimited choice in which businesses no longer need to fixate solely on profitable mainstream demands, but can rather exploit a multitude of low volume niche opportunities[7]. Chris Anderson sums this phenomenon up in the following manner:

> "The theory of the Long Tail can be boiled down to this: Our culture and economy are increasingly shifting away from a focus on a relatively small number of hits (mainstream products and markets) at the head of the demand curve, and moving toward a huge number of niches in the tail. In an era without the constraints of physical shelf space and other bottlenecks of distribution, narrowly targeted goods and services can be as economically attractive as mainstream fare."[8]

As a result of the ability to provide individuals with niche products, not only were existing markets expanded beyond what had ever been thought possible, but entirely new, more targeted and less mainstream markets were discovered as well[9]. The creation of these markets was accompanied by an entirely new assortment of marketing tactics, which were developed to exploit these new markets to their highest possible extent, and revolve around two main elements. The first element consists of targeting consumers based on their interests demonstrated through their online behaviour, which is achieved by using an assortment of technological devices to track their browsing habits and determine their preferences and market to them based on this data. The second element, on the other hand, entails reaching consumers in more innovative ways through the World Wide Web, which

---

[5] *Id.*, p. 25.
[6] *Id.*, p. 22.
[7] Jon HOWARD, "Wagging the Tail", July 20, 2006, online: <http://jonhoward.typepad.com/livingbrands/2006/07/wagging_the_tai.html> (site consulted on July 6, 2011).
[8] C. ANDERSON, prev. cited, note 2, p. 52.
[9] *Id.*

is accomplished by both conversing with consumers through the use of various forms of social media with the goal of determining their interests and marketing to them based on this data, as well as ensuring the visibility of businesses in online search engines in order to render it simpler for consumers to find what they are searching for.

While these tactics are beneficial to marketers, as they provide them with an insight into the personality of each consumer, allowing them to market to these individuals based on their personal interests and ultimately leading to greater market efficiency[10], these techniques may not necessarily be legally sound and pose significant issues in several areas of the law. To begin with, the online marketing tactic whereby users are targeted based on information acquired through tracking them, present numerous problems with regards to privacy protection. These tools essentially serve to track users throughout the Internet[11], and even in the physical world through cellular telephones[12], so as to determine patterns in their preferences and habits and then utilize that data to target consumers with advertising that would most appeal to them on a personal level, based on their interests as well as their

---

[10] Ari JUELS, "Targeted Advertising…And Privacy Too", in David NACCACHE (dir.), *Topics in Cryptology: The Cryptographers' Track at the RSA Conference 2001*, Berlin, Springer, 2001, 408, at page 409.

[11] *See:* Angela DALY, "The Legality of Deep Packet Inspection, June 17, 2010, online: <http://ssrn.com/abstract=1628024 or doi:10.2139/ssrn.1628024> (site consulted on January 19, 2012); Justin P. JOHNSON, "Targeted Advertising and Advertising Avoidance", July 28, 2009, p. 1, online: <http://www.econ.as.nyu.edu/docs/IO/12543/Johnson_20091027.pdf> (site consulted on November 24, 2011); Janet LO, "A 'Do Not Track List' for Canada?", December 3, 2009, online: <www.piac.ca/files/dntl_final_website.pdf> (site consulted on November 24, 2011); OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "Cookies – Following the crumbs", 2011, online: <http://www.priv.gc.ca/fs-fi/02_05_d_49_01_e.cfm> (site consulted on November 24, 2011); Andrea N. PERSON, "Behavioral Advertisement Regulation: How the Negative Perception of Deep Packet Inspection Technology May be Limiting the Online Experience", (2010) 62-2 *Federal Communications Law Journal* 435; Arnold ROOSENDAAL, "Facebook Tracks and Traces Everyone: Like This!", November 30, 2010, online: <http://ssrn.com/abstract=1717563> (site consulted on January 19, 2012).

[12] *See:* Nancy J. KING, "Direct Marketing, Mobile Phones, and Consumer Privacy: Ensuring Adequate Disclosure and Consent Mechanisms for Emerging Mobile Advertising Practices", (2007) 60-2 *Federal Communications Law Journal* 239; Stephanie LOCKWOOD, "Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators", (2004) 18 *Harv. J. L. & Tech.* 307; April A. OTTENBERG, "GPS Tracking Technology: The Case for Revisiting Knotts and Shifting the Supreme Court's Theory of the Public Space Under the Fourth Amendment", (2004) 46-3 *B. C. L. Rev.* 661.

location at the time the advertisement is targeted to them[13]. The use of such tools to basically stalk consumers throughout both the physical and virtual worlds is often viewed as a severe invasion of privacy[14], and therefore inevitably causes conflicts with regards to the protection of the privacy of these individuals, which is unequivocally guarded by Quebec[15] and Canadian[16] law alike.

Furthermore, the social media tools used to converse with users, such as blogs and social networks, are often also tackled with legal issues, more particularly from the perspectives of trade libel and consumer protection laws. To begin with, these forms of social media serve as forums which can often provide outlets for anti-competitive behaviour. These are venues upon which individuals are able to adopt an identity other than their own – a level of anonymity that is used by business officials to commit trade libel in an attempt to ruin the reputation of their competitors through defamatory comments[17].

---

[13] *See:* A. DALY, prev. cited, note 11; J. P. JOHNSON, prev. cited, note 11; A. JUELS, prev. cited, note 10; N. J. KING, *Id.*; J. LO, prev. cited, note 11; S. LOCKWOOD, *Id.*; OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, prev. cited, note 11; A. A. OTTENBERG, *Id.*; A. N. PERSON, prev. cited, note 11; A. ROOSENDAAL, prev. cited, note 11.

[14] A. DALY, *Id.*; J. P. JOHNSON, *Id.*; A. JUELS, *Id.*; N. J. KING, *Id.*; J. LO, *Id.*; S. LOCKWOOD, *Id.*; OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, *Id.*; A. A. OTTENBERG, *Id.*; A. N. PERSON, *Id.*; A. ROOSENDAAL, *Id.*

[15] *Charter of Human Rights and Freedoms*, L.R.Q., c. C-12, art. 5; *Civil Code of Quebec*, L.Q. 1991, c.64, art. 35-41; *An Act Respecting the Protection of Personal Information in the Private Sector*, L.R.Q., c. P-39.1; *An Act to establish the Legal framework for information technology*, R.S.Q., c. C-1; *Consumer Protection Act*, R.S.Q., c. P-40.1.

[16] *Canadian Charter of Rights and Freedoms,* part 1 of the *Constitution Act of 1982*, [schedule B to the *Canada Act 1982*, 1982, c. 11 (U.K.)], art. 8; *Criminal Code*, R.S.C. 1985, c. C-46; *Personal Information Protection and Electronic Documents Act*, L.C. 2000, c. 5; *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act*, S.C. 2010, c. 23.

[17] *See:* Michael A. ALBERT and Robert L. BOCCHINO JR., "Trade Libel: Theory and Practice Under the Common Law, The Lanham Act, and the First Amendment", (1999) 89 *Trademark Rep.* 826; Thomas G. CIARLONE JR. and Eric W. WIECHMANN, "Cybersmear May Be Coming to a Website Near You: A Primer for Corporate Victims", (2003) 70 *Def. Counsel J.* 51; Jonathan T. FEASBY, "Who Was That Masked Man? Online Defamation, Freedom of Expression, and the Right to Speak Anonymously", (2002) 1-1 *C.J.L.T*, online: <http://cjlt.dal.ca/vol1_no1/articles/01_01_Feasby_defam.pdf> (site consulted on January 20, 2011); Peter Carmichael KEEN, "Anonymity and the Supreme Court's Model of Expression: How Should Anonymity be Analyzed Under Section 2(b) of the Charter?", (2005) 2-3 *C.J.L.T* 167; Michael L. RUSTAD

These types of environments also serve as a threat to consumers. In effect, the nature of the content written in these forums is not sufficiently regulated to ensure consumer protection and is sometimes used by companies to impersonate consumers so that they may more effectively convince other consumers that their products and services are desirable in the eyes of the average person. This may ultimately violate numerous principles adopted by the laws that exist to protect these individuals against being misled with regards to the products or services being offered[18].

Finally, there are certain tools that are used to make sites more easily accessible online with the ultimate goal of reaching as many users as possible – a practice which is commonly referred to as Search Engine Marketing. This practice effectively requires the employment of various techniques that serve to increase the visibility of businesses in online search engines and may pose certain issues from both competition and trademark law perspectives. There are certain instances in which these tools are used in a dishonest fashion with the goal of diminishing the online presence of competitors, and as such, the back-handed use of these tools can be viewed as an anti-competitive practice[19]. With regards to the issues these tools raise in light of trademark law, on the other hand, several

---

and Thomas H. KOENIG, "Cybertorts and Legal Lag: An Empirical Analysis", (2003) 13 *S. Cal. Interdisc. L.J.* 77; Kim VON ARX, "LitOral: A New Form of Defamation Consciousness", (2002) 1-2 *C.J.L.T* 63.

[18] *See:* Alex W. CANNON, "Regulating AdWords: Consumer Protection in a Market Where the Commodity is Speech", (2009) 39-1 *Seton Hall Law Review* 291; Christian HOEDL, "How to Market Services: Advertising Consumer Protection and Personal Data", (1998) 3 *Int'l Bus. L.J.* 285; Nicole LADOUCEUR, "Calibrating the Electronic Scales: Tipping the Balance in Favour of a Vigorous and Competitive Electronic Market for Consumers", (1999) 25 *Can.-U.S. L.J.* 295; Gregory E. MAGGS, "Internet Solutions to Consumer Protection Problems", (1997) 49 *S. C. L. Rev.* 887; David WAITE, "Consumer Protection Issues in Internet Commerce", (1999) 32 *Can. Bus. L.J.* 132; Spencer Weber WALLER, "In Search of Economic Justice: Considering Competition and Consumer Protection Law", (2004) 36 *Loy. U. Chi. L.J.* 631.

[19] *See:* Cédric ARGENTON and Jens PRÜFER, "Search Engine Competition with Network Externalities", April 11, 2011, online: <http://www.tilburguniversity.edu/webwijs/files/center/prufer/search_engines.pdf> (site consulted on January 25, 2012); James GRIMMELMANN, "The Structure of Search Engine Law", (2007) 93 *Iowa Law Review* 1; Rossa MALAGA, "Worst Practices in Search Engine Optimization", (2008) 51-12 *Communications of the ACM* 147, 149; Frédéric RAYNAL and François GASPARD, "Small treatise about e-manipulation for honest people", (2010) 6-2 *Journal in Computer Virology* 143; Daniel F. SPULBER, "The Map of Commerce: Internet Search, Competition, and the Circular Flow of Information", (2009) 5-4 *Journal of Competition Law and Economics* 633; Herbert ZUZE, *The Crossover Point Between Keyword Rich Website*

online tools used to increase the visibility of companies in response to specific queries in search engines make use of trademarks owned by other entities – a practice which could be viewed as a form of trademark infringement[20]. Due to this, the legal world has been afflicted with constant debates regarding the manner in which to treat this issue, mostly trying to apply traditional principles of trademark law to determine a solution[21].

Although these marketing techniques suffer from numerous legal issues in the areas of privacy law, trade libel law, competition law, trademark law and consumer protection law, all of which will be discussed in detail throughout this thesis, certain measures may be taken to ensure that their continued use remains within the boundaries of the law without necessarily hindering the success of their use. In the present day and age, these areas of the law are the ones that Canadian marketing businesses are most confronted with when it comes to online marketing and this knowledge can therefore be extremely useful to them by permitting them to be aware of the legal boundaries within which they must function and ensuring that they do not surpass that which is permissible by the law, ultimately preventing them from having to face future legal action from this perspective.

While compliance to these laws may appear to be an onerous task for Internet marketers, as they impose several rules which they must obey without fault, many

---

Text and Spamdexing, Master's thesis, Cape Town, Faculty of Business, Cape Peninsula University of Technology, 2011.

[20] *See:* Regina NELSON ENG, "A Likelihood of Infringement: The Purchase and Sale of Trademarks as Adwords", (2009) 18-2 *Alb. L.J. Sci. & Tech* 493; Jacob JACOBY and Mark SABLEMAN, "Keyword-Based Advertising: Filling in Factual Voids (*GEICO v. Google*)", (2007) 97-3 *Trademark Rep.* 681; Jonathan MOSKIN, "Virtual Trademark Use – The Parallel World of Keyword Ads", (2008) 98-3 *Trademark Rep.* 873; Riana PFEFFERKORN, "Liability for Search Engine Triggering of Trademarked Keywords after Rescuecom", (2008) 5 *Shidler J.L. Com. & Tech.* 2; Kurt M. SAUNDERS, "Confusion is the Key: A Trademark Law Analysis of Keyword Banner Advertising", (2002) 71 *Fordham Law Review* 543; Gregory SHEA, "Trademarks and Keyword Banner Advertising", (2002) 75 *Southern California Law Review* 529; Ashley TAN, "Google Adwords: Trademark Infringer or Trade Liberalizer?", (2010) 16 *Michigan Telecommunications and Technology Law Review* 473; Reed W. TAUBNER, "Google AdWords and Canadian Trademark Law", (2010) 7-2 *C.J.L.T.* 289; Kevin ZECK, "Referential Fair Use & Keyword Advertising: The Necessity of Product Placement to our Domestic System of Free-Market Enterprise, (2008) 44-3 *Gonzaga Law Review* 519.

marketers fail to see the economic benefits that are enabled by these laws, which can be properly illustrated using Economic Analysis of Law.

Economic Analysis of Law essentially

> "seeks to trace the reason for the existence of judicial institutions. It postulates that [the writings of positive law] exhibit a uniform underlying rationality and provides the conceptual tools with which to update them […] in order to permit jurists to better comprehend and, by the interpretation of concepts, to extend their logic to novel disputes that may arise."[22] (our translation)

This analysis will thus be used throughout this thesis by illustrating the prevailing reasons for which the laws applicable to the area of Internet marketing were developed to ultimately demonstrate the effects of existing legal rules on this practice, whether or not these effects are socially desirable, and what changes must be incurred to ensure an outcome that is advantageous from both a consumer and a business perspective[23]. The reason for which this tool of legal analysis was chosen is due to the fact that marketing is often used to encourage economic efficiency, by both attracting consumers and serving as a basis for competition, and as such, we believe that any laws that apply to the regulation of this practice ought to be analyzed in a manner that promotes this particular purpose.

We will therefore begin by (I) illustrating the various marketing techniques used online to efficiently exploit the new and varying niche markets which the Internet has rendered possible to develop. After setting forth a comprehensible basis of the tools used for Internet marketing, we will then proceed by (II) discussing the legal implications of these techniques so as to ultimately determine a legally and economically sound middle

---

[21] *See:* R. N. ENG, *Id.*; J. JACOBY and M. SABLEMAN, *Id.*; J. MOSKIN, *Id.*; R. PFEFFERKORN, *Id.*; K. M. SAUNDERS, *Id.*; G. SHEA, *Id.*; A. TAN, *Id.*; R. W. TAUBNER, *Id.*; K. ZECK, *Id.*

[22] Ejan MACKAAY and Stéphane ROUSSEAU, *Analyse économique du droit*, 2nd ed., Montreal, Éditions Thémis, 2008, par. 22.

[23] Louis KAPLOW and Steven SHAVELL, "Economic Analysis of Law", February 1999, p. 4, online: <http://lsr.nellco.org/harvard_olin/251> (site consulted on February 20, 2012).

ground between the respect of existing legal principles and the achievement of socially desirable outcomes with regards to the practice of Internet marketing.

PART I MARKETING TECHNIQUES: EXPLOITING THE NICHES

The ultimate success of online marketing, and the result of the highest possible turnover rate, is based on the accomplishment of two elements: tracking consumers to determine their preferences and specifically targeting them based on this data[24], as well as rendering it significantly simpler for consumers to easily find what they are searching for, either through conversing with marketers[25] or performing a search engine query[26]. These elements are achieved by both (1) tracking users and (2) reaching users.

Chapter 1 Tracking Users

In the modern age of the virtual world, the ability to discover details about consumers and then target them with ads relevant to their preferences is unparalleled and quickly improving, thus exponentially increasing the price tag attached to the information

---

[24] eMARKETER, "New Ways to Target Your Customer", April 20, 2006, online: <http://www.emarketer.com/Article.aspx?id=1003937&R=1003937> (site consulted on September 9, 2012); Heather OSBORN NG, "Targeting Bad Behavior: Why Federal Regulators Must Treat Online Behavioral Marketing as Spyware", (2009) 31 *Hastings Comm. & Ent. L.J.* 369, 371; Pierre TRUDEL, France ABRAN and Gabriel DUPUIS, "Analyse du cadre réglementaire québécois et étranger à l'égard du pourriel, de l'hameçonnage et des logiciels espions", April 2007, p. 24, online : <http://collections.banq.qc.ca/ark:/52327/bs1565476> (site consulted on September 9, 2012).

[25] Melissa LANDAU STEINMAN and Mikhia HAWKINS, "When Marketing Through Social Media, Legal Risks Can Go Viral", May 2010, p. 4-5, online: <http://www.venable.com/files/Publication/b4f467b9-0666-4b36-b021-351540962d65/Presentation/PublicationAttachment/019f4e5f-d6f8-4eeb-af43-40a4323b9ff1/Social_Media_white_paper.pdf> (site consulted on September 9, 2012); MINISTRY OF ECONOMIC DEVELOPMENT AND TRADE, "Social Media Marketing", 2011, p. 1, online: <http://www.ontariocanada.com/ontcan/1medt/smallbiz/sb_downloads/ebiz_social_media_marketing_en.pdf > (site consulted on September 9, 2012).

[26] Bruce CLAY and Susan ESPARZA, *Search Engine Optimization: All-in-One For Dummies*, Hoboken, Wiley Publishing, 2009, p. 9; MINISTRY OF ECONOMIC DEVELOPMENT AND TRADE, "Increasing Traffic to Your Website Through Search Engine Optimization (SEO) Techniques", 2011, p. 1-2, online: <http://www.ontariocanada.com/ontcan/1medt/smallbiz/sb_downloads/ebiz_Search_Engine_en.pdf> (site consulted on September 9, 2012).

that renders this possible[27]. This amplified capacity to determine the particular inclination of consumers arises from the ability to track the behaviour of individuals in (1) the virtual world as well as (2) the physical world.

Section 1 Tracking in the Virtual World: Online Behavioural Advertising

The ability to track consumers throughout the virtual world is enabled by the use of certain technological tools, which are employed to trace user browsing activity and then utilize that information to target users with advertisements based on the preferences they exhibit while surfing the Internet – a practice known as Online Behavioural Advertising[28]. The tools often utilized for this purpose are (1) cookies, (2) Deep Packet Inspection and (3) Social Network Websites, all of which will be discussed in further detail heretofore in light of the manner in which they are used for Online Behavioural Advertising purposes.

Subsection 1 Cookies

A Web cookie is a small piece of text that a Web server places on an individual's Internet browser when they visit a website which saves information regarding that individual's visit to the site until the next time he decides to frequent it[29]. Cookies collect

---

[27] J. P. JOHNSON, prev. cited, note 11, p. 1.

[28] eMARKETER, prev. cited, note 22; FEDERAL TRADE COMMISSION, "FTC Staff Revises Online Behavioral Advertising Principles", February 2009, online: <http://www.ftc.gov/opa/2009/02/behavad.shtm> (site consulted on September 9, 2012); J. LO, prev. cited, note 11, p. 20; H. OSBORN NG, prev. cited, note 24, 371; P. TRUDEL, F. ABRAN and G. DUPUIS, prev. cited, note 24, p. 24.

[29] B. CLAY and S. ESPARZA, prev. cited, note 26, p. 560; Eric COLE, *Network Security Bible*, 2nd ed., 2009, Indianapolis, Wiley Publishing, p. 276; Dieter GOLLMANN, *Computer Security*, New York, John Wiley & Sons, 1999, p. 191; William T. HARDING, Anita J. REED and Robert L. GRAY, "Cookies and Web Bugs: What They Are and How They Work Together", in Harold F. TIPTON and Micki KRAUSE (dir.), *Information Security Management Handbook*, 6th ed., vol. 1, Boca Raton, Auerback Publications, 2007, 2133, at page 2134 and 2137; Joe KISSELL, *Mac Security Bible*, Indianapolis, Wiley Publishing, 2010, p. 343; OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, prev. cited, note 11; Emmaneul PAQUETTE, "Touche pas à mes cookies!, November 19, 2001, online: <http://archives.lesechos.fr/archives/2001/LesEchos/18533-512-ECH.htm> (site consulted on September 10, 2012); Pierre REBOUL and Dominique XARDEL, *Le Commerce électronique: Techniques et Enjeux*, Paris, Éditions Eyrolles, 1997, p. 122; Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF and Sophie HEIN, *Droit du cyberespace*, Montreal, Éditions Thémis, 1997, p. 11-44;

and store information about individuals based on their browsing patterns as well as any information the individual provides willingly, such as language preferences or passwords, in order to save the user from being obliged to enter this information upon each of his visits to the website in question[30]. Once a cookie is shared between a Web server and a user, each time the user requests content from that particular server, the cookie will be activated along with that request[31].

Moreover, Web cookies have become a great deal more versatile with the adoption of third-party cookies. Essentially, rather than cookies only being shared between a website's server (the "first-party") and a user (the "second-party"), cookies can now be transmitted to users from third-parties, such as advertising companies that display ads on certain websites[32]. The ability of third-parties to share cookies with users, however, exists only if they have content placed on the site that is being requested by the user[33]. When the user solicits this website, the content placed on it by the third-party is also entreated, making it possible for the third-party to send a cookie to the user along with the information requested[34].

Attached to each third-party cookie is a unique identifier, an element which makes it possible to identify the user in question and link together information regarding his visits to

---

Rachel K. ZIMMERMAN, "The Way the "Cookies" Crumble: Internet Privacy and Data Protection in the Twenty-First Century", (2000-2001) 4 *Legislation and Public Policy* 439, 442-443.

[30] E. COLE, *Id.*; W. T. HARDING, A. J. REED and R. L. GRAY, *Id.*; J. KISSELL, *Id.*, p. 343-344; OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, *Id.*; P. TRUDEL, F. ABRAN, K. BENYEKHLEF and S. HEIN, *Id.*; *See also:* Michael ERBSCHLOE, *Trojans, Worms, and Spyware: A Computer Security Professional's Guide to Malicious Code*, Oxford, Elsevier Butterworth-Heinemann, 2005, p. 25-26.

[31] W. T. HARDING, A. J. REED and R. L. GRAY, *Id.*, at page 2135; A. ROOSENDAAL, prev. cited, note 11, p. 4; Hong YIN, *Web Search Context Management Using Javascript/Cookie and JSP/Database Technologies*, Master's thesis, Auburn, Faculty of Computer Science and Software Engineering, Auburn University, 2011, p. 12.

[32] B. CLAY and S. ESPARZA, prev. cited, note 26, p. 560-561; Katherine MCKINLEY, "Cleaning Up After Cookies Version I.0", December 31, 2008, p. 2, online: <https://www.isecpartners.com/files/iSEC_Cleaning_Up_After_Cookies.pdf> (site consulted on September 4, 2012); OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, prev. cited, note 11.

[33] A. ROOSENDAAL, prev. cited, note 11, p. 2.

[34] *Id.*

various websites upon which the advertising company in question possesses content[35]. Thus, when the user revisits the same website through which the cookie was initially issued to him, or other websites upon which this same advertising company displays ads, the third-party cookie that was initially transmitted to the user may be read by the advertising company[36] and new information may be added to that cookie. It is important to point out, however, that only the Web server from which the cookie was sent may have access to the information stored therein[37]; the provider of the website itself therefore does not have access to all the third-party cookies emitted while a user visits their site[38].

As a result of their ability to store a significant amount of information about Internet users, cookies are invaluable when it comes to the practice of targeted marketing. Cookies are able to keep track of information ranging from the websites visited by a user to the click-through responses of the user to various advertisements, and everything in between, such as the duration of those visits, the searches performed by the user, the user's IP address[39], the purchases the user has made online, the geographical location information of the user using his IP address or GPS technology, should he be connecting through a mobile device with an embedded GPS[40], and the website which led the consumer to another site monitored by a particular ad network[41].

---

[35] B. CLAY and S. ESPARZA, prev. cited, note 26, p. 561; OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, prev. cited, note 11; Rachel K. ZIMMERMAN, prev. cited, note 29, 444-445.
[36] K. MCKINLEY, prev. cited, note 32, p. 2; OFFICE OF THE PRIVACY COMMISSIONER OF CANADA , *Id.*; Paul OHM, "The Rise and Fall of Invasive ISP Surveillance", (2009) 5 *University of Illinois Law Review* 1417, 1447.
[37] Daniel LIN and Michael C. LOUI, "Taking the Byte Out of Cookies: Privacy, Consent and the Web", (1998) *Computers and Society* 39, 48.
[38] B. CLAY and S. ESPARZA, prev. cited, note 26, p. 561; A. ROOSENDAAL, prev. cited, note 11, p. 4.
[39] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting and Cloud Computing", 2010, p. 10, online: <http://www.priv.gc.ca/resource/consultations/report_2010_e.pdf> (site consulted on January 20, 2012).
[40] *Id.*
[41] FEDERAL TRADE COMMISSION, BUREAU OF CONSUMER PROTECTION, "Online Profiling: A Report to Congress", 2000, p. 4, online: <http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf> (site consulted on November 25, 2011).

The information obtained through the use of cookies is utilized to create extremely detailed consumer profiles that provide an in-depth look at each individual[42]. The unbelievable detail with which these profiles are endowed results from the hoard of information available through cookies as well as other tracking tools. To begin with, data obtained through cookies is not only limited to a consumer's use of a single website at one particular moment, but is rather extended to his use of all the websites that are served by a particular ad network over a significantly long period of time[43].

Once collected, the user information contained within the cookie, as well as the "clickstream" information obtained through a user's use of various websites served by the same ad network[44], can be pooled together with other demographic and psychographic data that is available from third-party sources (such as from Internet Service Providers through their use of Deep Packet Inspection technology) or with information voluntarily supplied by the consumer himself (such as on his profile on a Social Network Website[45]), both of which will be discussed in further detail below[46]. This creates a rather detailed profile[47] of the consumer which ultimately makes it possible for ad networks "to predict the individual consumer's tastes, needs, and purchasing habits and enables the advertising companies' computers to make split-second decisions about how to deliver ads directly targeted to [a] consumer's specific interests"[48].

---

[42] Lori EICHELBERGER, "The Cookie Controversy: Cookies and Internet Privacy", online: <http://www.cookiecentral.com/ccstory/cc3.htm> (site consulted on September 6, 2012).
[43] FEDERAL TRADE COMMISSION, BUREAU OF CONSUMER PROTECTION, prev. cited, note 41, p. 5; *See also:* Janlori GOLDMAN, Zoe HUDSON, and Richard M. SMITH, "Privacy: Report on the Privacy Policies and Practices of Health Web Sites", January 2000, online: <http://www.chcf.org/~/media/MEDIA%20LIBRARY%20Files/PDF/P/PDF%20privacyexecsummary.pdf> (site consulted on September 5, 2012).
[44] FEDERAL TRADE COMMISSION, BUREAU OF CONSUMER PROTECTION, *Id.*, p. 6-8.
[45] *Id.*, p. 5; H. OSBORN NG, prev. cited, note 24, 371; *See also:* Daniel J. SOLOVE, *The Digital Person: Technology and Privacy in the Information Age*, New York, New York University Press, 2004.
[46] *Infra*, p. 17-31.
[47] *See:* Cynthia CHASSIGNEUX, *Vie privée et commerce électronique*, Montreal. Éditions Thémis, 2004, p. 24-44.
[48] FEDERAL TRADE COMMISSION, BUREAU OF CONSUMER PROTECTION, prev. cited, note 41, p. 5.

The creation of such consumer profiles has often been viewed as a privacy violation. It is upon this basis that a lawsuit was filed on January 27, 2000 against a company by the name of DoubleClick, one of the largest users of cookie technology for advertising purposes. This enterprise is basically an ad network that "is affiliated with over 11,000 Web sites for which and on which it provides targeted banner advertisements"[49], 1,500 sites of which produce the most traffic on the World Wide Web[50].

The chances of an Internet user coming across a site upon which DoubleClick has content is therefore rather significant and, as such, it is rare to find an individual's browser that does not possess a cookie emanating from this company. The users upon whose browsers the cookies are placed can be identified by the specific user ID attached to the cookie in question. These cookies generally contain a range of data including "names, e-mail addresses, home and business addresses, telephone numbers, searches performed on the Internet, Web pages or sites visited on the Internet and other communications and information that users would not ordinarily expect advertisers to be able to collect"[51].

Each time a user visits a site affiliated with DoubleClick, the consumer's browser is triggered to send a request to this company's network – a request which includes the user identifier of the cookie saved on that individual's computer as well as the browser type and the name of the websites associated with DoubleClick that the user is attempting to access[52]. At this point, the ad network identifies the consumer profile attached to the cookie's user identifier and then places advertisements upon the web page that the individual is viewing that most appeal to his interests.

---

[49] *Re DoubleClick Inc. Privacy Litigation*, 154 F. Supp. 2d 497, online: <http://cyber.law.harvard.edu/is02/readings/doubleclick.html> (site consulted on October 22, 2012).
[50] *Id.*
[51] *Id.*; *See also*: Ashkan SOLTANI, Shannon CANTY, Quentin MAYO, Lauren THOMAS and Chris Jay HOOFNAGLE, "Flash Cookies and Privacy", 2009, online: <http://ssrn.com/abstract=1446862> (site consulted on September 4, 2012).
[52] *Re DoubleClick Inc. Privacy Litigation*, prev. cited, note 49.

Due to the fact that DoubleClick is affiliated with such a significant number of websites, the profiles it is able to create tend to be rather detailed as it follows consumer behaviour across their use of these sites. As such, the advertisements it targets to individuals are often very well suited to their wants and needs. For example, if DoubleClick's client sells golf paraphernalia – a sport that is generally associated with wealthy individuals – the network will target this client's ads to "high-income people who follow golf and have a track record of making expensive online purchases"[53]. When the consumer fulfilling these criteria views this ad, it will often draw his attention, as it so directly appeals to his interests, causing him to click on it in most cases[54]. For the ad network, this means that their mission of targeting the consumer with advertisements relevant to his interests and desires has been successfully accomplished.

Despite the Plaintiffs' view that DoubleClick's creation of detailed consumer profiles violated their privacy, however, the United States District Court for the Southern District of New York ultimately dismissed the action following a lengthy analysis whereby they did not consider that DoubleClick's practices violated American federal laws[55]. Whether or not such practices would be prohibited by Canadian laws, on the other hand, will be discussed in further detail in the next part of this thesis.

Nevertheless, it is evident that the consumer information available to advertisers through the use of cookies is rather significant. However, while the accrual of the personal data of individuals through cookies is considerable, the nature of Web cookie technology puts the ability of marketers to utilize this information at risk. All Web cookies, whether they are first-party cookies or third-party cookies, are stored in a user's browser, thus providing users with the option to delete cookies should they so wish. This would

---

[53] *Re DoubleClick Inc. Privacy Litigation*, *Id.*
[54] FEDERAL TRADE COMMISSION, BUREAU OF CONSUMER PROTECTION, *Id.*
[55] WILEY REIN LLP, "DoubleClick, Inc. Wins Privacy Lawsuit – May Continue Shipping Cookies", April 2001, online: <http://www.wileyrein.com/publications.cfm?sp=articles&newsletter=4&id=2942> (site consulted on October 22, 2012).

ultimately render all the data contained within the cookies lost to the website or entity that shared the cookie with the user. Web cookies therefore require some sort of minimal participation on the part of users to be able to fulfill their purpose, thus providing the user with the choice of whether or not they want to enable cookies to store their personal data.

In response to this problem, another type of cookie was created that renders the user's choice regarding whether or not they want their browsing habits to be tracked entirely obsolete as options to control or delete them are usually absent or virtually impossible to find[56]. These types of cookies are commonly referred to as Flash cookies or zombie cookies, which fulfill the same purposes as Web cookies, but are rather stored on a user's hard drive instead of his browser[57], rendering them invisible to users[58]. Due to the difficulty of deleting Flash cookies, users are essentially stripped of the choice regarding whether or not they desire their movement on the Internet to be tracked[59]. Furthermore, not only are Flash cookies difficult to delete, but they also serve to recreate Web cookies that have already been deleted by a user[60], thus stripping users of the choice offered to them with regards to Web cookies by association.

The use of such cookies by some of the most prominent sites on the World Wide Web was documented by researchers at UC Berkeley in 2009[61], and includes the sites run by MTV, ESPN, MySpace, Hulu, ABC, NBC and Scribd, all of whose Flash cookies

---

[56] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, prev. cited, note 11.
[57] FEDERAL TRADE COMMISSION, "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers", December 2010, p. 66, online: <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf> (site consulted on January 20, 2011); Joey LOTT, Darron SCHALL, and Keith PETERS, *Actionscript 3.0 Cookbook*, Sebastopol, O'Reilly, 2006, p. 410; Den ODELL, *Pro JavaScript RIA Techniques: Best Practices, Performance, and Presentation*, Berkeley, Apress, 2009, p. 322.
[58] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, prev. cited, note 11; A. SOLTANI, S. CANTY, Q. M., L. THOMAS and C. J. HOOFNAGLE, prev. cited, note 51, p. 1.
[59] Seth SCHOEN, "New Cookie Technologies: Harder to See and Remove, Widely Used to Track You", September 14, 2009, online: <https://www.eff.org/deeplinks/2009/09/new-cookie-technologies-harder-see-and-remove-wide> (site consulted on September 4, 2012).
[60] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, prev. cited, note 11; A. SOLTANI, S. CANTY, Q. MAYO, L. THOMAS and C. J. HOOFNAGLE, prev. cited, note 51, p. 1.

emanate from a company called Quantcast[62]. As a result of their use of Flash cookies, a lawsuit was filed against these companies in the United States District Court of Central California on July 23, 2010 which was settled only a few months later. While this leaves us at a loss regarding the manner in which such a case would be treated in a court of law, Quantcast's immediate action to remedy this situation and preserve consumer privacy is most definitely an indication that advertising companies may agree that the use of such technology is invasive[63].

Regardless of the type of cookie that may be used by websites or ad networks, however, it is clear that this type of technology renders these entities privy to a significant amount of consumer information to which they would not otherwise have access. Thus, between the information contained about the user in the cookies issued by the websites he visited, as well as the cookies issued by the ad networks that serve these websites, a significant amount of information is able to be inferred about the consumer's preferences – information which is then used to target him with advertisements that would comply to his interests and that would mostly likely result in him clicking on the advertisement.

Subsection 2 Deep Packet Inspection

Deep Packet Inspection[64] is a networking technology that is also employed to aggregate data regarding Internet users. It is used by both businesses and Internet Service Providers[65] to monitor network traffic as well as examine the information being transmitted

---

[61] *See:* A. SOLTANI, S. CANTY, Q. MAYO, L. THOMAS and C. J. HOOFNAGLE, *Id.*
[62] Ryan SINGEL, "Privacy lawsuit Targets Net Giants Over 'Zombie' Cookies", July 27, 2010, online: <http://www.wired.com/threatlevel/2010/07/zombie-cookies-lawsuit/> (site consulted on October 22, 2012).
[63] QUANTCAST, "Reaffirming Our Commitment to Consumer Choice and Control", December 4, 2010, online: <http://www.quantcast.com/inside-quantcast/2010/12/reaffirming-our-commitment-to-consumer-choice-and-control/> (site consulted on September 22, 2012).
[64] Hereafter referred to as "DPI".
[65] Hereafter referred to as "ISP".

by users throughout the Internet[66]. DPI technology was created to protect ISPs from threats inherent to the Web, such as viruses and spam email, which have the ability to affect its proper functioning[67]. However, while permitting them to protect themselves from such threats, this form of technology also renders it possible for ISPs to collect all the communications made by consumers over the Internet[68] and ultimately "monitor, analyze, and potentially manipulate Internet traffic"[69].

DPI technology functions by collecting information viewed by consumers on the Internet – data which flows through the Web in the form of packets[70]. Packets are often compared to mailed letters in that each one contains both a header, which is akin to an address that directs the packet to its final destination in the same way as an address placed on an envelope directs that mail to a particular domicile, as well as payload data, which holds the actual content detained within the packet similarly to the letter found within the envelope[71]. The only distinction between the contents of a packet and a letter is that, while

---

[66] A. DALY, prev. cited, note 11, p. 2; Christopher PARSONS, "Literature Review of Deep Packet Inspection: Prepared for the New Transparency Project's Cyber-Surveillance Workshop", March 6, 2011, p. 3, online: <http://www.christopher-parsons.com/blog/wp-content/uploads/2011/04/Parsons-Deep_packet_inspection.pdf> (site consulted on November 24, 2011).

[67] Ralf BENDRATH, "Global technology trends and national regulation: Explaining Variation in the Governance of Deep Packet Inspection", February 2009, p. 16, online: http://userpage.fu-berlin.de/bendrath/ISA09_Paper_Ralf%20Bendrath_DPI.pdf> (site consulted on September 6, 2012); A. DALY, *Id.*, p. 3; Christopher PARSONS, "Deep Packet Inspection: Privacy, Mash-ups, and Dignity", March 2010, p. 12, online: <http://www.christopher-parsons.com/Academic/Deep_Packet_Inspection-Privacy_Mash-ups_and%20Dignities_1.0(for%20web).pdf> (site consulted on January 20, 2012); Anderson RAMOS, "Deep Packet Inspection Technologies", in Harold F. TIPTON and Micki KRAUSE (dir.), *Information Security Management Handbook*, 6th ed., vol. 3, New York, Auerbach Publications, 2009, 2195, at page 2195-2196.

[68] Tim HILLS, "Deep Packet Inspection", December 14, 2006, online: http://www.lightreading.com/document.asp?doc_id=111404> (site consulted on September 6, 2012); A. N. PERSON, prev. cited, note 11, 438; Kevin WERBACH, "Breaking the Ice: Rethinking Telecommunications Law for the Digital Age", (2005) 4 *J. Telecomm. & High Tech. L.* 59, 92.

[69] A. N. PERSON, *Id.*; *See also:* Danielle Keats CITRON, "The Privacy Implications of Deep Packet Inspection", online: http://dpi.priv.gc.ca/index.php/essays/the-privacy-implications-of-deep-packet-inspection/> (site consulted on September 6, 2012).

[70] A. DALY, prev. cited, note 11, p. 3; C. PARSONS, prev. cited, note 66, p. 3; A. N. PERSON, prev. cited, note 11, 438.

[71] P. OHM, prev. cited, note 34, 1453; C. PARSONS, *Id.*, p. 3; A. N. PERSON, *Id.*, 438; Gigi B. SOHN, "Hearing on Broadband Providers and Consumer Privacy Before the U.S. Senate Committee on Commerce, Science,

reading the latter provides sufficient information about an individual, the former is rarely useful unless it is combined with the data contained in the other packets emanating from the same individual's device at a given time as online communications are often subdivided into several packets upon transmission[72].

The payload data contained within each packet can range from information regarding web browsing habits, to the content contained in emails or information transfers, and even to what was said during voice conversations held over the Internet[73] – all of which is made available to ISPs through DPI technology. The amount of information available to ISPs will, however, differ depending on the type of DPI technology employed[74]. Some DPI technologies render it possible to track all information going to, and leaving from, a specific Internet Protocol address[75], while pinpointing and accessing any type of information desired[76]. Such technology would render it possible to identify traffic leading to and from a particular user's email account, and even allow for the possibility of reassembling an email message as it is being typed out by the user[77].

---

and Transportation", September 25, 2008, p. 3, online: <http://www.publicknowledge.org/pdf/gbsohn-testimony-20080925.pdf> (site consulted on September 6, 2012).

[72] ABOUT.COM, "Packet", 2012, online: <http://compnetworking.about.com/od/networkprotocols/l/bldef_packet.htm> (site consulted on November 7, 2012).

[73] A. N. PERSON, prev. cited, note 11, 438; P. OHM, prev. cited, note 36, 1438-1439.

[74] Nate ANDERSON, "Deep packet inspections meets 'Net neutrality, CALEA", July 26, 2007, online: <http://arstechnica.com/hardware/news/2007/07/Deep-packet-inspection-meets-net-neutrality.ars> (site consulted on January 20, 2012); A. N. PERSON, *Id.*, 439.

[75] An Internet Protocol address "is a code made up of numbers separated by three dots that identifies a particular computer on the Internet. Every computer […] requires an [Internet Protocol] address to connect to the Internet." (TECHTERMS, "IP Address", 2012, online: <http://www.techterms.com/definition/ipaddress> (site consulted on September 10, 2012)) (Hereafter referred to as "IP address").

[76] N. ANDERSON, prev. cited, note 74; C. PARSONS, prev. cited, note 67, p. 13; A. N. PERSON, prev. cited, note 11, 439.

[77] N. ANDERSON, *Id.*; Christopher PARSONS, "Moving Across the Internet: Code-Bodies, Code-Corpses, and Network Architecture", 2010, online: <http://www.ctheory.net/printer.aspx?id=642> (site consulted on September 7, 2012); A. N. PERSON, *Id.*, 439; *See also:* Ralf BENDRATH and Milton MUELLER, "The End of the Net as we know it? Deep Packet Inspection and Internet Governance", August 4, 2010, p. 4, online: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1653259> (site consulted on September 7, 2012), about how the scanning of information accomplished by the use of Deep Packet Inspection takes place in real time.

Other DPI technology, on the other hand, is not nearly as invasive, only being used to recognize trends in user behaviour by analyzing their use of the Internet based on the queries they make, the content they download and the applications they use. Regardless of the type of DPI technology employed, however, it is clear that this type of technology basically makes it possible for any information being transmitted over the Internet to be visible to uninvolved third parties thus allowing them to gain access to more detailed information regarding Internet users[78].

Thus, contrary to cookies, DPI technology is not an element that is shared between a user's computer and a website's or ad network's server, but is rather an elaborate system set up by the product's developer in collaboration with an ISP[79]. DPI is a great deal more dynamic[80] and is actually able to track everything a user is doing on the Internet, as opposed to only specific pre-programmed elements[81]. The information acquired through DPI by intercepting, copying and reading packets of Internet traffic thus render ISPs privy to hoards of information regarding consumer online activities and communications[82]. In addition, ISPs have access to all the Internet users that make use of their services. Thus, rather than requiring a user to go on a specific website so that a cookie may be stored in his browser or hard drive, allowing information to be collected about him, ISPs can gather information about Internet users simply through the use of their services[83].

---

[78] R. BENDRATH, prev. cited, note 67, p. 12-15; R. BENDRATH and M. MUELLER, *Id.*, p. 3-6; D. K. CITRON, prev. cited, note 69; A. DALY, prev. cited, note 11, p. 5-6; J. LO, prev. cited, note 11, p. 34-42; P. OHM, prev. cited, note 36, 1438-1439; C. PARSONS, prev. cited, note 67, 11-14; C. PARSONS, *Id.*; A. N. PERSON, *Id.*
[79] A. DALY, *Id.*, p. 6; J. LO, *Id.*, p. 34; A. N. PERSON, *Id.*, 441-442.
[80] R. BENDRATH, prev. cited, note 67, p. 12-15; R. BENDRATH and M. MUELLER, prev. cited, note 77, p. 3-6; D. K. CITRON, prev. cited, note 69; A. DALY, *Id.*, p. 5-6; J. LO, *Id.*, p. 34-42; P. OHM, prev. cited, note 36, 1438-1439; C. PARSONS, prev. cited, note 67, 11-14; C. PARSONS, prev. cited, note 77; A. N. PERSON, *Id.*, 442.
[81] A. DALY, *Id.*, p. 6.
[82] R. BENDRATH, prev. cited, note 67, p. 12-15; R. BENDRATH and M. MUELLER, prev. cited, note 77, p. 3-6; D. K. CITRON, prev. cited, note 69; A. DALY, *Id.*, p. 5-6; J. LO, prev. cited, note 11, p. 34-42; P. OHM, prev. cited, note 36, 1438-1439; C. PARSONS, prev. cited, note 67, 11-14; C. PARSONS, prev. cited, note 77.
[83] A. DALY, *Id.*, p. 6; A. N. PERSON, prev. cited, note 11, 442.

The utilization of this type of technology by two different companies, Phorm and NebuAd, met with severe criticism. To begin with, Phorm, an advertising company, signed agreements with three of United Kingdom's largest ISPs whereby it would install its advertising system and apply it to the clients of these providers[84]. The advertising system used DPI technology to intercept all of the web pages viewed by the customers of these ISPs and scan them all for keywords[85], while at the same time tracking them throughout the World Wide Web using cookies assigned with user identifiers[86]. A customer profile would be constructed using the keywords that appear with a high frequency on these Web pages, and would be constantly updated simultaneously to his use of the Internet[87]. This data was then utilized by Phorm to target these individuals with advertisements on websites that also possess agreements with the advertising company[88]. In such a manner, if a customer was found searching for exotic summer getaways, Phorm would be aware of this and they would then target these individuals with advertisements for hotels in destinations like Hawaii or Fiji, for example[89].

It was revealed in April 2008 that Phorm deployed its DPI technology for trial purposes on tens of thousands of individuals without their knowledge or consent, which led to quite an uproar[90]. Their unauthorized use of this technology was severely criticized,

---

[84] Christopher WILLIAMS, "BT and Phorm: how an online privacy scandal unfolded", April 8, 2011, online: <http://www.telegraph.co.uk/technology/news/8438461/BT-and-Phorm-how-an-online-privacy-scandal-unfolded.html> (site consulted on October 22, 2012).
[85] *Id.*; Richard CLAYTON, "The Phorm "Webwise" System", May 18, 2008, online: <http://www.cl.cam.ac.uk/~rnc1/080518-phorm.pdf> (site consulted on October 22, 2012); EDRI-GRAM, "UK: Phorm Targeted Advertising Practices – Under Pressure", March 26, 2008, online: <http://www.edri.org/edrigram/number6.6/phorm-uk-ifpr> (site consulted on October 22, 2012); J. LO, prev. cited, note 11, p. 38.
[86] J. LO, *Id.*
[87] C. WILLIAMS, prev. cited, note 84.
[88] EDRI-GRAM, prev. cited, note 85; J. LO, prev. cited, note 11, p. 38; C. WILLIAMS, *Id.*
[89] C. WILLIAMS, *Id.*
[90] Arnaud DEVILLARD, "Affaire Phorm: Bruxelles demande des comptes au Royaume-Uni, La Commission européenne a ouvert une procédure d'infraction, à l'origine de laquelle se trouve une technologie de ciblage comportemental appelée Phorm", April 15, 2009, online: <http://www.01net.com/editorial/501173/affaire-phorm-bruxelles-demande-des-comptes-au-royaume-uni/> (site consulted on October 22, 2012); EUROPEAN UNION, "Telecom: Commission launches case against UK over privacy and personal data protection", April

causing the European Commission to intervene following a lack of action on the part of British Authorities[91]. Phorm experienced what was described by one of the ISPs it was associated with as being "a year of the most intensive personal-reputation-destroying PR trench warfare" which ultimately resulted in the desertion of Phorm by its investors and partners and a crumbling of their company within the United Kingdom[92]. Rather than attempting to re-establish its reputation in that part of the world, Phorm is now endeavouring to create a new name for itself in Turkey, China and Brazil[93].

Even closer to home is the case of the American company NebuAd who partnered with American, and even some Canadian, ISPs to access the data they acquire through the use of DPI in order to be able to use that data for the behavioural advertising technology that NebuAd developed[94]. The advertising company's technology functioned by amassing the information of the customers of the ISPs through installing a hardware device within the provider's network[95]. All the data that was acquired in this fashion was associated with the user's IP address, and all of the traffic emanating from a particular IP address was monitored and analyzed based on "the pages visited, the search terms entered, and the keywords that appear on those pages. This information [was] distilled to about 1000

14, 2009, online: <http://europa.eu/rapid/press-release_IP-09-570_en.htm?locale=en.> (site consulted on October 22, 2012); Christopher WILLIAMS, "BT and Phorm secretly tracked 18,000 customers in 2006: spied on, profiled and targeted for credit cards", April 1, 2008, online: <http://www.theregister.co.uk/2008/04/01/bt_phorm_2006_trial/> (site consulted on October 22, 2012);

[91] A. DEVILLARD, *Id.*; ZDNET FRANCE, « Vie privee et protection des données : la Commission européenne ouvre une procédure contre le Royaume Uni », April 15, 2009, online : <http://www.zdnet.fr/actualites/vie-privee-et-protection-des-donnees-la-commission-europeenne-ouvre-une-procedure-contre-le-royaume-uni-39392143.htm> (site consulted on October 22, 2012).

[92] C. WILLIAMS, prev. cited, note 84.

[93] DAILY RESEARCH NEWS ONLINE, "Phorm Approaches 'Defining Moment'", October 1, 2012, online: <http://www.mrweb.com/drno/news16166.htm> (site consulted on October 22, 2012); Georgia MANORS, "Phorm jumps after Turkey trial", October 16, 2012, online: <http://www.ifamagazine.com/news/phorm-jumps-after-turkey-trial/26159/> (site consulted on October 22, 2012).

[94] Stacey HIGGINBOTHAM, "NebuAd Bites The Dust", May 19, 2009, online: <http://gigaom.com/2009/05/19/nebuad-bites-the-dust/> (site consulted on October 23, 2012); Zachary RODGERS, "Questions for Bob Dykes, NebuAd CEO", January 3, 2008, online: <http://www.clickz.com/3628009> (site consulted on October 23, 2012).

categories representing various purchase interest: shopping for a mortgage, researching lawnmowers, and so on"[96]. The frequency with which a particular user viewed a specific web page was also examined by the advertising system. In such a manner, when a user "[visited] a Web page, NebuAd [could] check which categories the user [appeared] to be interested in and display a message from an advertiser interested in that sort of product"[97].

The practices of NebuAd were severely criticized by privacy advocates in the United States, which ultimately led to hearings being held in Congress regarding the potentially invasive technology developed and used by this company[98]. As a result of the less than flattering attention NebuAd was receiving, the ISPs with which it had partnerships reneged on their agreements. A class action lawsuit was later filed against NebuAd, for which it agreed to a $2.4 million settlement as well as to testify against the ISPs it was previously partnered with so that their testimony may be used in cases instituted against these entities[99]. The ill effects suffered by NebuAd as a result of all of this negative publicity ultimately led to the company being shut down on May 15, 2009[100].

---

[95] Saul HANSELL, "NebuAd Observes 'Useful, but Innocuous' Web Browsing", April 7, 2008, online: <http://bits.blogs.nytimes.com/2008/04/07/nebuad-observes-useful-but-innocuous-web-browsing/> (site consulted on October 23, 2012).
[96] *Id.*
[97] *Id.*
[98] Grant GROSS, "Senators question NebuAd, targeted ad privacy", July 9, 2008, online: <http://www.pcworld.com/article/148136/article.html> (site consulted on October 23, 2012); Peter WHORISKEY, "Internet Provider Halts Plan to Track, Sell Users' Surfing Data", June 25, 2008, online: < http://www.washingtonpost.com/wp-dyn/content/article/2008/06/24/AR2008062401033_pf.html> (site consulted on October 23, 2012).
[99] Wendy DAVIS, "NebuAd Settles Lawsuit Over Behavioral Targeting Tests", August 16, 2011, online <http://www.mediapost.com/publications/article/155980/> (site consulted on October 23, 2012).
[100] Nate ANDERSON, "NebuAd loses CEO, business model in wake of tracking furor", September 5, 2008, online: http://arstechnica.com/techpolicy/news/2008/09/nebuad-loses-ceo-business-model-in-wake-of-tracking-furor.ars (site consulted on October 23, 2012); Wendy DAVIS, "Case Close: NebuAd Shuts Down", May 18, 2009, online: <http://www.mediapost.com/publications/article/106277/> (site consulted on October 23, 2012).

Subsection 3 Social Network Websites: Consumer Profiles

Social Network Websites[101] are yet another one of the tools employed by online marketers to gather consumer data. These sites are web-based services that permit individuals to create personal profiles[102] which they use to connect with other people, be it their friends, acquaintances, or simply individuals who possess profiles that are of interest to them[103]. Most SNWs are made up of various user profiles, often consisting of a picture of the user, and containing personal data which typically includes his name, date of birth and location, as well as a section where the user can provide more detailed information about himself, such as his education or personal preferences[104]. This data is rendered available to other users on the network and permits them to identify their friends and add them to a list of contacts[105]. This ultimately leads to the creation of online communities where people can share user created content[106].

Users of SNWs keep in contact with their friends and acquaintances through the use of these profiles by befriending them on these sites and connecting with them. Connections between users on such sites are enabled through mechanisms provided by SNWs that allow users to leave publicly visible comments or even send private messages[107]. It is also possible for users to connect with one another by displaying their interests, their likes, their

---

[101] Hereafter referred to as "SNW".
[102] Daniel CARON, "Privacy, Social Networking Sites, and the Canadian Approach: Protecting a Pluralistic Conception of Privacy Through Principle-Based Regulation", May 20, 2010, online: <http://www.priv.gc.ca/speech/2010/sp-d_20100520_dc_e.cfm> (site consulted on August 8, 2011).
[103] Caroline HAYTHORNTHWAITE, "Social Networks and Internet Connectivity Effects", (2005) 8-2 *Information, Communication & Society* 125, 136-138; Pierre TRUDEL, *Introduction à la Loi concernant le cadre juridique des technologies de l'information*, Cowansville, Éditions Yvon Blais, 2012, p. 204.
[104] Danah M. BOYD and Nicole B. ELLISON, "Social Network Sites: Definition, History, and Scholarship", (2008) 13 *Journal of Computer-Mediated Communication* 210, 211-213; Marc FANELLI-ISLA, *Guide pratique des réseaux sociaux: Twitter, Facebook…des outils pour communiquer*, Paris, Dunod, 2010, p. 18; P. TRUDEL, *Id.*
[105] Marc FANELLI-ISLA, *Id.*; Vala Ali ROHANI and Ow Siew HOCK, "On Social Network Web Sites: Definition, Features, Architectures and Analysis Tools", (2010) 2 *Journal of Advances in Computer Research* 41, 42; P. TRUDEL, *Id.*
[106] V. A. ROHANI and O. S. HOCK, *Id.*, 43; Won KIM, Ok-Ran JEONG and Sang-Won LEE, "On Social Web Sites", (2010) 35-2 *Information Systems Journal* 215, 216-217.

dislikes, and various other elements that further describe them as a person[108]. The data available about individuals on SNWs is therefore nearly unlimited.

Aside from connecting with individuals with whom the user is acquainted, a good number of SNWs enable various other elements that permit users to enhance their social experience on the Web. In the cases of many such sites, this is achieved through allowing users to interact with various applications such as games, birthday calendars, trivia applications and countless others[109]. One of the most popular SNWs, Facebook, even extends the social experience of its users beyond its own website and onto other sites. It achieves this by enabling social enhancement tools known as "social plug-ins" which can be incorporated into a website and ultimately allow users to share their opinions regarding various websites with their Facebook friends[110].

The various connections and relationships formed between users in such a fashion results in the creation of a marketing tool known as the Social Graph, which is essentially a public display of connections linking people to one another based on their associations with each other[111], thus providing "rich sources of naturalistic behavioral data"[112]. The

---

[107] M. FANELLI-ISLA, prev. cited, note 104, p. 17-18.
[108] *Id.*, p. 20
[109] D. M. BOYD and N. B. ELLISON, prev. cited, note 104, 213.
[110] *See :* Abdelberi CHAABANE, Mohamed Ali KAAFAR and Roksana BORELI, "Big Friend is Watching You: Analyzing Online Social Networks Tracking Capability", August 17, 2012, p. 8, online: <http://conferences.sigcomm.org/sigcomm/2012/paper/wosn/p7.pdf> (site consulted on September 7, 2012); FACEBOOK DEVELOPERS, "Social Plugins", 2012, online: <http://developers.facebook.com/docs/plugins/> (site consulted on September 10, 2012); A. ROOSENDAAL, prev. cited, note 11.
[111] Michael BEYE, Arjan JECKMANS, Zekeriya ERKIN, Pieter HARTEL, Reginald LAGENDIJK and Qiang TANG, "Literature Overview - Privacy in Online Social Networks", 2010, p. 3, online: <http://doc.utwente.nl/74094/1/literaturereview.pdf> (site consulted on January 29, 2012); Julia HEIDEMANN, Mathias KLIER and Florian PROBST, "Identifying Key Users in Online Social Networks: A PageRank Based Approach", December 2010, p. 3-4, online: <http://www.wi-if.de/paperliste/paper/wi-301.pdf> (site consulted on January 29, 2012); Romain RISSOAN, *Les réseaux sociaux – Facebook, Twitter, LinkedIn, Viadeo, Google+: Comprendre et maîtriser ces nouveaux outils de communication*, St-Herblain, Éditions ENI, 2011, p. 34-44.
[112] D. M. BOYD and N. B. ELLISON, prev. cited, note 104, 221.

connections linking individuals to one another that are exhibited in the Social Graph[113] can simply be based on the fact that they are acquainted with one another, but they can also be further pinpointed to demonstrate the various traits and interests people have in common[114].

More importantly than the functioning of SNWs, however, is the extreme popularity of these sites, which has seen a significant increase since 2004[115]. Facebook, for example, possesses over 687 million users[116] – an increase of 287 million since 2010[117] – and continues to grow each day. The part Facebook plays in our everyday lives is extremely significant, so much so that 48% of 18 to 34 year olds check their Facebook accounts the moment they awaken in the morning[118]. With the number of consumers connected to SNWs, the user data available through this medium is therefore tremendously extensive.

The data that can be accessed about users through the use of SNWs, however, is not solely limited to their behaviour on the website itself, but is also expanded to the users' use of the Internet as a whole. One of the most refined methods of modern day technology is tracking users across the Internet with the use of social plug-ins emitted by SNWs. Though the extensive ability of cookies emanating from ad networks to track users is rather impressive, as demonstrated above[119], the tentacles of cookies emitted by social plug-ins reach far beyond those originating from ad networks.

---

[113] Joseph BONNEAU, Frank STAJANO, Jonathan ANDERSON and Ross ANDERSON, "Eight Friends Are Enough: Social Graph Approximation via Public Listings", 2009, p. 1, online: <http://www.cl.cam.ac.uk/~jcb82/doc/BASA09-SNS-eight_friends.pdf> (site consulted on January 29, 2012).
[114] John BRESLIN and Stefan DECKER, "The Future of Social Networks on the Internet: The Need for Semantics", (2007) 11-6 *IEEE Internet Computing* 86, 87.
[115] D. CARON, prev. cited, note 102.
[116] CBC NEWS, "Facebook use drops in Canada, U.S.", June 13, 2011, online: <http://www.cbc.ca/news/technology/story/2011/06/13/facebook-users-drop.html> (site consulted on January 20, 2012).
[117] Aden HEPBURN, "Facebook: Facts and Figures for 2010", March 22, 2010, online: <http://www.digitalbuzzblog.com/facebook-statistics-facts-figures-for-2010/> (site consulted on January 20, 2012).
[118] Aden HEPBURN, "Facebook Statistics, Stats & Facts for 2011", January 18, 2011, online: <http://www.digitalbuzzblog.com/facebook-statistics-stats-facts-2011/> (site consulted on January 20, 2012).
[119] *Supra*, p. 10-17.

Some of the most widely spread social plug-ins are those offered by Facebook, which are often incorporated on numerous websites throughout the Internet. One of the most popular social plug-ins is Facebook's "Like" button, which is depicted by a thumbs-up image along with the word "like"[120]. This button, which can be freely integrated into a website, enables Facebook users to demonstrate that they like a given web page by clicking on the "Like" button – information which will then appear as a link on their friends' news feed, allowing them to share this information with their friends, and ultimately holding a permanent place on the user's own Facebook profile[121].

Despite the versatility of the "Like" button, however, this seemingly innocent plug-in is used to place cookies, analogous to third-party cookies[122], on the browsers of those people who frequent the websites who incorporate the "Like" button – whether or not they actually click on the button[123]. This ultimately allows Facebook to collect information about these individuals by tracking and tracing their movement across any and all websites containing this button, which has, up to date, reached a total of 2.5 million websites – a number which is steadily increasing by about 10,000 sites each day[124]. The amount of information regarding user browsing habits that is available to this company through the "Like" button is thus tremendously extensive. Furthermore, while the data collected is generally traced back to an individual's Facebook account, a person does not forcibly require such an account for information to be collected about him in this manner[125].

---

[120] FACEBOOK DEVELOPERS, "Like Button", 2012, online: <http://developers.facebook.com/docs/reference/plugins/like/> (site consulted on September 7, 2012).
[121] *Id.*
[122] A. ROOSENDAAL, prev. cited, note 11, p. 4;
[123] Yasamine HASHEMI, "Note – Facebook's Privacy Policy and its Third-Party Partnerships : Lucrativity and Liability", (2009) 15 *B. U. J. Sci. & Tech. L.* 140, 144.
[124] Josh CONSTINE, "Facebook Celebrates the Like Button's 1st Birthday By Showing Off Its Footprint", April 21, 2011, online: <http://www.insidefacebook.com/2011/04/21/like-button-birthday/> (site consulted on January 29, 2012).
[125] A. CHAABANE, M. A. KAAFAR and R. BORELI, prev. cited, note 110, p. 8; Y. HASHEMI, prev. cited, note 123, 147; A. ROOSENDAAL, prev. cited, note 11, p. 2.

The manner in which Facebook functions to collect information about individuals in this fashion will, however, differ depending on whether or not the individual in question possesses a Facebook account. Those users who possess Facebook accounts are issued a cookie with a unique user ID which identifies a particular user throughout the Internet. As a result, similarly to ad networks who access the cookie that it already shares with an individual whenever he frequents a site served by the network in question, each time the user either logs onto the Facebook website or goes onto a site that has incorporated Facebook content such as the "Like" button, the cookie is accessed and information concerning the user is immediately sent back to Facebook even if the individual did not actually click on the button and regardless of whether or not he happens to be logged on to Facebook at the time[126]. This therefore enables Facebook to collect a significant amount of information regarding the browsing habits of Facebook account holders, especially considering the proliferation of the "Like" button throughout the Internet[127].

When a person does not possess a Facebook account, on the other hand, there is no cookie with a unique user ID that specifically identifies him, and the "Like" button does not emit cookies simply by being incorporated into a website. However, another one of Facebook's social plug-ins, known as the Facebook Connect button, which allows users to connect to a particular site through their Facebook account, *does* issue a cookie to those who are not account holders. As a result, from the moment in which an individual browses through a site which contains the Connect button, they will be identified by this entity in the future, and each time they visit a website with the "Like" button, or any other Facebook content, data regarding the individual's browsing history will be accessible to Facebook[128].

---

[126] Y. HASHEMI, *Id.*, 149.
[127] Josh CONSTINE, "Facebook Says "Likers" Click Links To External Websites 5.4x More", September 29, 2010, online: <http://www.insidefacebook.com/2010/09/29/facebook-stats-likers/> (site consulted on January 20, 2012).
[128] A. ROOSENDAAL, prev. cited, note 11, p. 5-6.

The possibility of an individual browsing a site that contains the Facebook Connect application, causing him to ultimately end up sharing a cookie with this entity, is actually quite considerable. Two years following its launch by Facebook, the Connect button was incorporated into over two million sites – a number which is increasing exponentially[129]. Many of the sites which integrate Facebook Connect are frequently utilized by Internet users for practical purposes, such as www.canada411.ca, where individuals often search for the telephone numbers of businesses or individuals. The possibility of obtaining information regarding the browsing habits of individuals who do not possess a Facebook account is therefore quite substantial, simply due to the extensive incorporation of the Facebook Connect button into websites throughout the Internet.

An individual who does not possess a Facebook account, and has his information gathered in the above described manner, but later decides to sign up to Facebook, will find all the data previously collected about him linked to the new cookie with the unique user ID issued by Facebook upon the opening of his new account[130]. What happens is that, when this individual takes the necessary steps to open a Facebook account, the site will issue a cookie with a unique user ID to this new user, and the cookie in question will make the connection with the cookie previously issued by Facebook, thus ensuring that this entity does not lose all the data it has already collected about the individual in question[131].

Facebook, however, does not stop merely at tracking users through cookies on the browsers of their desktop computers; in the event that a user connects to this website through the use of his laptop or smart phone, these devices are recognized as belonging to that particular individual[132]. Facebook is therefore able to track users in their daily routines by being connected to these individuals through devices they use on a constant basis. This

---

[129] *Id.*, p. 5; Jennifer VAN GROVE, "Each Month 250 Million People Use Facebook Connect on the Web", December 8, 2010, online: <http://mashable.com/2010/12/08/facebook-connect-stats/> (site consulted on January 29, 2012).
[130] A. CHAABANE, M. A. KAAFAR and R. BORELI, prev. cited, note 110, p. 8; A. ROOSENDAAL, *Id.*, p. 6.
[131] A. CHAABANE, M. A. KAAFAR and R. BORELI, *Id.*; A. ROOSENDAAL, *Id.*

ultimately results in the creation of very personalized profiles of these people, allowing the site to cater to their desires by targeting them with advertisements that are of particular interest to them[133]. This SNW thus achieves the same goal as ad networks, but due to its proliferation, it has a much farther reach.

Facebook is not the only entity that provides social plug-ins on other websites, however. As for other plug-ins, such as Twitter's Tweet button, the Digg button, and Google's Buzz, their reach is not as extensive as that of Facebook[134]. The reason for this is because they function differently. The Digg button and Google's Buzz, for example, do not possess a plug-in like the Facebook Connect button that can automatically issue a cookie to an individual without that person possessing an account on their site, therefore limiting their access solely to members of their websites[135]. Twitter, on the other hand, only issues cookies to those individuals who have visited their homepage[136]. Otherwise, this entity only has access to individuals who actually possess accounts on their site[137]. Regardless of which SNW's reach is greater, however, it is quite clear that cookies are extremely versatile, and their ability to gather data about individuals is quite extensive.

While the plug-ins issued by SNWs emit cookies that have the ability to determine a rather significant amount of information about Internet users, this is not the only tool available to marketers through these types of sites that enrich them with this kind of data; the Social Graphs created by these types of websites also serve to provide information about individuals, but rather with regards to their entire social network. These graphs

---

[132] A. ROOSENDAAL, *Id.*
[133] A. ROOSENDAAL, *Id.*, p. 7; *See also:* Y. HASHEMI, prev. cited, note 123; Kristen E. MARTIN, "Facebook (A): Beacon and Privacy", p. 5-6, <http://www.darden.virginia.edu/corporate-ethics/pdf/Facebook%20_A_business_ethics-case_bri-1006a.pdf> (site consulted on September 7, 2012).
[134] K. E. MARTIN, *Id.*, p. 3; Jeremiah OWYANG, "Web Strategy Matrix: Google Buzz vs Facebook vs MySpace vs Twitter", February 2010, online: <http://www.web-strategist.com/blog/2010/02/11/matrix-buzz-vs-facebook-vs-myspace-vs-twitter-feb-2009/> (site consulted on September 7, 2012); A. ROOSENDAAL, *Id.*
[135] A. ROOSENDAAL, *Id.*
[136] *Id.*; TWITTER, "Twitter Privacy Policy", May 17, 2012, online: <https://twitter.com/privacy> (site consulted on September 7, 2012).
[137] A. ROOSENDAAL, *Id.*; TWITTER, *Id.*

demonstrate an individual's connections based on elements that he has in common with his friends and acquaintances, thus providing marketers with access, not only to information about that particular individual, but also about all of the friends that are included in this person's Social Graph – whether or not this person's friends consent to this use of their information[138]. As such, even if marketers do not directly have access to the information of the person's friends, a quick analysis of his Social Graph will demonstrate the elements he has in common with his acquaintances and thus provide marketers with data that will allow them to infer the preferences of these individuals as well.

Furthermore, in addition to the data that is available to marketers through the Social Graph, they may also be in the position of viewing more excessive amounts of information on the profiles of individuals based on the degree to which the user enables his profile to be visible to third parties. Essentially, depending on the SNW in question, the visibility of user profiles will differ. Some websites make user profiles visible to everyone, whether they are connected to that network or not, while others only permit users who have befriended one another on the website to view each other's profiles but leave information such as name and the photo of the individual publicly available, while others still, leave the user with the choice of whether or not he would like his profile to be made public or remain private[139]. In cases where visibility is enabled, marketers thus possess access to a great deal of information that can aid them in determining the preferences of consumers.

* * *

Online tracking tools are therefore extremely efficient in their ability to determine large amounts of data regarding the desires and interests of Internet users, which is then utilized by marketers to target these users with advertisements that fit those preferences. While the use of these tools may be extremely beneficial to marketers as they enable them

---

[138] J. HEIDEMANN, M. KLIER and F. PROBST, prev. cited, note 111, p. 3-5.
[139] D. M. BOYD and N. B. ELLISON, prev. cited, note 104, 213.

to better circumscribe their audience, they do present certain implications with regards to privacy protection that we will address in further detail in the next part of this thesis[140].

Despite the privacy issues with respect to the use of such tools to aggregate user information, however, marketers do not often stop at collecting information regarding the personal preferences of users by tracking them online. While this form of tracking can be efficiently used to advertise to individuals while they surf the Web, it can prove to be even more successful should the information acquired through online tracking tools be used to provide individuals with location-specific advertisements that appeal to their interests on their cellular telephones. The next section of this chapter will therefore be dedicated to a thorough discussion of mobile advertising.

Section 2 Tracking in the Physical World: Mobile Advertising

Similarly to online behavioural tracking tools, there exist certain tools that enable consumers to be tracked throughout the physical world[141]. These are employed to follow the daily habits of consumers, ultimately using both their location and any data relative to the establishments they frequent in order to target them with advertisements on their Internet enabled cellular telephones based on this information – a practice known as mobile advertising. This section will thus be dedicated to providing a detailed description of the various mobile tracking tools that render it possible to track and target consumers in such a fashion, namely (1) GPS, (2) Signal Triangulation Systems and Wi-Fi Positioning Systems and (3) Location-Based Social Networks, in light of the manner in which these tools are used to efficiently market to consumers.

---

[140] *Infra*, p. 62-116.

[141] *See:* Alain CORPEL and Marc LEMERCIER, "Traces numériques des smartphones: De l'investigation à la protection de la vie privée", 2001, online : <http://www.lifl.fr/ict/fichiers/1.pdf> (site consulted on September 7, 2012).

Subsection 1 Global Positioning Systems

Nearly all cellular telephones in the present day and age are equipped with Global Positioning Systems[142], which render it possible for the geographic position of individuals to be pinpointed anywhere around the globe within 3 metres[143]. GPS makes use of 24 different satellites that orbit the earth and serve to broadcast precise time signals[144]. In practice, these signals are transmitted between the various satellites and the global positioning chips contained in mobile phones, calculating the amount of time it takes for these signals to travel between these two points[145]. The determination of the point of convergence of four different satellite signals received simultaneously permits the cellular telephone's three-dimensional location to be calculated almost precisely[146], ultimately rendering it possible to pinpoint the various movements of the owner of that particular phone on a daily basis[147].

This particular tool for tracking individuals is used by Nimbuzz, a mobile instant messaging and voice over IP company, which is becoming increasingly popular with 100 million users worldwide as at August 2, 2012, seeing an increase of 50 million users since the previous year[148]. Nimbuzz is a free application that "is available across all major platforms such as Symbian, iPhone, iPod touch, Android, BlackBerry, J2ME, as well as on

---

[142] Hereafter referred to as "GPS".
[143] Kristen E. EDMUNDSON, "Global Position System Implants: Must Consumer Privacy Be Lost in order for People to Be Found?", (2005) 38 *Ind. L. Rev.* 207, 209; N. J. KING, prev. cited, note 12, 254-255; NOTE: "Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators", (2004) 18-1 *Harv. J.L. & Tech.* 307, 308; A. A. OTTENBERG, prev. cited, note 12, 665.
[144] A. A. OTTENBERG, *Id.*; Aaron STROUT and Mike SCHNEIDER, *Location Based Marketing for Dummies*, Hoboken, John Wiley & Sons, 2011, p. 228.
[145] Alfred VILLOCH III, "Europe's Mobile Opportunity: Can the European Union Legislate Consumer Trust and Compete in the E-Commerce Market with the United States?", (2002) 20 *Penn. St. Int'l L. Rev.* 439, 448-449.
[146] *Id.*
[147] NOTE: "Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators", prev. cited, note 143, 308.
[148] NIMBUZZ! BLOG, "We have hit 100 Million users mark! Thank you guys :)", August 2, 2012, online: <http://blog.nimbuzz.com/2012/08/02/we-have-hit-100-million-users-mark-thank-you-guys/> (site consulted on October 23, 2012).

Windows and Mac desktop computers and enables users to enjoy free chatting, mobile [and] video calls, […] instant messaging and social networking"[149]. Through its application, this company provides location-based advertising services by tracking an individual's location through the GPS embedded in his mobile device and then targeting him with ads relative to his physical position as well as his personal preferences to better appeal to his desires and ensure that the ads presented to him are relevant[150].

Alternatively, GPS is also utilized for mobile advertising purposes by creating geo-fences, which is the formation of geographical boundaries utilizing global positioning technology that "[allows] an administrator to set up triggers so when a device crosses a geofence and enters the boundaries defined by the administrator, [a text message] or email alert is sent"[151]. This particular technology is one of the tracking tools utilized by the cellular telephone service provider, O2 Media, for its location-based advertising services[152]. The telecommunications company in question contracts with various businesses and ultimately serves advertisements on their behalf onto the mobile devices of over one million of O2's clients who opted in to the service[153]. Amongst the numerous entities to sign agreements with O2 are Starbucks and L'Oreal. The customers of the telecommunications company that demonstrate an interest in food and drink will receive a text message on their cellular telephone when they enter Starbucks' geo-fenced areas,

---

[149] Apurva CHAUDHARY, "Nimbuzz to Offer Location Based Advertising On Mobile App", April 20, 2012, online: <http://www.medianama.com/2012/04/223-nimbuzz-location-based-ads/> (site consulted on October 23, 2012).
[150] Alap NAIK DESAI, "Nimbuzz Reveals Insights About Mobile Based Advertising", July 30, 2012, online: <http://www.watblog.com/2012/07/30/nimbuzz-reveals-insights-about-mobile-based-advertising/> (site consulted on October 23, 2012).
[151] Margaret ROUSE, "Geofencing", January 2011, online <http://whatis.techtarget.com/definition/geofencing> (site consulted on October 23, 2012).
[152] O2 MEDIA, "Location Based Messaging: Connect with your customers when they are exactly where you want them!", online: <http://o2media.ie/location-based-messaging.html> (site consulted on October 23, 2012).
[153] Sarah SHEARMAN, "Starbucks trials 02 location-based mobile marketing service", October 15, 2010, online: <http://www.brandrepublic.com/news/1035146/> (site consulted on October 18, 2012); Neil TURNER, "O2 enters the location-based deals arena", July 15, 2011, online: <http://www.dma.org.uk/news/o2-enters-locationbased-deals-arena> (site consulted on October 23, 2012).

offering them a discount in the event that they purchase a beverage[154]. The agreement signed with L'Oreal, on the other hand, involved the United Kingdom pharmacy chain Superdrug that carries L'Oreal beauty products[155]. Similarly to the case of Starbucks, customers interested in beauty and hair care products will be targeted with a text message regarding L'Oreal's merchandise when they enter Superdrug's geo-fenced areas, offering them a buy-one-get-one-free voucher on L'Oreal's Elvive hair care products[156].

Subsection 2 Signal Triangulation Systems and Wi-Fi Positioning Systems

There are two other positioning systems that function similarly to GPS, but rather than using signals generated between satellites and GPS devices, these systems use signals generated by cellular receiving towers or Wi-Fi access points and are known as Signal Triangulation Systems and Wi-Fi Positioning Systems respectively. To begin with, Signal Triangulation Systems "track the geographic locations and Web surfing behaviours of mobile phone users"[157], using the signals generated between the unique Mobile Identification Numbers, which is an unchangeable number assigned by the manufacturer to each mobile phone[158], and the cellular receiving towers[159]. When two or more such signals are received by these cellular towers from the same cellular phone, meaning that the signals in question can all be linked back to the same unique Mobile Identification Number, the towers compare these signals, allowing the location of the mobile phone in question to be pinpointed[160]. The process used to identify the location of the cellular phone using Signal

---

[154] Emma HALL, "U.K.'s o2 Works With Marks & Spencer, Starbucks, L'Oreal on Location-Based Marketing: Mobile Phone Operators Text Marketers' Deals to Customers; Orange Will Be Next to Add Service", (January 20, 2011, online: <http://adage.com/article/global-news/02-location-based-marketing-m-s-starbucks-l-oreal/148343/> (site consulted on October 18, 2012); S. SHEARMAN, prev. cited, note 153.
[155] E. HALL, *Id.*
[156] *Id.*; S. SHEARMAN, prev. cited, note 153.
[157] N. J. KING, prev. cited, note 12, 253.
[158] *Id.*
[159] *Id.*, 254; A. STROUT and M. SCHNEIDER, prev. cited, note 144, p. 228.
[160] N. J. KING, *Id.*

Triangulation Systems is thus very similar to the one that is used by GPS, but simply employs different signals.

While the process used by Wi-Fi Positioning Systems is also rather analogous to the one used by GPS, in that it uses the signals transmitted between Wi-Fi access points and Wi-Fi enabled cellular telephones to determine the location of the devices in question[161], this system requires additional steps to ensure its proper functioning[162]. Essentially, while the locations of satellites and cellular receiving towers are known, the locations of Wi-Fi access points are not. As a result, to be in the position of using this system to locate cellular telephone users, a database containing Wi-Fi access points must be created[163]. This database is generally produced using a technique called "wardriving", which is a practice whereby a portable computer or a Portable Digital Assistant is used to search a particular area for Wi-Fi networks while travelling by car[164]. At this point, the Media Access Control Address[165], which is the particular number assigned to each network device as well as all other devices that are able to connect to a network[166], of each Wi-Fi access point is

---

[161] Kim CAMERON and Ann CAVOUKIAN, "Wi-Fi Positioning Systems: Beware of Unintended Consequences Issues Involving Unforeseen uses of pre-existing Architecture", June 2011, p. 5, online: <http://www.ipc.on.ca/images/Resources/wi-fi.pdf> (site consulted on January 20, 2012); A. STROUT and M. SCHNEIDER, prev. cited, note 144, p. 229.

[162] K. CAMERON and A. CAVOUKIAN, *Id.*, p. 5-6.

[163] *Id.*, p. 6; Kaveh PAHLAVAN, Ferit AKGUL, Yunxing YE, Ted MORGAN, Farshid ALIZADEH-SHABDIZ, Mohammad HEIDARI and Christopher STEGER, "Taking Positioning Indoors: Wi-Fi Localization and GNSS", 2010, p. 40 and 44, online: <http://www.cwins.wpi.edu/publications/docs/Taking%20Positioning%20IndoorsWi-Fi%20Localization%20and%20GNS.pdf> (site consulted on September 8, 2012).

[164] K. CAMERON and A. CAVOUKIAN, *Id.*; Ionut CONSTANDACHE, Romit Roy CHOUDHURY and Injong RHEE, "Towards Mobile Phone Localization without War-Driving", p. 1-2, online: <http://synrg.ee.duke.edu/papers/compAcc.pdf> (site consulted on September 8, 2012); K. PAHLAVAN, F. AKGUL, Y. YE, T. MORGAN, F. ALIZADEH-SHABDIZ, M. HEIDARI and C. STEGER, *Id.*; *See also:* Edward H. FREEMAN, "Wardriving: Unauthorized Access to Wi-Fi Networks", (2006) 15-1 *Information Systems Security* 11; Chris HURLEY, Frank THORNTON, Michael PUCHOL and Russ ROGERS, *Wardriving: Drive, Detect, Defend: A Guide to Wireless Security*, Rockland, Syngress Publishing, 2004.

[165] Hereafter referred to as "MAC Adress".

[166] Jason I. HONG, Gaetano BORIELLO, James A. LANDAY, David W. MCDONALD, Bill N. SCHILIT and J. D. TYGAR, "Privacy and Security in the Location-enhanced World Wide Web", p. 1, online: <http://www.seattle.intel-research.net/pubs/100220061021_335.pdf> (site consulted on September 8, 2012).

collected[167]. This number is then linked to the precise location at which this signal became available, as well as the signal strength in that particular location, and this information is then uploaded to the database[168].

It must be pointed out, however, that while the technique of wardriving is used with the ultimate goal of being able to track the physical location of individuals, the process involved in the collection of Wi-Fi access points presents certain risks with regards to the acquisition of the personal information of individuals as well. It is a rather recent occurrence with regards to Google that brought this risk to our attention when, in May 2010, "Google discovered that it had [inadvertently] been collecting payload data from unsecured wireless networks as part of its collection of Wi-Fi data [though their intention had only been to collect publicly broadcast SSID information and MAC addresses]"[169]. A large amount of the payload data that had been collected included "the full names, telephone numbers, and addresses of many Canadians [as well as] complete email messages, along with email headers, IP addresses, machine hostnames, and the contents of cookies, instant messages and chat sessions"[170] and even certain "particular sensitive information, including computer login credentials (i.e., usernames and passwords), the details of legal infractions, and certain medical listings"[171].

These risks aside, it is only upon the accumulation of a sufficient amount of Wi-Fi access points within the database that this data can be employed to pinpoint the location of

---

[167] K. CAMERON and A. CAVOUKIAN, prev. cited, note 161, p. 6; I. CONSTANDACHE, R. R. CHOUDHURY and I. RHEE, prev. cited, note 164, p. 1-2; K. PAHLAVAN, F. AKGUL, Y. YE, T. MORGAN, F. ALIZADEH-SHABDIZ, M. HEIDARI and C. STEGER, prev. cited, note 163, p. 40 and 44.
[168] K. CAMERON and A. CAVOUKIAN, *Id.*; I. CONSTANDACHE, R. R. CHOUDHURY and I. RHEE, *Id.*; K. PAHLAVAN, F. AKGUL, Y. YE, T. MORGAN, F. ALIZADEH-SHABDIZ, M. HEIDARI and C. STEGER, *Id.*
[169] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "PIPEDA Report of Findings #2011-001: Google Inc. WiFi Data Collection", June 6, 2011, online: <http://www.priv.gc.ca/cf-dc/2011/2011_001_0520_e.cfm> (site consulted on March 17, 2012).
[170] *Id.*
[171] *Id.*

various devices, including cellular telephones[172]. The position of these devices is determined by establishing the various access points that are in the same general range as the device at that moment, then determining the MAC Addresses linked to each one of these access points, and finally, triangulating the device's precise location using the positions associated with these addresses[173]. The more Wi-Fi access points contained in a given database, the more accurate the determined position of the device will be[174].

The efficient use of Wi-Fi Positioning Systems for location-based advertising can be illustrated by the examples of O2 Media and JiWire. To begin with, O2 set up a number of free public Wi-Fi hotspots across the city of London upon which it promoted the company Wall's Ice Cream[175]. Where this gets more interesting, however, is that these advertisements only appeared on O2's Wi-Fi homepage throughout the summer months when the temperature reached a certain level, essentially "[combining] two fast-emerging trends in digital media: location-based and contextual marketing"[176] to create a practice referred to as Thermal Targeted Proximity Messaging[177].

Even more impressive is the campaign created by a location-based advertising company called JiWire. This enterprise utilizes a Wi-Fi Positioning System to keep track

---

[172] K. CAMERON and A. CAVOUKIAN, *Id.*, p. 9; *See also:* William CHING, Rue Jing TEH, Binghao LI, Chris RIZOS, "Uniwide WiFi Based Positioning System", *IEEE International Symposium on Technology and Society*, Shanghai, China, 2010, 180.
[173] K. CAMERON and A. CAVOUKIAN, *Id.*
[174] *Id.*
[175] Mike SHAW, "Location-based advertising takes a cool step forward", August 10, 2012, online: <http://www.mobile-ent.biz/news/read/location-based-advertising-takes-a-cool-step-forward/018981> (site consulted on October 24, 2012).
[176] THE BLUE NEWS & VIEWS FROM O2, "Free O2 Wifi tempts consumers with Wall's Ice Cream", August 9, 2012, online: <http://news.o2.co.uk/?press-release=free-o2-wifi-tempts-consumers-with-walls-ice-cream#> (site consulted on October 24, 2012).
[177] Jaimie KAFFASH, "Wall's and O2 target ice cream ads around weather", August 9, 2012, online: <http://www.marketingweek.co.uk/news/walls-and-o2-target-ads-around-weather/4003193.article> (site consulted on October 23, 2012).

of the various locations frequented by individuals[178] and create something called a Location Graph, which is "a revolutionary mobile solution that [assigns] audience profiles based on past and present locations. [The] data provides a unique look at how a person's behavior is interconnected with their locations and each other"[179]. The location information of individuals is then combined with user data emanating from third-parties, in turn allowing them to determine various target audiences. For example, JiWire's Location Graph has demonstrated that

> "sixty percent of women eat at the same three restaurants each month[;] Moms who go to beauty salons are also likely to visit health clubs, child care centers, counseling services and restaurants[;] Twenty-three percent of people who go to Peet's Coffee and Tea also go to Starbucks[;] Thirty percent of people who shopped at Best Buy also shopped at a competitor's location."[180]

This information therefore allows JiWire to target individuals with advertisements that are relevant to both their desires as well as their location at a given moment in time[181]. For example, if an individual who had previously frequented Peet's Coffee and Tea happens to be located near a Starbucks, JiWire would target that individual with an ad for this coffee shop based on the correlation between the two demonstrated by its Location Graph.

Subsection 3 Location-Based Social Networks

Location-based Social Networks[182] are very similar to SNWs[183] in that they allow individuals to connect with one another. LBSNs, however, take matters one step further.

---

[178] TELECOMPAPER, "JiWire licenses Wi-Fi positioning system from Skyhook", May 31, 2007, online: <http://www.telecompaper.com/news/jiwire-licenses-wifi-positioning-system-from-skyhook> (site consulted on October 24, 2012).
[179] JIWIRE, "JiWire's Location Graph: Because where you've been says more about you than the websites you visit", 2012, online: <http://www.jiwire.com/locationgraph> (site consulted on October 24, 2012).
[180] Anthony HA, "JiWire Aims to Improve Mobile Ad Targeting With Its New Location Graph", August 14, 2012, online: <http://techcrunch.com/2012/08/14/jiwire-location-graph/> (site consulted on October 24, 2012).
[181] *Id.*
[182] Hereafter referred to as "LBSN".

Not only can users contact their acquaintances and share profile information, but these social networks also render it possible for individuals to share their particular location at any given moment with their network friends, as well as the location of any of their friends who happen to be accompanying them. This thus permits people to connect, not only based on whatever information they provide regarding their personality and preferences, but also based on their location by "[allowing] users to see where their friends are, to search location-tagged content within their social graph, and to meet others nearby"[184].

These types of social networks are also extremely sophisticated and accurate in the location information they provide. They function using GPS, Signal Triangulation or Wi-Fi Positioning Systems to determine an individual's precise location, allowing these users to share this data with their friends on their social network[185]. With the increased use of smartphones containing Internet capabilities, these types of social networks have become much more accessible to users and thus tremendously popular[186]. It has been estimated that by the year 2013, 82 million users will have subscribed to LBSNs worldwide[187].

One of the most popular LBSNs is Foursquare with over twenty million users, a number that doubled in less than a year, and two billion check-ins as at April 27, 2012[188]. This Social Network recently updated its application to include what it calls "Radar". According to the company's blog,

---

[183] *See: Supra*, p. 24-32.
[184] Nan LI and Guanling CHEN, "Analysis of a Location-based Social Network", p. 1, online: <http://rio.ecs.umass.edu/~lgao/ece697_10/Paper/LocationBasedSocialNetwork.pdf> (site consulted on January 20, 2012).
[185] *Id.*
[186] *Id.*; *See also:* Guanling CHEN and Faruq RAHMAN, "Analyzing privacy designs of mobile social networking applications", in *Proceedings of the IEEE/IFIP International Symposium on Trust, Security and Privacy for Pervasive Applications (TSP)*, Shanghai, China, 2008, 83.
[187] N. LI and G. CHEN, *Id.*
[188] STAT SPOTTING, "Foursquare Statistics: 20 Million Users, 2 Billion Check-Ins", April 27, 2012, online: <http://statspotting.com/2012/04/foursquare-statistics-20-million-users-2-billion-check-ins/> (site consulted on October 24, 2012).

> "Now, if you follow a list, like the 101 Best Dishes of 2011, foursquare will let you know when you're next to one. Or you save that yoga studio to your To-Do List (because you really want to try it); we can remind you when you're close. Or, better yet, if you're driving home and three of your friends are getting together nearby, we'll tell you so you can meet up. The app doesn't even have to be open, it just works. We call it foursquare Radar, because it finds things nearby that you normally wouldn't know about."[189]

* * *

Mobile tracking tools thus make it possible for businesses to track the every move of individuals in the physical world, whether through data these users voluntarily provide through their use of LBSNs, or through their GPS enabled mobile telephones or the Signal Triangulation System or Wi-Fi Positioning System rendered possible through cellular phones. The information concerning the various locations of users is combined with the data regarding their personal preferences collected using cookies[190], DPI[191] and SNWs[192], so as to ultimately target them with location specific advertisements using this information.

With the unbelievable proliferation of mobile tracking tools, it has become nearly effortless to locate individuals and target them with advertisements tailored to their interests, ultimately serving to "maximize [their] engagement with products and services"[193]. The ability to attract the business of customers in such a manner is therefore rather extensive, and the market resulting from this practice is expected to reach 2.5 billion dollars by the year 2015[194]. However, despite the fact that the market for this form of advertising is gradually increasing, it does not change the fact that tracking the location of

---

[189] FOURSQUARE BLOG, "The real world, now in real-time! Say hi to foursquare Radar!", October 12, 2011, online: <http://blog.foursquare.com/2011/10/12/the-real-world-now-in-real-time-say-hi-to-foursquare-radar/> (site consulted on October 24, 2012).
[190] *See : Supra*, p. 10-17.
[191] *See : Supra*, p. 17-23.
[192] *See : Supra*, p. 24-31.
[193] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, prev. cited, note 39, p. 13.
[194] Asha RICHARDSON, "Location based mobile advertising – Google's following you", May 4, 2011, online: <http://www.youthradio.org/news/location-based-mobile-advertising-googles-following-you> (site consulted on January 20, 2012).

individuals and targeting them with advertisements in such a manner may effectively violate their privacy, as we will discuss in further detail in Part II of this thesis[195].

* * *

When taken together, both online tracking tools as well as mobile tracking tools make it possible to determine precisely what a consumer wants, and present him with an offer to acquire the object of his desire at the exact right moment – such as when he is near a location which can help him obtain what he wishes. The versatility of these tools from a marketing perspective is therefore undeniable; they provide marketers with the precise information they require to successfully market to individuals and prevent them from having to waste their resources on people upon whom the products or services being advertised would be lost. Due to its highly beneficial nature for enterprises, the use of these tools has therefore become rather common, as illustrated by the numerous examples provided throughout this chapter. On the other hand, the issues with regards to the privacy protection of individuals that the use of such tools presents are also indisputable, as will be discussed in further detail below[196].

However, while tracking and targeting users using both online and mobile tracking tools is very valuable to marketers, the use of these tools for marketing purposes merely represents a single factor in the practice of Internet marketing. Though the benefit of targeting users cannot be denied, it can only be used by marketers to find users and present them with what the marketers believe they want, as inferred by their use of the Internet. In the event that consumers desire something that marketers have not endeavoured to present them with, on the other hand, the users must be in the position of finding what they are searching for. Reaching users is therefore just as important as targeting them, and we will

---

[195] *See: Infra*, p. 62-116.
[196] *Id.*

thus dedicate the next chapter of this thesis to an in-depth discussion of the various Internet marketing strategies used to simplify a consumer's search.

Chapter 2 Reaching Users

While tracking users is very useful in providing a certain insight into a consumer's personality, the benefit of being able to reach users cannot be ignored from a marketing perspective. Without maintaining a certain level of contact with a user, the efficiency of marketing is inevitably reduced. This chapter will therefore be dedicated to an in-depth discussion of the various manners in which marketers may reach consumers, either through (1) using social media to converse with them or through (2) ensuring that they are accessible to users via search engines.

Section 1 Conversing With Users: Social Media Marketing

The ability of users to participate through the use of social media, by both creating and sharing content, enables marketers to engage individuals on such platforms and to converse with them in the goal of increasing brand awareness and acquiring consumer input and ideas[197] – a strategy known as Social Media Marketing[198]. This form of marketing is tremendously useful to businesses. While targeted marketing does provide marketers with a certain insight into the personality, preferences and habits of individuals, SMM provides a forum upon which consumers voluntarily provide marketers with a glimpse into their mind – their opinions, their thoughts and their true desires – simply by enabling a conversation to be created between both marketers and consumers. This section will therefore examine two particular tools used for this form of marketing, namely (1) blogs and micro-blogs, and (2) SNWs, and ultimately outline the various manners, both licit and illicit, in which these tools are utilized by businesses.

---

[197] David Joshua PERDUE, *Social Media Marketing: Gaining a Competitive Advantage by Reaching the Masses*, Virginia, Center for Computer and Information Technology, Liberty University, 2010, p. 5.
[198] Hereafter referred to as "SMM".

Subsection 1 Blogs and Micro-blogs

A blog, a term which has arisen as a shortened version of the words "Web log", is a form of social media that has been adopted by many corporations as a part of their marketing strategy. Blogs are platforms upon which companies can post information about themselves and even provide links to other content on the Internet, such as web pages or videos and other rich media content, viewable to anyone on the web, and which are updated on a regular basis[199]. All of the entries ever posted on blogs are accessible on the site and appear in reverse chronological order, meaning the latest entry appears first, with archived entries available through links at the bottom or sides of the page[200]. Not only do blogs contain the entries posted by the originator of the blog in question, but they also allow for the possibility of individuals who read the blog to leave comments, either in the form of questions, opinions or suggestions[201].

Corporate blogging has become an extremely popular practice. In 2011, the percentage of businesses that employed blogs for their marketing strategy was 65% – which represents a 27% increase from the year 2009[202]. Approximately 57% of the companies that use blogs to interact with their customers have reported that they have acquired new customers directly from their blogs[203]. While 85% of companies find that blogs are very useful to their business, 27% of them consider blogs to be critical to their business[204].

---

[199] INTERACTIVE ADVERTISING BUREAU, "Platform Status Report: User Generated Content, Social Media, and Advertising – An Overview", April 2008, p. 4, online: <http://www.slideshare.net/AutomotiveSocial/2008-ugc-platform-2931455> (site consulted on January 21, 2012); P. TRUDEL, prev. cited, note 103, p. 200-202; Ahuja VANDANA, "Using Corporate Blogs for Supporting Interactive Marketing and CRM", September 8, 2011, p. 12-13, online: <http://shodhganga.inflibnet.ac.in/bitstream/10603/2697/9/09_chapter%202.pdf> (site consulted on January 21, 2012).

[200] INTERACTIVE ADVERTISING BUREAU, *Id.*, p.4

[201] A. VANDANA, prev. cited, note 199, p. 13-14.

[202] HUBSPOT, "The 2011 State of Inbound Marketing", February 2011, p. 3, online: <http://www.hubspot.com/Portals/53/docs/ebooks/the%20state%20of%20inbound%20marketing%20final%20v3-2.pdf> (site consulted on January 21, 2012).

[203] *Id.*

[204] *Id.*

While blogging is extremely popular in this day and age, another phenomenon known as micro-blogging is also on the rise. Similarly to blogging, micro-blogging allows individuals to share opinions and ideas, but in a much more shortened format, often limited to 140 characters. Additionally, contrary to blogs, which are generally updated once every few days, individuals using micro-blogs often post commentary several times a day[205]. In such a way, micro-blogging "fulfills a need for an even faster [and more frequent] mode of communication"[206]. The most common forum for micro-blogging is presently the social media service known as Twitter. This service is currently provided to over 200 million subscribed users who post a combined amount of 110 million micro-blogs per day[207]. Micro-blogging is thus also quite a popular form of social media and is of as much use to corporations as are blogs.

While blogs and micro-blogs are used by corporations to provide consumers with updates about matters that may concern them, they also supply a venue that promotes participation[208] by enabling comments to be made by these individuals[209]. These comments are "integrated into a post, resulting in a themed conversation between the corporate, the user (consumer) and other users (consumers) who have posted a comment, forming an interesting supplement to the post hosted by the organization"[210].

This form of communication between corporations and consumers is becoming very common. For example, many CEO's and employees of major corporations have created

---

[205] Victor ERNESTAD and Robert HENRIKSSON, "Social media marketing from a bottom-up perspective – the social media transition", p. 5, online: <http://umu.diva-portal.org/smash/get/diva2:325207/FULLTEXT01> (site consulted on January 21, 2012); Akshay JAVA, Tim FININ, Xiaodan SONG and Belle TSENG, "Why We Twitter: Understanding Microblogging Usage and Communities", 2007, p. 2, online: <http://ebiquity.umbc.edu/_file_directory_/papers/369.pdf> (site consulted on January 21, 2012).
[206] V. ERNESTAD and R. HENRIKSSON, *Id.*
[207] Oliver CHIANG, "Twitter Hits Nearly 200M Accounts, 110M Tweets Per Day, Focuses On Global Expansion", January 19, 2011, online: <http://www.forbes.com/sites/oliverchiang/2011/01/19/twitter-hits-nearly-200m-users-110m-tweets-per-day-focuses-on-global-expansion/> (site consulted on January 20, 2012).
[208] A. VANDANA, prev. cited, note 199, p. 18.
[209] INTERACTIVE ADVERTISING BUREAU, prev. cited, note 199, p. 4.
[210] A. VANDANA, prev. cited, note 199, p. 18-19.

blogs as a means to maintain public relations, and they use these forums to permit their consumers to ask them questions or provide suggestions[211]. This type of consumer participation is also promoted on many newspaper websites that permit their readers to comment on articles or blog posts written by their reporters[212]. There are even many testimonial websites upon which consumers may rate various establishments and recount their experiences to their fellow consumers, which also serve to incite user participation.

By communicating with individuals in such a manner, marketers are able to increase company and brand awareness[213], while also receiving feedback about a business's products or services, or even exchanging ideas for new products or services with customers, ultimately rendering it possible for them to be in the position of providing users with what they truly want. Not only does this manner of maintaining a conversation with consumers incite their loyalty by giving weight to their opinions thus motivating them to "help promote the company and get the attention of mainstream media"[214], but it also enables businesses to remain relevant to their customers and ultimately ensures that their products or services move forward with the times and the ever-changing desires of their audience[215].

Yet, while social media is a primary tool that is often used by businesses to communicate with their audience, serving to increase brand awareness and reach out to consumers for brand ideas[216], businesses do not always use this tool in a suitable manner. There are several examples where companies have utilized social media inappropriately, either to deceive consumers or to overturn their competitors.

To begin with, there have been several cases where "some firms have [tried] to con the consumer by pushing their own propaganda on websites while pretending to be the

---

[211] INTERACTIVE ADVERTISING BUREAU, prev. cited, note 199, p. 4.
[212] *Id.*
[213] D. J. PERDUE, prev. cited, note 197, p. 24.
[214] *Id.*, p. 28.
[215] Tanuja SINGH, Liza VERON-JACKSON and Joe CULLINANE, "Blogging: A New Play in Your Marketing Game Plan", (2008) 51 *Business Horizons* 281, 285.

voice of the people"[217]. An example of such an occurrence took place in April 2005 where a subsidiary of the cosmetics company L'Oreal Paris, Laboratoires Vichy, created a fake blog supposedly produced by a woman named Claire who spoke of her so-called positive experiences regarding her use of a Vichy anti-wrinkle product[218]. Suspicions regarding Claire's true identity began to arise as a result of the blog's structure, which made it appear as if it had been fabricated by a professional rather than by an ordinary consumer[219]. After a large number of individuals aired their doubts on various online blogs, a representative of Vichy finally came forth and admitted that Claire was a fictional character created by an advertising agency simply to promote Vichy's products to other consumers[220], ultimately asking for the forgiveness of both their clients as well as the members of the blogosphere for their deceitful behaviour[221]. The consequences suffered by Vichy as a result of this occurrence revolve around the company being publicly ridiculed and labelled non-credible, thus experiencing a certain decline in their previously stellar reputation[222].

Unfortunately, this was not the last instance in which such a fiasco occurred – a year following Vichy's creation of a fake blog, Wal-Mart decided to produce one itself[223]. Their blog, called Wal-Marting Across America, was supposedly created by a couple, Jim and Laura, traveling across the United States and blogging about their positive Wal-Mart experiences along the way[224]. When every Wal-Mart employee interviewed by the couple spoke only about how much they love working at the store, suspicions began to arise

---

[216] *Id.*, p. 5.
[217] Robert PLUMMER, "Will fake business blogs crash and burn?", May 22, 2008, online: <http://news.bbc.co.uk/2/hi/7287413.stm> (site consulted on January 25, 2011).
[218] *Id.*
[219] José ESTEVES, "France Vichy Cosmetics: Blog or Not To Blog?", May 9, 2008, p. 3, online: <http://openmultimedia.ie.edu/openproducts/vichy_i/vichy_i/pdf/teaching_case_vichy.pdf> (site consulted on August 25, 2012).
[220] R. PLUMMER, prev. cited, note 217.
[221] J. ESTEVES, prev. cited, note 219, p. 4.
[222] *Id.*
[223] R. PLUMMER, prev. cited, note 217; Heather WINN, "Internet Marketing: Using New Forms of Internet Media to Market to Today's Generation", (2010) 8 *Liberty Business Review* 11, 17.
[224] R. PLUMMER, *Id.*; H. WINN, *Id.*.

simply because Wal-Mart's history with employee relations is said to leave much to be desired[225]. Eventually, it was uncovered that Jim was a photographer for the Washington Post and Laura was a freelance writer[226], and not only did Wal-Mart fund their entire trip, but they also provided them with additional financial incentive on the side[227]. Similarly to the case of Vichy, however, Wal-Mart did not suffer any adverse effects as a result of the fake blog that they funded[228].

Not too long after that, the popular electronics company, Sony, produced a fake blog upon which individuals, who were supposedly regular consumers, wrote about their adamant desire to receive a Playstation Portable game console for Christmas[229]. It was quickly discovered that the individuals posting these comments were not ordinary consumers and that the blog was in fact created by a marketing firm hired by Sony for precisely this purpose[230]. Aside from emitting an official apology, however, no legal consequences were suffered by Sony for their creation of this fake blog.

These fake blogs were created by the companies in question so as to appeal to their customers by essentially providing them with false testimonials regarding the grandiosity of their products and services. The use of social media in such a manner, however, presents

---

[225] Pallavi GOGOI, "Wal-Mart's Jim and Laura: The Real Story", October 9, 2006, online: <http://www.businessweek.com/stories/2006-10-09/wal-marts-jim-and-laura-the-real-storybusinessweek-business-news-stock-market-and-financial-advice> (site consulted on August 27, 2012).
[226] WAL-MART WATCH, "The Wal-Mart Fake Blog Controversy: Anatomy of a Public Relations Disaster", online: <http://walmartwatch.com/wp-content/blogs.dir/2/files/pdf/flog_controversy.pdf> (site consulted on August 27, 2012).
[227] P. GOGOI, prev. cited, note 225.
[228] Dave TAYLOR, "Edelman screws up with duplicitous Wal-Mart blog, but it's okay?", October 16, 2006, online: <http://www.intuitive.com/blog/edelman_screws_up_with_duplicitious_walmart_blog.html> (site consulted on August 27, 2012).
[229] Aleks KROTOSKI, "New Sony viral marketing ploy angers consumers: Sony has generated ire with another alleged viral marketing campaign posing as real Web 2.0", December 11, 2006, online: <http://www.guardian.co.uk/technology/gamesblog/2006/dec/11/newsonyviral> (site consulted on January 25, 2012); R. PLUMMER, prev. cited, note 217.
[230] MEGA GAMES, "Sony Fake PSP Blog Busted", December 14, 2006, online: <http://megagames.com/news/sony-fake-psp-blog-busted> (site consulted on August 27, 2012).

certain issues from a consumer protection law perspective, namely with regards to false advertising, which will be discussed in further detail in the next part of this thesis[231].

Subsection 2 Social Network Websites: Business Profiles

SNWs, as defined above[232], are not only limited to the use by individuals through the creation of personal profiles allowing them to maintain contact with their friends and acquaintances, but can also be used by businesses to create company profiles that allow their customers to interact with them on a more personal basis[233]. Similarly to personal profiles, the profiles they create describe their business and can be followed by other users who are members of the same SNW, should they so desire[234]. This allows these users to follow the posts emitted upon the profile of the business in question and ultimately contribute their own comments and opinions[235].

While there are cases in which companies created fake blogs to appeal to their consumers, as discussed above[236], it is not unheard of for businesses to join a SNW and create a page upon which it interacts with its consumers, while having their employees assume false identities and post positive comments about the company's products or services. This is precisely what was orchestrated by Kohl's, whose Vice President of Marketing and the Group Director of the advertising agency working with Kohl's were impersonating consumers and sharing tales regarding the significant amount of money they saved during their "shopping experiences" at Kohl's[237]. Thus, while creating fake blogs is more common than it should be, the act of high ranking company management assuming

---

[231] *Infra*, p. 156-166.
[232] *Supra*, p. 24.
[233] INTERACTIVE ADVERTISING BUREAU, prev. cited, note 199, p. 9.
[234] *Id.*
[235] *Id.*
[236] *Supra*, p. 46-49.
[237] Clive MACLEAN, "Social Media Deception…Warning to Ad-Agencies and Clients", June 30, 2009, online: <http://clivemaclean.wordpress.com/2009/06/30/social-media-warning-to-ad-agencies-and-their-clients/> (site consulted on January 25, 2012).

the identity of consumers to promote their company is also quite a likely occurrence and, similarly to the case of fake company blogs, poses consumer protection issues as well[238].

In the past, however, business officials have not only assumed false identities with the purpose of deceiving their consumers, but have done so with the aim of denigrating their competitors as well. Such an occurrence took place in 2007 where Whole Foods Market's Chief Executive Officer participated in a Yahoo! chat forum under a false identity which he used to attack his company's competitor, Wild Oats Markets, for which an offer to purchase was made by Whole Foods later on that year[239]. Comments such as "[t]he end game is now underway for [Wild Oats.] […] Whole Foods is systematically destroying their viability as a business – market by market, city by city"[240] and "Bankruptcy remains a distinct possibility [for Wild Oats] IMO if the business isn't sold within the next few years"[241] were made by Whole Foods' CEO, ultimately attempting to devaluate Wild Oats shares and hurt their business[242]. This merger was, however, blocked by the Federal Trade Commission, whose lawsuit against Whole Foods is pending in United States District Court in Washington[243].

Unfortunately, this is not an isolated incident, and has actually become quite an epidemic in some countries around the world, particularly China. In the year 2010, "Chinese authorities […] uncovered several cases in which major companies paid members of [a group of people, known as the] online army[,] to flood influential message boards,

---

[238] *Infra*, p. 156-166.
[239] MSNBC.COM, "Whole Foods CEO's anonymous online life: Postings on financial forums attacked a rival company trying to buy", July 12, 2007, online: <http://www.msnbc.msn.com/id/19718742/ns/business-us_business/t/whole-foods-ceos-anonymous-online-life/ > (site consulted on January 25, 2012); H. WINN, prev. cited, note 223, 17.
[240] Peter KAPLAN, "John Mackey panned Wild Oats on Web", July 12, 2007, online: <http://www.reuters.com/article/2007/07/12/us-wholefoods-ftc-idUSN1133440820070712> (site consulted on January 25, 2012).
[241] *Id.*
[242] *Id.*
[243] MSNBC.COM, prev. cited, note 239.

blogs and chat rooms with false information about competitors"[244]. One such organization was used by Mengniu, China's leading dairy company, who paid marketers to spread a rumour about its largest competitor, Yili, regarding their apparent use of deep-sea fish oil in their children's milk products which could supposedly cause them to prematurely go through puberty[245]. This rumour ultimately resulted in the swift plummeting of Yili's sales of children's products[246]. The manager at Mengniu in charge of this scheme as well as the employees of the marketing agency involved in it were arrested[247] and convicted to prison sentences ranging from 25 days to one year[248].

Even more recently, it was discovered that one of the world's largest SNWs, Facebook, orchestrated such a scheme against Google's Social Circles' feature[249]. Facebook paid a public relations firm to supply bloggers with negative stories about Google's new feature, apparently bringing forth certain alleged privacy concerns, and even offer to write those stories in their place[250] – a scheme which came to light after one of the bloggers approached by the marketing firm in question publicized the issue online[251].

---

[244] Chico HARLAN, "China pushing back against online smear campaigns", January 27, 2011, online: <http://www.washingtonpost.com/business/china-pushing-back-against-online-smear-campaigns/2011/01/27/ABMY93Q_story.html> (site consulted on January 25, 2012).
[245] *Id.*; Austin RAMZY, "China's New Scandal: Tainted Milk or Smear Campaign?", October 22, 2010, online: <http://www.time.com/time/world/article/0,8599,2027076,00.html> (site consulted on January 25, 2012).
[246] C. HARLAN, *Id.*; A. RAMZY, *Id.*
[247] Wang QINGCHU, "Mengniu says sorry, and accuses", October 23, 2010, online: <http://mobile.shanghaidaily.com/article/?id=452467> (site consulted on August 27, 2012).
[248] Zhuang PINGHUI, "Mengniu smear blitz against Yili ends with jail sentences", March 16, 2011, online: <http://www.scmp.com/article/741054/mengniu-smear-blitz-against-yili-ends-jail-sentences> (site consulted on October 18, 2012).
[249] Dean WILSON, "Facebook admits hiring a PR firm to bad mouth Google", May 13, 2011, online: <http://www.theinquirer.net/inquirer/news/2070674/facebook-admits-hiring-firm-bad-mouth-google> (site consulted on January 25, 2012).
[250] C. HARLAN, prev. cited, note 244; A. RAMZY, prev. cited, note 245.
[251] Dan LYONS, "Facebook Busted in Clumsy Smear on Google", May 11, 2011, online: <http://www.thedailybeast.com/articles/2011/05/12/facebook-busted-in-clumsy-smear-attempt-on-google.html> (site consulted on August 27, 2012); Jane MCENTEGART, "Facebook Hires PR Firm to Smear Google", May 12, 2011, online: <http://www.tomsguide.com/us/Facebook-Burson-Marsteller-Smear-Campaign-Anti-Google-Social-Circle,news-11171.html> (site consulted on August 27, 2012).

Facebook claimed that it was merely further exposing information that was already public and as such was not faced with any further consequences[252].

This type of behaviour, whereby companies utilize social media platforms to create smear campaigns against their competitors, poses certain legal issues as these actions can be viewed as trade libel – an occurrence which companies are protected from by law. Those enterprises responsible for the communication and publication of negative statements against their competitors could therefore likely find themselves implicated in a lawsuit, as will be further discussed in Part II of this thesis[253].

* * *

SMM is thus a double edged sword. While it is true that many companies use this form of marketing honestly, simply to communicate with their consumers and increase brand awareness, there are many businesses whose presence in online social media forums is not nearly as forthcoming and transparent – as is evidenced by the various underhanded practices described in the examples provided above. The use of SMM as a marketing strategy is thus one whose employment, while it has a great deal of potential, is not nearly as clear cut as consumers, as well as affected competitors, might like it to be.

While SMM provides marketers with the opportunity to reach consumers by engaging in online conversations with them upon various platforms, it is not the only form of marketing that provides the possibility of reaching users. The potential to reach users effectively is also provided through Search Engine Marketing, another form of marketing that will be discussed in further detail in the next section.

---

[252] Josh HALLIDAY, "Facebook paid PR firm to smear Google", May 12, 2011, online: <http://www.guardian.co.uk/technology/2011/may/12/facebook-pr-firm-google> (site consulted on August 27, 2012).
[253] *Infra*, p. 126-139.

Section 2 Being Accessible to Users: Search Engine Marketing

As is well-known, search engines are platforms upon which millions of websites throughout the Web are indexed so that Internet users may search and find any data they like. For businesses, being easily accessible to users through such platforms is one of the keys to their success. This feat is often achieved through a practice known as Search Engine Marketing[254], which utilizes various tools to place the business's website in a good position on the search engines' index and ultimately increase both traffic to that site and its visibility on the Web[255]. Though SEM tools are varied, we will limit our discussion to two main elements with respect to this practice, namely (1) those upon which the visibility of websites in search engines are based, and (2) the use of a particular tool known as keyword advertising in light of the manner in which companies use these tools for marketing purposes.

Subsection 1 Visibility

The success of businesses in the modern age of the Internet is often directly linked to their visibility in online search engines. Regardless of their creation of the most visually attractive and user friendly website, it will be impossible for any business to relate to their customers should these individuals be unable to find them online[256]. That being said, however, the race to visibility on the Internet is a difficult one, as it has been discovered that users often only look at the first 20 postings listed by a search engine[257].

The order of appearance of search results, and thus the ultimate visibility of a site on the Internet, is based on the manner in which search engines function. Search engines

---

[254] Hereafter referred to as "SEM".
[255] V. ERNESTAD and R. HENRIKSSON, prev. cited, note 205, p. 6.
[256] Grant Warren SHERSON, *Internet Marketing and Society*, Master's thesis, Wellington, Faculty of Commerce and Administration, Victoria University of Wellington, 2000, p. 3.
[257] *Id.*; Maria DUGGAN and John DEVENEY, "How to Make Internet Marketing Simple", 2003, p. 1, online: <http://www.deveney.com/public/userfiles/5_internet20marketing2.pdf> (site consulted on January 23, 2012).

index all of the Web pages throughout the Web based on two elements[258]: relevance to the search, which usually revolves around the correlation between the query performed and the keywords associated with the site[259], and overall importance, which generally increases relatively to the number of links leading to that page from other sites or Web pages[260].

Both of these elements, and thus the ultimate visibility, of a business's website are determined by the search engine's algorithm. As a result, should a business want to increase their visibility online, they must attempt to appeal to this algorithm, using various tactics, to "ensure that [it] gives the page a higher score in comparison to other pages that qualify to be displayed in the search-results"[261]. The tactics that are able to achieve this

---

[258] Frank PASQUALE, "Rankings, Reductionism and Responsibility", (2006) 54 *Cleveland St. L. Rev.* 115, 117.

[259] The determination of whether or not a particular web page would be a relevant result to a specific search is determined by comparing the query in question with the text on the page, the various tags attached to the page, and other constituents found thereon (F. PASQUALE, prev. cited, note 258, 117). A website's relevance will often be based on its use of keywords in its content. Keywords may appear in the title of a website, in the names of the various pages of a website, in the actual written material that is placed on a site and on the various tags of a website (Marziah KARCH, "How to Improve Your Website's Google Ranking", 2012, online: <http://google.about.com/od/searchengineoptimization/qt/improverank.htm> (site consulted on January 23, 2012). Essentially, if keywords are used in a site's main title or in the headings of the various web pages that make up the site, that website would have a much greater chance to appear in the search results for any query using those words (Marziah KARCH, "Why Titles Matter – How to Get More People to See Your Pages in Google", 2012, online: <http://google.about.com/od/searchengineoptimization/qt/titleseoqt.htm> (site consulted on January 23, 2012)). Furthermore, the more often a keyword is used in the content of the website, the greater the chances are of that website being ranked higher for the particular keyword in question ((Marziah KARCH, "How to Improve Your Website's Google Ranking", prev. cited, note 259). Often times, keywords have a better chance of increasing a site's rank if they are used in the form of phrases as users frequently tend to search terms and not only single words (*Id.*).

[260] In addition to the relevance of a website to a query performed on a search engine, the importance of the website will also play a role in the site's ranking. The overall importance of a particular web page relies on its popularity, so to speak, essentially depending upon the number of links leading to that specific page (F. PASQUALE, prev. cited, note 258, 117). It is not, however, only the quantity of links that increases a page's rank, but also the quality of those links. The quality of a link is based on the ranking of the website that links to the site in question – the higher the ranking of the website that created the link, the more weight that particular link possesses, and the greater the chance for the business's website to have its ranking increased (Marziah KARCH, "What Is PageRank and How Do I Use It?", 2012, online: <http://google.about.com/od/searchengineoptimization/a/pagerankexplain.htm> (site consulted on January 23, 2012)).

[261] Ravi SEN, "Optimal Search Engine Marketing Strategy", (2005) 10-1 *International Journal of Electronic Commerce* 9, 10.

feat revolve around the proper choice of keywords[262] and increasing keyword density throughout the content of the site[263]. Additionally, increasing both the quantity[264] and quality of links leading to a site will also serve to improve its position in search results, especially when those links originate from sites considered authoritative by search engines, such as those of government or educational institutions[265].

While modifying keywords and increasing the number of links leading to a site in a reasonable manner is considered an acceptable practice, there are certain abusive tactics that are used by website owners to attempt to manipulate a search engine's algorithm into

---

[262] To begin with, choosing keywords that are closely associated to terms that fall into niche categories can increase the search engine optimization of a particular site. This is due to the fact that, contrary to overbroad keywords that can be applicable to a large amount of websites, using a niche term limits the quantity of sites that will appear in the list of search results thus avoiding having that site buried amongst other search results (Glenn GABE, "The Long Tail of SEO, How Long Tail Keywords Impact Natural Search Traffic, Bounce Rate and Conversion", <http://www.hmtweb.com/blog/2008/08/long-tail-of-seo-how-long-tail-keywords.html> (site consulted on January 23, 2012)).

[263] It is also possible for a business to enhance the relevance of its website by increasing the density of keyword use on the site in question. While search engines consider it unacceptable to abuse the use of keywords by constantly repeating the same word out of context, increasing word density is rendered possible by the incorporation of a blog into a website and using it as a SEM platform (Douglas KARR and Chantelle FLANNERY, *Corporate Blogging for Dummies*, Indianapolis, Wiley Publishing, 2010, p. 12). Using a blog renders it possible for a website owner to increase the number of keywords on his site by continuously adding more postings and including keywords therein (*Id.*).

[264] There are essentially several manners in which websites may increase the quantity of high quality links leading to their site. To begin with, it is possible for them to submit themselves to an online directory dedicated to listing various websites that pertain to a particular topic (M. KARCH, "How to Improve Your Website's Google Ranking", prev. cited, note 259). It is also possible for companies to create business profiles on SNWs and use that to promote their site and link back to it (*Id.*).

Furthermore, when it comes to links, it is not only the links leading from one website to another that are considered by search engines, but also hyperlinks that direct a user around the website in question, which essentially consists of inter-linking between the various pages of a site. The relevance of these hyperlinks will be based on the keywords or phrases which they highlight (Marziah KARCH, "Don't Make 'Click Here' Links – Why Hyperlink Names Matter to Google", 2012, online: <http://google.about.com/od/searchengineoptimization/qt/hyperlinkqt.htm> (site consulted on January 23, 2012)). For example, a search engine will accord more importance to a hyperlink using the term "Search Engine Marketing" than to one that simply states "click here" in order to acquire more information about this form of marketing. This is due to the fact that the first actually utilizes relevant keywords while the second is more generic and does not denote anything of importance (M. KARCH, "How to Improve Your Website's Google Ranking", prev. cited, note 259).

[265] Eric ENGE, "11 Guidelines for getting Authoritative Links", February 23, 2007, online: <http://searchenginewatch.com/article/2056780/11-Guidelines-for-Getting-Authoritative-Links> (site consulted on October 27, 2012).

providing them with a higher ranking using rather backhanded techniques, commonly referred to as black hat SEM methods. These practices are generally used in the hopes of increasing a business's website rankings at the detriment of its competitors, but can rather serve to negatively affect the position of a site on a search engine.

There have been several examples of the use of black hat SEM tactics by companies that have come to light over the years. For instance, it was discovered in early 2006 that BMW was using a particular black hat practice known as "doorway pages" to increase traffic to its website[266] "which exist to attract search engines [by using various search terms] and then redirect traffic to a different site"[267] essentially "[tricking] search engines into sending users to Web sites that are not directly related to the search terms they are searching for"[268]. BMW's use of this tactic resulted in its being removed from Google's index and therefore not appearing in the search engine's results[269].

With regards to the use of this technique, however, it is important to point out that while in this case BMW placed keywords such as "new cars" and "used cars" in the offending doorway pages, it has not been unheard of for sites to use the trademarks of other companies in these pages to direct the traffic of those companies' sites onto their own. Since these doorway pages are designed solely for search engine ranking purposes, thus remaining invisible to Internet users, these individuals may be led to believe that the page they have landed on is associated with the trademark they have searched[270]. The use of this

---

[266] CNN.COM, "Google blacklists BMW Web site", February 7, 2006, online: <http://www.cnn.com/2006/BUSINESS/02/07/google/> (site consulted on October 25, 2012).
[267] David SEGAL, "The Dirty Little Secrets of Search", February 12, 2011, online: <http://www.nytimes.com/2011/02/13/business/13search.html?pagewanted=all&_r=0> (site consulted on October 25, 2012).
[268] CNN.COM, prev. cited, note 266.
[269] *Id.*
[270] James A. ROSSI, "Protection for Trademark owners: The Ultimate System of Regulating Search Engine Results", (2001) 42 *Santa Clara L. Rev.* 295, 321; SEW STAFF, "What are Doorway Pages?", March 1, 2007, online: <http://searchenginewatch.com/article/2048653/What-Are-Doorway-Pages> (site consulted on September 9, 2012).

tactic in such a manner may thus present certain issues with regards to trademark infringement, as will be discussed in further detail below[271].

Another company, Overstock.com, was caught using black hat practices in February 2011 when it attempted to increase the links leading to its site[272] by "[offering] students and faculty discounts in exchange for posting links from college and university websites to Overtock.com"[273]. Due to the authoritative nature of the sites of educational institutions[274], these links managed to get Overstock.com a top spot in search results for several generic terms such as "vacuum cleaners" and "laptop computers"[275]. While websites are permitted to increase the links leading to their site in an honest manner, such as by interlinking their own websites or the pages thereon, artificially increasing the number of links in order to enhance a site's importance[276] by remunerating the individuals who create them is forbidden by Google and considered to be a black hat practice[277]. As such, Overstock was penalized by Google, resulting in them sinking low down in the list of search results[278].

Even more recently, in September 2012, it was discovered that a string of nineteen websites run by the family members of a British politician, Grant Shapps, were using a black hat technique called "scraping", which revolves around the duplication of the content of other sites that relate to keywords relevant to the topic of their site and the placement of

---

[271] *Infra*, p. 139-156.
[272] Phil TERRY, "Overstock gets a black eye from black hat", February 25, 2011, online: <http://dailyartifacts.com/overstock-gets-a-black-eye-from-black-hat > (site consulted on October 25, 2012).
[273] Eric MCGEHEARTY, "Overstock.com Busted Against – Using Black Hat SEO", August 31, 2011, online: <http://globerunnerseo.com/overstock-com-busted-again-using-black-hat-seo> (site consulted on October 24, 2012).
[274] Danny GOODWIN, "Overstock.com Lands in Google's Penalty Box Over Links-for-Discounts Deal", February 24, 2011, online < http://searchenginewatch.com/article/2049969/Overstock.com-Lands-in-Googles-Penalty-Box-Over-Links-for-Discounts-Deal > (site consulted on October 25, 2012).
[275] Amir EFRAIT, "Google Penalizes Overstock for Search Tactics", February 24, 2011, online: <http://searchenginewatch.com/article/2049969/Overstock.com-Lands-in-Googles-Penalty-Box-Over-Links-for-Discounts-Deal> (site consulted on October 25, 2012).
[276] R. MALAGA, prev. cited, note 19, 149; H. ZUZE, prev. cited, note 19, p. 37.
[277] E. MCGEHEARTY, prev. cited, note 273.
[278] A. EFRAIT, prev. cited, note 275.

that material on their own website[279]. The use of this practice was enabled by a software developed by a company owned by the politician in question[280]. Their main goal in using this tactic was to rise higher in the search results appearing on Google and ultimately increase their advertising revenue by boosting traffic to their site, but only resulted in Google penalizing them and reducing their rank in the search engine results[281]. However, it is important to note that the use of this tactic has also been known to result in the removal of the original site from the search engine's index, as the indexing software is programmed to omit any duplicate site for the purposes of avoiding redundant listings[282], and in so doing may inadvertently remove the original site from the list of results if it has been scraped[283].

These last two examples, whereby websites seek to artificially increase their rankings in search engine results or behave in a manner that may have another site removed from the search engine's index, may consist of acts of unfair competition, as will be discussed in further detail in Part II of this thesis[284]. Essentially, often times, these tactics tend to raise a site's ranking at the detriment of its competitors by using these dishonest techniques[285]. It is thus due to the unjust, and potentially illegal, nature of these tactics that

---

[279] GOOGLE, "Duplicate Content", November 17, 2011, online: <http://support.google.com/webmasters/bin/answer.py?hl=en&answer=66359> (site consulted on January 23, 2012).

[280] Rupert NEATE, "Google blacklists websites run by family of Grant Shapps", September 7, 2012, online: <http://www.guardian.co.uk/politics/2012/sep/07/google-blacklists-websites-grant-shapps-family> (site consulted on October 25, 2012); Graeme MCMILLAN, "Google blacklists sites run by a family of British politician", September 7, 2012, online: <http://www.digitaltrends.com/web/google-blacklists-sites-run-by-family-of-british-politician/> (site consulted on October 24, 2012).

[281] *Id.*

[282] Bruce CLAY and Susan ESPARZA, *Search Engine Optimization All-in-One for Dummies*, New Jersey, John Wiley & Sons, 2012, p. 333; *See also:* Fraser HOWARD and Onur KOMILI, "Poisoned search results: How hackers have automated search engine poisoning attacks to distribute malware", March 2010, p. 8, online: <http://www.sophos.com/security/technical-papers/sophos-seo-insights.pdf> (site consulted on January 23, 2012).

[283] B. CLAY and S. ESPARZA, *Id.*

[284] *Infra*, p. 117-121.

[285] Jon ROGNERUD, *Ultimate Guide to Search Engine Optimization: Drive Traffic, Boost Conversion Rates and Make Tons of Money*, 2nd ed., Irvine, Entrepreneur Press, 2011, p. 66.

causes the use of black hat techniques to be frowned upon in the cyber society[286], which is even more evident by the consequences emitted by Google to offending websites.

Subsection 2 Keyword Advertising

Keyword advertising is a form of SEM whereby a website owner purchases certain keywords upon which he will have an advantage over all other sites by "being presented together with – usually above and/or alongside – other unsponsored or "natural" search results concerning those keyword terms"[287]. Keyword advertising is often compared to the practice of using meta-tags, which are keywords that are not visible to the user but are used to communicate terms relevant to a site to search engines[288], as a means to increase a site's ranking in the search results for particular keywords[289]. The only difference between the use of meta-tags and keyword advertising is that the latter requires the payment of a fee.

The most common example of the adoption of the new advent of keyword advertising is the paid listing program developed by Google, known as Adwords, the popularity of which is significant. Its appeal to website owners is undeniable as "[b]y paying for a "sponsored link", a seller improves [his] chances of attracting customers because [his] website may appear in a discrete sponsored links section rather than buried among organic results"[290]. Though the ad format is left to the choice of the purchaser of the keywords, the most common format used is that of simple text ads that are similar in format to natural search results[291] and thus seem to be an integral part of those results.

---

[286] *See, for example:* CNN.COM, prev. cited, note 266; R. MALAGA, prev. cited, note 19.
[287] J. MOSKIN, prev. cited, note 20, 874.
[288] Jeffrey R. KUESTER and Peter A. NIEVES, "Hyperlinks, Frames and Metatags: An Intellectual Property Analysis", (1997) 38 *I.D.E.A.* 243, 247.
[289] Hung P. CHANG, "Return to Confusion: Call for Abandonment of the Initial Interest Confusion Doctrine", (2008) 12 *Intell. Prop. L. Bull.* 131, 136–138; A. TAN, prev. cited, note 20, 483.
[290] R. W. TAUBNER, prev. cited, note 20, 290.
[291] GOOGLE, "Choose an ad format", December 21, 2011, online: <http://support.google.com/adwords/bin/answer.py?hl=en&answer=1722124&topic=1713898&ctx=topic> (site consulted on January 23, 2012); A. TAN, prev. cited, note 20, 475.

It must be pointed out, however, that while using black hat SEM techniques may be viewed as a manipulation, as discussed in the previous subsection[292], it cannot be denied that keyword advertising "manipulates search results to artificially prioritize an advertiser's website over other possible results"[293] in a similar fashion. Nevertheless, due to the fact that this form of manipulation is endorsed by the search engine itself, it is not viewed as negatively as the use of black hat techniques.

As a result of the general acceptance of keyword advertising, the proliferation of its use has become extremely significant in the cyber world. The most particular use of this tool, which has become increasingly popular since this form of advertising was introduced, is the purchasing by a website of its competitor's trademark as a keyword. As a result, each time a user types in that particular trademarked term, the website in question will appear higher up in the search results than the website of the company that actually owns the trademark in question[294]. While, after several disputes[295], Google altered its policy so that "[i]f a trademark owner files a complaint with Google about the use of their trademark in AdWords ads, Google will investigate and may enforce certain restrictions on the use of that trademark in AdWords ads and as keywords"[296] the purchase of the trademarks of other companies as keywords is still a rather common occurrence. As such, this practice may fall under the gambit of trademark infringement, as will be addressed in further detail below[297].

* * *

The tactical uses of SEM are thus numerous and varied and can be used in many different fashions to increase a site's visibility on search engines, and ultimately its ability

---

[292] *Supra*, p. 55-58.
[293] Ashley TAN, prev. cited, note 20, 475.
[294] *Id.*, 474.
[295] *See, for example: Google France SARL* v. *Louis Vuitton Malletier SA*, Joined Cases C 236/08, C-237/08 & C-238/08, 2010 ECJ EUR-Lex LEXIS 119 (Mar. 23, 2010).
[296] GOOGLE, "AdWords Trademark Policy", 2012, online: <http://support.google.com/adwordspolicy/bin/answer.py?hl=en&answer=6118> (site consulted on October 18, 2012).

to reach its customers. The success of any site in the virtual world is essentially based on its ability to properly use these tactics to garner an online presence. At the same time, these techniques must be used within the boundaries of the law to ensure that the entities utilizing it are not ultimately faced with lawsuits for their online behaviour.

* * *

The first two chapters of this paper serve to demonstrate that Internet marketing is a very large and diverse domain, which includes the use of techniques allowing marketers to track individuals throughout both the physical and virtual worlds, while at the same time rendering it much simpler for them to be reached by these same individuals at all times. The use of such techniques are undoubtedly invaluable to marketers, as they serve to increase market efficiency by targeting all their advertising resources towards strategies aimed at an audience that is most likely to notice the product or service being offered[298].

Yet, while these methods are tremendously useful from a marketing perspective, their legal viability is much more questionable. These tools must thus be used in a manner that would ensure the respect of the law, while still allowing the domain of marketing to flourish with their use. In order to achieve this, however, a balance must necessarily be established between marketing goals and legal rules – a feat which is tremendously difficult to achieve when two such opposing interests are at stake. The next part of this paper will therefore be dedicated to an in-depth discussion of the various legal implications that arise from the use of these digital marketing techniques and will ultimately attempt to strike a balance between the law and the use of Internet marketing tools.

---

[297] *Infra*, p. 139-156.
[298] Susan ATHEY and Joshua S. GANS, "The Impact of Targeted Technology on Advertising Markets and Media Competition", January 11, 2009, online: <http://works.bepress.com/joshuagans/39/> (site consulted on June 4, 2011).

PART II THE LEGAL IMPLICATIONS OF DIGITAL MARKETING TECHNIQUES

The legal implications of the various digital marketing techniques described above are numerous and exist with regards to several domains of the law, namely privacy law, competition law, trademark law and consumer protection law. This part will therefore be dedicated to (1) providing an outline of privacy laws and their application to the practice of targeted marketing, and (2) to illustrating the competition, trademark and consumer protection laws and their application to the practices of SMM and SEM, so as to ultimately demonstrate the benefits that these laws present to the practice of Internet marketing from an economic perspective.

Chapter 1 Privacy Issues In Internet Marketing

The right to privacy is a fundamental right that is unequivocally protected by both Canadian and Quebec law. To begin with, while it is true that the Canadian *Charter of Rights and Freedoms*[299] does not apply to marketers, it is important to point out that sections 7[300] and 8[301] of this legislation have been broadly interpreted by the Courts as covering a right to privacy from the state[302]. In Quebec, on the other hand, the right to privacy was initially inferred by the Courts based on the notion of fault enshrined in section 1053 of the *Civil Code of Lower Canada*[303], and was later given explicit protection by the

---

[299] prev. cited, note 16.
[300] "Everyone has 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."
[301] "Everyone has the right to be secure against unreasonable search or seizure."
[302] *Hunter* v. *Southam*,[1984] 2 S.C.R. 145; *James Richardson & Sons* v. *Ministry of Nat'l Revenue*, [1984] 1 S.C.R. 614; *R.* v. *Dyment*, [1988] 2 S.C.R. 417; *R.* v. *Duarte*, [1990] 1 S.C.R. 30; Karim BENYEKHLEF, "Les dimensions constitutionnelles du droit à la vie privée", in Pierre TRUDEL and France ABRAN (dir.), *Droit du public à l'information et vie privée. Deux droits irréconciliables?*, Montreal, Éditions Thémis, 1992, p. 17-43; David H. FLAHERTY, "On the Utility of Constitutional Rights to Privacy and Data Protection", (1991) 41 *Case Western Reserve Law Review* 831, 844-845; Martine GINGRAS, "Quand *Big Brother* fait du pouce sur l'inforoute", 1997, p. 7, online: <http://commposite.org/index.php/revue/article/view/109/87> (site consulted on March 18, 2012); Benoit PELLETIER, "La protection de la vie privée au Canada", (2001) 35 *R.J.T.* 485, 485.
[303] *Robbins* c. *Canadian Broadcasting Corporation*, [1958] C.S. 152; *Field* c. *United Amusement Co.*, [1971] C.S. 283; *Reibeiro* c. *Shawinigan Chemicals*, [1973] C.S. 389; *Deschamps* c. *Renault Canada*, [1977] 18 C. de D. 1937; P. TRUDEL, F. ABRAN, K. BENYEKHLEF and S. HEIN, prev. cited, note 29, p. 11-23.

Quebec *Charter of Human Rights and Freedoms*[304] as well as by the *Civil Code of Quebec*[305]. Additionally, privacy is protected under Quebec law through the *Act Respecting the Protection of Personal Information in the Privacy Sector*[306] which serves to set the parameters that must be respected by companies when dealing with the personal information of Quebec citizens.

Unfortunately, the rise of Internet tracking technology that enables the gathering of unbelievable amounts of personal information[307] has severely threatened the protection of this right as prescribed by both Canadian and Quebec legislation. The existence of this technology has given rise to "cyber voyeurism"[308], essentially allowing for the invasion of the private lives of individuals worldwide[309] and thus "by this fact rendering possible intrusions or divulgations that would have otherwise been inconceivable"[310] (our translation).

In light of this new reality and in the hopes of responding to these threats, the Federal government adopted both the *Personal Information Protection and Electronic Documents Act*[311] and the *Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act*[312] as a means to further ensure the protection of the privacy of Canadian citizens. Similarly, the *Act to*

---

[304] *Charter of Human Rights and Freedoms*, prev. cited, note 15, section 5 (hereafter referred to as the "Quebec Charter"); For application in jurisprudence, *see: Reid* c. *Belzile*, [1980] C.S. 717 (C.S. Q.C.); *Centre local de services communautaires de l'érable* c. *Lambert*, [1981] C.S. 1077; *The Gazette* c. *Valiquette*, [1997] R.J.Q. 30 (C.A.).
[305] *Civil Code of Quebec*, prev. cited, note 15, sections 3, 35 and 36 (hereafter referred to as the "C.C.Q.).
[306] prev. cited, note 15 (hereafter reffered to as the "ARPPIPS").
[307] P. TRUDEL, F. ABRAN, K. BENYEKHLEF and S. HEIN, prev. cited, note 29, p. 11-20.
[308] B. PELLETIER, prev. cited, note 302, 485.
[309] *Id.*
[310] P. TRUDEL, F. ABRAN, K. BENYEKHLEF and S. HEIN, prev. cited, note 29, p. 11-20.
[311] prev. cited, note 16 (hereafter referred to as the "PIPEDA").
[312] prev. cited, note 16, (hereafter referred to as the "Anti-Spam Act").

Establish a Legal Framework for Information Technology[313] was emitted in Quebec in order to adapt to the new position we find ourselves in as a result of modern technology and contains certain sections meant to ensure privacy protection.

The possibility of an individual's privacy being violated in this new technological age is significantly increased, especially since the Internet serves to amplify the number of situations in which privacy protection must be afforded. Two such situations to which the right to privacy extends are (1) the right to control ones personal information[314] and (2) the right to live in peace and solitude without intrusions nor interruptions[315] – two violations which are enabled by the technological tracking tools used for targeted marketing purposes and which will be discussed in further detail heretofore.

Section 1 The Protection of Personal Information in Canadian and Quebec Law and Its Application to the Practice of Targeted Marketing

The protection of personal information is one of the elements that are safeguarded by the right to privacy. Such a protection is necessary as it is considered as a prelude to free, open, and honest communication[316] – all elements upon which marketers rely to acquire the behavioural data of individuals for the purposes of targeted marketing. A lack of privacy protection could create a strain on the behaviour of individuals, resulting in a

---

[313] prev. cited, note 15 (hereafter referred to as the "AELFIT").
[314] INDUSTRY CANADA, *La protection de la vie privée et l'autoroute canadienne de l'information: une nouvelle infrastructure de l'information et des télécommunications*, Ottawa, Industry Canada, 1994, p. 5; Pierre TRUDEL and Karim BENYEKHLEF, "Approches et stratégies pour améliorer la protection de la vie privée dans le contexte des inforoutes", p. 14, online: <https://depot.erudit.org/bitstream/002690dd/1/0072.pdf> (site consulted on March 17, 2012); Ana Isabel VICENTE, "La convergence de la sécurité informatique et de la protection des renseignements personnels : Vers une nouvelle approche juridique", 2003, p. 9, online : <http://www.lex-electronica.org/docs/articles_114.pdf> (site consulted on October 18, 2012); Alan F. WESTIN, *Privacy and Freedom*, New York, Athenum, 1967, p. 7.
[315] *R.* v. *Dyment*, prev. cited, note 302, par. 19-20; Jean-Louis BAUDOUIN, *La Responsabilité Civile*, 4th ed., Cowansville, Yvon Blais, 1994, no. 393, p. 225; D. H. FLAHERTY, prev. cited, note 302; INDUSTRY CANADA, *Id.*
[316] Richard A. POSNER, "John A. Sibley Lecture: The Right of Privacy", (1978) 12-3 *Georgia Law Review* 393, 403-404; Richard A. POSNER, "The 1978 James McCormick Mitchell Lecture: Privacy, Secrecy, and Reputation", (1978) 28 *Buffalo Law Review* 1, 17-20; *See also:* Ruth GAVISON, "Privacy and the Limits of Law", (1980) 89-3 *The Yale Law Journal* 421.

much more subdued and less open manner, ultimately adversely affecting society as a whole[317], and placing marketers at risk of losing access to this crucial data.

This effect on the inter-personal communications of individuals could manifest itself in one of two ways, the second being more detrimental to marketers than the first, but both of which are still severe. To begin with, minimal privacy safeguards may result in increasing preference falsification[318], which is "the act of misrepresenting one's genuine wants under perceived social pressures"[319]. The knowledge that their personal data is not kept private, will often cause individuals to adhere to acceptable norms and reject their private preferences for the sake of blending in with the majority[320], which could be harmful to the practice of targeted marketing as it would skew behavioural data[321].

Even more pressing than the possibility of preference falsification, however, is the second possible outcome, where individuals will limit their use of the Internet or mobile telephones as a result of privacy concerns, thus severely restraining the amount of

---

[317] R. A. POSNER, "John A. Sibley Lecture: The Right of Privacy", *Id.*; R. A. POSNER, "The 1978 James McCormick Mitchell Lecture: Privacy, Secrecy, and Reputation", *Id.*; *See also:* R. GAVISON, *Id.*

[318] Paul M. SCHWARTZ, "Internet Privacy and the State", (1999-2000) 32 Conn. L. Rev. 815, 840.

[319] Timur KURAN, *Private Truths, Public Lies: The Social Consequences of Reference Falsification*, Cambridge, Harvard University Press, 1995, p. 23-24; Richard H. MCADAMS, "The Origin, Development and Regulation of Norms", (1997) 96 *Mich. L Rev.* 338,419-424.

[320] P. M. SCHWARTZ, prev. cited, note 318, 841.

[321] On the other hand, however, it has been held that "the cover of privacy might encourage individuals not only to engage in activity unjustifiably stigmatized but also justifiably stigmatized" (Jerry KANG, "Information Privacy in Cyberspace Transactions", (1998) 50 *Stanford Law Review* 1193, 1218-1219) essentially enabling deception and self-misrepresentation. While it would be impossible to deny that privacy does enable such an outcome, it is also impracticable to presume that one's desire to conceal information about themselves means that they have something to hide (*Id.*, 1219; *See also:* Edward J. BLOUSTEIN, "Privacy Is Dear at Any Price: A Response to Professor Posner's Economic Theory", (1978) 12 *Ga. L. Rev.* 429, 445). In fact, there are many instances in which secrecy is necessary without possessing the intention to mask a lie – take the secret ballot, for example (J. KANG, *Id.*). Furthermore, an individual cannot be considered at fault for behaving differently under varying circumstances and essentially concealing certain aspects of his personality. Such behaviour is rather an inherent part of society; an individual will not behave the same within the confines of his home as he will at work, for example, and it is this "ability to maintain divergent public and private personae [that] creates the elbowroom necessary to resist social and political homogeneity" (*Id.*, 1220). In such a manner, we reach the same conclusion previously established which holds that privacy protection is necessary to avoid preference falsification, which is a state of affairs that is crucial for marketing to be efficient. In this light, the instauration of legislation to protect the personal information of individuals, makes a great deal of sense and, in our opinion, can be construed as nothing other than beneficial to online marketers.

behavioural data available to marketers. To provide an example, many individuals are apprehensive about making online purchases as they are concerned that their credit card information will not be properly protected, and "[with] additional instances of intrusion, that fear will increase. The harm here is not simply commercial – for if […] individual users' personal files [are targeted], people will reduce their connections to the Internet"[322]. Such an end result would be undesirable to marketers, as it is upon the use of the Internet that they depend to obtain the data they require for their purposes, and it is therefore crucial for them to adopt an approach that will assuage the fears of Internet users by properly protecting their personal information.

The manner in which the personal information of individuals is protected is outlined by the PIPEDA[323] and the new Anti-Spam Act[324], on a Canadian level, and the ARPPIPS[325], as well as the C.C.Q.[326] and the AELFIT[327], on a Quebec level. This protection is limited to the collection, use and retention of what is considered by the PIPEDA and the ARPPIPS as personal information, therefore covering any data collected or used for the practice of targeted marketing.

Depending on the nature of the enterprise or organization gathering the information considered by these laws to be personal, however, the law that will apply will differ. The PIPEDA only applies in provinces that have not enacted substantially similar privacy laws, and in those that have, it will only apply to the federally regulated private sector and to personal information emitted in inter-provincial and international transactions by all

---

[322] Neal K. KATYAL, "The Dark Side of Private Ordering: The Network/Community Harm of Crime", in Mark F. Grady and Francesco Parisi (dir.), *The Law and Economics of Cybersecurity*, New York, Cambridge University Press, 2006, 193, at page 197.
[323] *Personal Information Protection and Electronic Documents Act*, prev. cited, note 16.
[324] *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act*, prev. cited, note 16.
[325] *An Act Respecting the Protection of Personal Information in the Private Sector*, prev. cited, note 15.
[326] *Civil Code of Quebec*, prev. cited, note 15.
[327] *Act to establish a Legal framework for information technology*, prev. cited, note 15.

organizations engaged in commercial activities[328]. Quebec's adoption of the ARPPIPS therefore renders the PIPEDA inapplicable upon the territory of that province except with regards to those two particular sectors.

While the PIPEDA applies to any organization that collects information in the course of commercial activity[329], the ARPPIPS applies to all private sector enterprises which is defined by article 1525 C.C.Q as "[t]he carrying on by one or more persons of an organized economic activity, whether or not it is commercial in nature, consisting of producing, administering or alienating property, or providing a service", thus encompassing a much larger sphere of activities than the federal law. The area of application of both of these laws, however, is commonly interpreted largely so as to ensure that the personal data of both Canadian and Quebec citizens alike is protected to the highest possible extent[330].

In light of the differing spheres of application of these laws, this section will (1) outline precisely what information collected through technological tracking tools is considered to be personal data by both the PIPEDA and the ARPPIPS, in order to ultimately (2) be able to determine the protection afforded to the information aggregated for targeted marketing purposes by both of these laws.

---

[328] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "PIPEDA Self-Assessment Tool: Personal Information Protection and Electronic Documents Act", August 12, 2008, online: <http://www.priv.gc.ca/information/pub/ar-vr/pipeda_sa_tool_200807_e.cfm> (site consulted on March 17, 2012).

[329] *Personal Information Protection and Electronic Documents Act*, prev. cited, note 16, section 4(1)(a).

[330] With regards to the PIPEDA, *See: Dagg* v. *Canada (Minister of Finance)*, [1997] 2 S.C.R. 403, par. 68 (J. La Forest, dissenting); *Canada (Information Commissioner)* v. *Canada (Commissioner of the Royal Canadian Mounted Police*), [2003] 1 S.C.R. 66, par. 23; *Canada (Information Commissioner)* v. *Canada (Transportation Accident Investigation and Safety Board)*, 2006 F.C.A. 157; With regards to the ARPPIPS, *See: Adam* v. *Gauthier*, [1997] C.A.I 18; *Québec (Sous-ministre du revenu)* c. *Lasalle*, J.E. 97-1575 (C.Q.); *Gauthier* c. *Syndicat des employés de la Bibliothèque de Québec*, [1997] C.A.I 1; *Institut d'assurance du Canada* c. *Guay*, J.E. 1998-141 (C.Q.); *Beaudoin* c. *Syndicat canadien des communications, de l'énergie et du papier (S.C.E.P.), section locale 530*, [2001] C.A.I 188; *Reeves* c. *Fasken Martineau DuMoulin*, [2001] C.A.I 322; Karl DELWAIDE and Antoine AYLWIN, "Learning From a Decade of Experience: Quebec's Private Sector Privacy Act", 2005, p. 6, online: <http://www.priv.gc.ca/information/pub/dec_050816_e.pdf> (site consulted on March 17, 2012).

Subsection 1 The Qualification of Information Collected Through Tracking Tools as Personal Data

Both the PIPEDA and the ARPPIPS provide very similar definitions of the term personal information. The PIPEDA considers personal information to be any "information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization"[331]. The ARPPIPS, on the other hand, defines personal information as "any information which relates to a natural person and allows that person to be identified"[332]. Both of these definitions lack a certain specificity as to which precise forms of data could fall under this category. Case law related to this matter, however, requires a broad and expansive interpretation of the term "personal information"[333]. As such, general consensus holds that, to qualify as personal information, the data in question need not specifically identify the person to whom the information relates, but must merely *allow for the possibility* of that person's identity to be determined[334]. With regards to the practice of targeted marketing, this definition thus begs the question of which data collected through the use of both online and mobile tracking tools renders it possible to identify individuals when combined, and can thus ultimately be considered to be personal information[335].

---

[331] *Personal Information and Electronic Documents Act*, prev. cited, note 16, section 2.
[332] *Act Respecting the Protection of Personal Information in the Private Sector*, prev. cited, note 15, section 2.
[333] *Dagg* v. *Canada (Minister of Finance)*, prev. cited, note 330, par. 68 (J. La Forest, dissenting); *Canada (Information Commissioner)* v. *Canada (Commissioner of the Royal Canadian Mounted Police)*, prev. cited, note 330, par. 23; *Canada (Information Commissioner)* v. *Canada (Transportation Accident Investigation and Safety Board)*, prev. cited, note 330.
[334] With regards to the PIPEDA, *see: Gordon* v. *Canada (Health)*, 2008 F.C. 258; With regards to the ARPPIPS, *see: Antonio Sergi* c. *Ville de Mont Royal*, [1977] C.A.I. 198; *E.* c. *Office de la protection du consommateur*, [1987] C.A.I. 350; *Ségal* c. *Centre de services sociaux de Québec*, [1988] C.A.I. 315; Diane POITRAS and Lina DESBIENS, "Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et Loi sur la protection des renseignements personnels dans le secteur privé, textes annotés", S.O.Q.U.I.J., 1996, p. 269; P. TRUDEL and K. BENYEKHLEF, prev. cited, note 314, p. 3; A. I. VICENTE, prev. cited, note 314, p. 9-13.
[335] *Gordon* v. *Canada (Health)*, *Id.*, par. 33.

As discussed above[336], the forms of data collected with the use of such tools are varied in nature, but namely relate to data regarding an individual's personal preferences and interests that may be inferred from browsing history, online purchases and search engine queries, and often include IP address, email address, online communications, and physical location. The qualification of data regarding the personal preferences of individuals through the use of both Internet and mobile tracking tools as personal information is not so cut and dry, and must be analyzed in light of the characteristics of the technology utilized to acquire the data in question.

When cookies are used to gather information relating to consumer interests, the cookies in question often contain a unique identifier that excludes the name and email address of the individual with whom the cookie is shared, ultimately allowing the person to remain anonymous[337]. In this grain, one would believe that the data collected through cookies cannot be linked back to an identifiable person thus making it questionable as to whether such information can be classified as personal or not[338]. Such an impression is, however, false, as "[t]he profiles derived from tracking online users' activities on the Internet may be linked or merged with the [personally identifiable information] of these users"[339] thus de-anonymizing these individuals by identifying them through data that is publicly available[340]. There is therefore no guarantee that cookies which are programmed to maintain the anonymity of individuals will not ultimately serve to identify them. It is due to this possibility to de-anonymize the information contained within cookies that the

---

[336] *Supra*, p. 10-43.
[337] Eloïse GRATTON, *Internet and Wireless Privacy: A Legal Guide to Global Business Practices*, Toronto, CCH Canadian, 2003, p. 46.
[338] *Id.*
[339] *Id.*; Cynthia CHASSIGNEUX, "La protection des informations à caractère personnel", in Eric LABBÉ, Daniel POULIN, François JACQUOT and Jean-François BOURQUE (dir.), *Le guide juridique du commerçant électronique*, p. 171-172, online : <http://www.jurisint.org/pub/05/fr/guide_final.pdf> (site consulted on March 21, 2012).
[340] J. LO, prev. cited, note 11, p. 52.

Privacy Commissioner of Canada came to the conclusion that any data collected through the use of cookies is considered to be personal information[341].

Even in the event that the information collected through cookies is not combined with any personally identifiable data about an individual, however, the chance that this individual could be identified still exists. To begin with, in most cases, cookies collect the IP address of the consumer upon whose computer the cookie resides – a piece of information which may be able to identify the individual[342]. The consideration of an IP address as personal data would, however, most likely be based on whether the address in question is dynamic, meaning that it varies each time an individual connects to the Internet, or static, meaning that it is an address that uniquely identifies an individual's computer or device[343]. It is only in the latter case that an IP address could be qualified as personal information[344], and if this type of address is collected by cookies, the data therein would ultimately fall under the spheres of application of both the PIPEDA and the ARPPIPS.

---

[341] *Finding #162*, 2003 CanLII 37655 (P.C.C.).

[342] E. GRATTON, prev. cited, note 337, p. 46; *Finding* #25, 2001 CanLII 21526 (P.C.C.); *Finding #315*, 2005 CanLII 37355 (P.C.C.); *Finding #319*, 2005 CanLII 50763 (P.C.C.); *Finding #2009-010*, September 2009, online: <http://www.priv.gc.ca/cf-dc/2009/2009_010_rep_0813_e.cfm> (site consulted on March 16, 2012).; *See also:* CANADIAN RADIO-TELEVISION AND TELECOMMUNICATIONS COMMISSION, "Telecom Regulatory Policy CRTC 2009-657: Review of the Internet traffic management practices of Internet service providers", October 21, 2009, online: <http://www.crtc.gc.ca/eng/archive/2009/2009-657.htm> (site consulted on February 18, 2012); OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "Review of the Internet traffic management practices of Internet service providers: Submission of the Office of the Privacy Commissioner of Canada to the Canadian Radio-television and Telecommunication Commission (CRTC)", March 3, 2009, online: <http://www.priv.gc.ca/information/pub/sub_crtc_090218_e.cfm> (site consulted on February 18, 2012); OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "Review of the Internet traffic management practices of Internet service providers: Final reply of the Office of the Privacy Commissioner of Canada to the Canadian Radio-television and Telecommunication Commission (CRTC)", September 15, 2009, online: <http://www.priv.gc.ca/information/pub/sub_crtc_090728_e.cfm> (site consulted on February 18, 2012).

[343] E. GRATTON, *Id.*, p. 46.

[344] *Id.*; *Finding* #25, prev. cited, note 342; *Finding #315*, prev. cited, note 342; *Finding #319*, prev. cited, note 342; *Finding #2009-010*, prev. cited, note 342; *See also:* CANADIAN RADIO-TELEVISION AND TELECOMMUNICATIONS COMMISSION, prev. cited, note 342; OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, prev. cited, note 342; OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, prev. cited, note 342.

Additionally, while it is true that cookies do not automatically store the email address of an individual[345], there are certain situations in which individuals are prompted by websites to provide their email address and in such cases, the address typed in by these people *is* saved within the cookie, which could ultimately jeopardize the anonymous nature of the information collected by cookies should the email address in question allow the person to whom it belongs to be identified[346]. Although not all email addresses can be linked to the individuals to whom they belong[347], they have generally been considered to constitute personal information as they could *allow for the possibility* of a person to be identified[348]. Thus, since there is a serious possibility that individuals may be "identifiable" or "identified" through the data collected by cookies, whether it be because it could be linked to other identifiable data or because it could contain a static IP address or an email address that could lead to the identification of an individual, all the information contained within cookies must therefore qualify as personal information[349].

While the data aggregated through the use of cookies presents a certain debate with regards to the nature of that data, there can be no question that information collected through the practice of DPI qualifies as personal information. Essentially, the practice of DPI "raises privacy concerns because it can involve the inspection of information […] sent over the Internet"[350] by their users. While many ISPs claim that the data they gather in this manner for targeted advertising purposes is anonymous[351], they are still in the position of

---

[345] Khoa Duc TRAN, "Cookies: Technology and Security Issues", p. 6, online: <http://home.earthlink.net/~ktran/research_papers/Cookies%20Technology%20and%20Security%20Issues.pdf> (site consulted on September 6, 2012).
[346] R. K. ZIMMERMAN, prev. cited, note 29, 443.
[347] E. GRATTON, prev. cited, note 337, p. 44-45.
[348] *Finding #13*, 2009 CanLII 74730 (P.C.C.); *Id.*, p. 45; OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "A Guide for Individuals: Your Guide to PIPEDA", April 2009, online: <http://www.priv.gc.ca/information/02_05_d_08_e.cfm< (site consulted on February 13, 2012).
[349] *E.* c. *Office de la protection du consommateur*, prev. cited, note 334; *Gordon* v. *Canada (Health)*, prev. cited, note 334.
[350] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "What is Deep Packet Inspection?", online: <http://dpi.priv.gc.ca/index.php/what-is-deep-packet-inspection/> (site consulted on February 20, 2012).
[351] Alex CAMERON, "Facebook, Streetview, and What's Next: Navigating Your Way Through New Issues in Privacy Law", April 23, 2010, p. 38, online: <http://www.fasken.com/files/Publication/78b5cf7e-31cf-4654-

identifying the users in question, thus rendering the individuals affected by this technology identifiable[352] and causing the data collected in such a manner to be considered as personal information as prescribed by both the PIPEDA and the ARPPIPS.

It is not, however, only the data that is collected via online tracking tools that must be examined to determine its qualification as personal information, but also any data collected using mobile tracking methods, namely with regards to physical location. As discussed above[353], various positioning systems accessible through cellular telephones are used to locate individuals and target them with real-time advertisements based on their particular position at a given moment. Since each cellular telephone has a unique Mobile Identification Number[354], a number which can be captured and possibly linked back to the individual to whom the device belongs[355], any data collected through cellular phones allows for the possibility of the identification of an individual, thus causing this data to be considered as personal information[356].

It must be pointed out, however, that the privacy risks associated with the use of tracking tools to collect data about individuals do not end with the information voluntarily collected in this manner, but also extend to the data that is accidentally aggregated throughout the procedures involved with the use of these tools – a risk that exists mainly with regards to the practice of wardriving used to create Wi-Fi Positioning Systems, as discussed above and illustrated with the example of Google's involuntary aggregation of personal information using this method[357]. In this case, it was considered by the Office of the Privacy Commissioner that "[w]hile the raw data collected by Google would not always

---

b6a0-5fd2adea69fb/Presentation/PublicationAttachment/9d6f81cb-f178-4bc3-b302-5fd4b4c87e63/Alex_Cameron_LSUC_2010_Paper.pdf> (site consulted on February 20, 2012).

[352] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "Review of the Internet traffic management practices of Internet service providers", March 3, 2009, online: <http://dpi.priv.gc.ca/index.php/essays/review-of-the-internet-traffic-management-practices-of-internet-service-providers/> (site consulted on February 20, 2012).

[353] *Supra*, p. 32-41.

[354] *See: Supra*, p. 35.

[355] E. GRATTON, prev. cited, note 337, p. 47.

[356] *Id.*

[357] *Supra*, p. 37.

allow for perfect identification, the information collected was sufficiently capable of being linked to individuals through data matching or aggregation"[358].

The amount of data that qualifies as personal information that is collected, both purposely and inadvertently, through the use of technological tracking tools, online as well as mobile, is thus significant and ultimately places a strain on marketers who desire to collect this data for targeted marketing purposes. In this light, we are led to wonder whether or not the definition of personal information held by both the PIPEDA and the ARPPIPS, which places a significant amount of data under the gambit of this term, may unnecessarily reduce the economic benefits presented by these laws. This is due to the fact that the definitions upheld by the law neglect to distinguish between data that truly presents privacy risks and that which does not, and therefore forces marketers to spend their resources protecting information that may not necessarily require protection[359]. From this perspective, it has been considered that

> "the definition of the notions of personal information in both the Quebec [and Canadian] laws is too general : it prevents the circulation of information that has no effect on the privacy of individuals and ultimately results in a dilution of the protection of information that truly falls in the domain of privacy.
>
> […]
>
> The notion of privacy does not cover all the information regarding a person. Considering we live in society, there are elements of each person's activities that possess a public characteristic. By ignoring this and by persisting to promote a general definition, such as the notion of "personal information", we expose ourselves to placing a hoard of information under protection (essentially, all the information that concerns a person and permits them to be identified) and we find ourselves under the obligation of multiplying the circumstances under which it would be necessary, in the name of

---

[358] *Id.*

[359] Vincent GAUTRAIS, "Introduction générale : Le défi de la protection de la vie privée face aux besoins de circulation de l'information personnelle", June 5, 2003, p. 9, online : <http://www.lex-electronica.org/docs/articles_107.pdf> (site consulted on March 22, 2012).

> public welfare, to wave (by the multiplication of dispensatory provisions) certain protections that may be essential to the preservation of the privacy of each person."[360] (our translation)

If the law were thus to limit its definition of personal information solely to that data which is truly private[361], the obligation of marketers to protect the personal information of individuals would be less onerous, as this limitation would, in consequence, minimize the resources that they would be obliged to dedicate to the protection of this data. This would, however, require an adjustment of privacy laws to prevent organizations from attempting to positively identify individuals by linking the private information that they have collected with data that is publicly available about these people[362]. Such a modification would be much more economically sound than requiring that protection be afforded to any information that may potentially identify a person, which extends to numerous types of information, as exposed throughout this section in light of the case of targeted marketing. This in turn would reduce the costs associated with the implementation of privacy protection for marketers, while still allowing adequate protection for the personal information of individuals that is truly private.

Regardless of the enlarged definition of personal information enshrined in both the PIPEDA and the ARPPIPS, and whether or not it may be economically sound, the fact remains that all the data identified in this section as falling under the definition of personal information must effectively be protected in the manner set forth by both the PIPEDA and the ARPPIPS. In order to ensure that the private nature of this information is protected in the realm of cyberspace, both of these laws have emitted certain rules and principles that must be respected by all enterprises and organizations throughout their collection, use and retention of personal data, which will be discussed in further detail in the next subsection.

---

[360] P. TRUDEL and K. BENYEKHLEF, prev. cited, note 314, p. 3 and 11.
[361] *Id.*, p. 12; V. GAUTRAIS, prev. cited, note 359, p. 9.
[362] P. TRUDEL and K. BENYEKHLEF, *Id.*, p. 13.

Subsection 2 Principles of Privacy Protection

Since the data collected by marketers using both online and mobile tracking tools qualifies as personal information in the sense accorded to the term by both the PIPEDA and the ARPPIPS[363], marketers are required to abide by these laws when they collect, use and retain such data for targeted marketing purposes. While both these laws pose various principles[364] that ensure the protection of the privacy of Canadian and Quebec citizens as a whole, this thesis will concentrate upon two principles that we believe present the greatest issues with regards to the practice of targeted marketing, namely those relating to (a) identifying the purposes for which personal information is collected and being transparent about the privacy practices of the entity collecting the information, and (b) acquiring the consent of the individual whose personal data is being collected, used and retained, both of which will be discussed in further detail heretofore.

Paragraph 1 Identifying Purposes and Disclosure

Both the PIPEDA[365] and the ARPPIPS[366] require that the purposes for which the personal information of an individual is being collected be identified. While the PIPEDA specifies the point in time at which these purposes must be brought forth, namely upon the aggregation of that data or prior to that time, the ARPPIPS makes no such specification. According to the ARPPIPS, these purposes must be explained to the individual whose

---

[363] *See: Supra*, p. 68-74.

[364] The other principles are: (1) Accountability of the organization for the personal information under its control; (2) Limiting the collection of personal information to that which is necessary for the purposes identified by the organization; (3) Limiting the use, disclosure and retention of the personal information solely to that which is required to accomplish the identified purposes; (4) Accuracy of the personal information in the organization's possession; (5 The implementation of safeguards to protection the personal information in the possession of the organization; (6) Openness with regards to the policies and practices of the organization with regards to the management of the personal information in its possession; (7) Providing access to the individual whose personal information is in the possession of the organization; (8) Providing the individual with the ability to challenge the compliance of the organization to these principles to the individual accountable for the organization's compliance.

[365] *Personal Information Protection and Electronic Documents Act*, prev. cited, note 16, Schedule 1, section 4.2.

[366] *Act respecting the Protection of Personal Information in the Private Sector*, prev. cited, note 15, section 14.

information is being collected by outlining the subject of the file being created in his respect as well as the manner in which his data will be used and the categories of individuals who will have access to this information[367], essentially holding that "consent to the collection […] of personal information […] must be given for specific purposes"[368]. This therefore means that consent to the collection of such data can only exist when the purposes for such collection are exposed and thus that no collection can occur prior to the description of the reasons for which such compilation is taking place. As such, this would lead us to believe that the point in time at which the purposes must be identified in light of the ARPPIPS is the same as that ordered by the PIPEDA – which in both cases is a requirement that serves as a prelude to ensure that, when the consent of the individual is ultimately acquired, it will be free and enlightened[369].

The requirement for the identification of the purposes for which an individual's personal data is being aggregated, prior to the collection of that information, appears to be viable from an economic analysis perspective, particularly when it comes to the case of targeted marketing. A study conducted in 2007 demonstrated that disclosure by websites as to their treatment of personal information induced more individuals to be forthcoming with the provision of this data[370]. Interestingly enough, their willingness to communicate this information did not change regardless of whether or not they had actually read the disclosure statement provided[371]. These findings are in accordance with the general standing that the disclosure of privacy practices by a company "help consumers make a

---

[367] *Id.*, section 8.
[368] *Id.*
[369] *Id.*; *Personal Information Protection and Electronic Documents Act*, prev. cited, note 16, Schedule 1, section 4.3.2; Ann CAVOUKIAN and Mike GURSKI, "Privacy in a wireless world", January 1, 2002, online: <http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=334> (site consulted on March 21, 2002); Evelyne Beatrix CLEFF, "Mobile advertising regulation: Implementing the legal criteria of meaningful consent in the concept of mobile advertising", (2007) 23 *Computer Law & Security Report* 262, 265; Eloïse GRATTON, "M-commerce: The Notion of Consumer Consent in Receiving Location-Based Advertising", (2002) 1-2 *C.J.L.T.* 59, 65.
[370] Kai-Lung HUI, Hock Hai TEO and Sang-Yong Tom LEE, "The Value of Privacy Assurance: An Exploratory Field Experiment", (2007) 31-1 *MIS Quarterly* 19, 26.
[371] *Id.*, 27.

more accurate assessment of the risks of [providing] personal information to websites, and therefore displaying them should promote consumer [cooperation]"[372].

In this light, the economic benefit for marketers to provide adequate disclosure is rather significant as it will increase the amount of behavioural data available to them, while at the same time ensuring privacy protection and thus less of a risk of inhibited communications and preference falsification, as discussed above[373]. However, in order for this goal to be achieved to its highest possible extent, disclosure must be provided to individuals at the precise moment at which their personal data is being collected. If this data is collected without any prior notification and individuals are only sought out to provide consent once it has already been aggregated, they may feel blindsided, as if they have no control over their personal data, and may ultimately end up harbouring the outlook that their private information is collected without their knowledge, which may therefore result in the predicament that is striving to be avoided through disclosure in the first place.

In order to affirm that the purposes for collection are properly identified it is crucial to determine both who should be responsible for providing such information as well as the form that it should take. To begin with, both the PIPEDA and the ARPPIPS state that the purposes for the collection of personal information must be exposed, but nowhere do these laws specifically state who should be the one to provide it[374]. This complicates matters when it comes to online targeted advertising, as, while the entity who collects the information is generally the one who ultimately uses it, it often occurs that the data may be collected by one entity and sold to another who uses it for advertising purposes[375]. Yet,

---

[372] *Id.*, 20; *See also:* George R. MILNE and Mary J. CULNAN, "Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices", (2004) 18-3 *Journal of Interactive Marketing* 15.
[373] *Supra*, p. 65.
[374] E. GRATTON, prev. cited, note 369, 63.
[375] *Id.*

while this may be a common practice when it comes to targeted marketing[376], and it is here that the PIPEDA and the ARPPIPS differ, the Quebec law prohibits the acquisition of an individual's personal data from a third-party but rather holds that such data must be directly acquired from the person in question[377], whereas the PIPEDA implies that such data may be attained from third parties[378]. Thus, for the intents and purposes of the ARPPIPS, although it does not specifically state who should be responsible for identifying the purposes of collection, due to the fact that data must always be collected directly from an individual and cannot be sold to third parties, the question of who should provide disclosure is moot.

When it comes to the PIPEDA, however, determining who should be the one to provide disclosure in cases where the personal data of individuals is transmitted to third parties is not nearly so clear cut. In such cases, it is crucial to establish whether or not it should be up to the entity that collects the information or the third-party who ultimately uses the data to identify the purposes for collection. According to the PIPEDA, however, any entity who either collects, uses or discloses the personal data of an individual is faced with the obligation of identifying the purposes for collection[379].

This requirement makes a great deal of sense, as it is rather difficult to conceive the manner in which the entity collecting the data can provide information regarding the exact purposes for which the data is collected when they ultimately sell this data to a third-party and do not possess sufficient details regarding the manner in which this third-party will utilize that information. Thus, the entity that aggregates the data for the purposes of selling it to a third-party must disclose this particular use to consumers. In such cases, however, it would not be sufficient for this entity to state that they share this information with an "affiliate" or a "third-party" or a "partner", as these vague terms are rather unclear and do

---

[376] *See for example:* Blachander KRISHNAMURTHY and Craig E. WILLS, "On the Leakage of Personally Identifiable Information Via Online Social Networks", August 17, 2009, online: <http://www2.research.att.com/~bala/papers/wosn09.pdf> (site consulted on September 10, 2012).
[377] *Act respecting the Protection of Personal Information in the Private Sector*, prev. cited, note 15, section 6.
[378] *Personal Information Protection and Electronic Documents Act*, prev. cited, note 16, Schedule 1, sections 4.3.7(b), 4.9.1, 4.9.3 and 4.9.5.
[379] *Id.*, Schedule 1, section 4.3.

not really inform the individual as to who ultimately uses their personal data[380]. The third-party who acquires that data must then notify the individual in question and ultimately identify the manners in which they will be using that information for their own purposes.

While this solution may be impractical, we believe that it is the only one that would make sense in light of the ultimate goals meant to be achieved. Essentially, if one entity collects data for the purposes of selling it to a third-party, and the individual whose personal data was aggregated for this purpose is notified solely of the collector's intention to sell, but receives no information regarding the manner in which the purchaser will utilize that data, this lack of knowledge will make it difficult for him to be able to assess the risks involved with providing these entities with access to his personal information, and may thus result in his refusal to consent to any use of his data. This outcome would, however, not be beneficial to marketers. As such, it would still be more advantageous for marketers to invest additional funds in providing adequate notification to individuals regarding precisely how their personal data will be utilized by each entity, whether it is the direct collector or the third-party that will eventually use that data, rather than risking an individual's refusal to provide his consent due to lack of information in this respect and ultimately rendering it impossible for marketers to use this behavioural information for targeted advertising purposes.

When it comes to targeted advertising on mobile telephones, on the other hand, the actors involved are much more numerous, and it is difficult to know whether the entity to provide disclosure should be the one who supplies the location-based advertising services, the telecommunications company with whom the owner of the cellular phone is subscribed, or the advertisers and content providers[381]. While it has been considered that all of these entities are required to provide disclosure, such a view may not be practical and may serve

---

[380] J. LO, prev. cited, note 11, p. 51-52.
[381] E. GRATTON, prev. cited, note 369, 63; Eloïse GRATTON, *Wireless Privacy and Personalized Location-based Services: The Challenge of Translating the Legal Framework into Business Practices*, Master's thesis, Montreal, Faculté des études supérieures, University of Montreal, 2002, p. 58.

to further confuse the user by overloading him with information[382], as, differently from online targeted advertising where there will be a maximum of two actors involved in a particular collection, there are twice as many entities involved in mobile targeted marketing. As such, it has been considered that it may be possible, and more effective, that disclosure by the wireless service provider at the time of the conclusion of the contract with the user is sufficient to adequately provide disclosure to the individual and render it unnecessary for any further disclosures by location-based service providers[383].

While we agree that this solution would ultimately be more effective from a practical point of view, we believe that its economic efficiency may not be so clear cut. Requiring each of the actors involved in mobile marketing to identify the purposes for their collection of the personal data of individuals would be quite costly – much more so than in the case of online targeted marketing as the number of actors implicated is doubled. At the same time, however, such an all-global clause may be viewed by individuals as a lack of disclosure, which may result in their refusal to consent to use of their personal data for similar reasons as those outlined with regards to the case of the sale of personal data to third parties[384]. As such an outcome would be undesirable, we believe that a possible solution to this issue would be for the telecommunications provider to include a clause in its contract with respect to the manner in which the mobile telephone holder's location information will be used by each location-based service provider that the cellular telephone provider possesses agreements with, and each time a new contract is signed with such an entity, the client in question will be notified by the mobile telephone service provider of the use that this new entity will make of their personal information. Such a solution would address the privacy concerns of individuals while not running the risk that they will refuse to provide their consent for such use of their data.

---

[382] E. GRATTON, "M-commerce: The Notion of Consumer Consent in Receiving Location-Based Advertising", *Id*; E. GRATTON, *Wireless Privacy and Personalized Location-based Services: The Challenge of Translating the Legal Framework into Business Practices*, *Id.*

[383] E. B. CLEFF, prev. cited, note 369, 266; E. GRATTON , *Wireless Privacy and Personalized Location-based Services: The Challenge of Translating the Legal Framework into Business Practices*, *Id.*, p. 58.

[384] *Supra*, p. 78.

In addition to knowing who is required to provide disclosure, it is also important to determine the form that this disclosure must take. The form of the disclosure entails two elements – the content of the disclosure and the manner in which it is presented. In order to grant adequate disclosure, the information provided must be both detailed and comprehensible to Internet users. This feat may be achieved by noting each form of data collected by the entity – whether it is name, birthday, email address, browsing habits, search queries performed, city of inhabitation and so on – and then describing the various precise manners in which this information is to be used in very simple terms.

There has been a new initiative in this respect, meant to ensure the utmost disclosure and transparency, which consists of placing a small icon in the form of the letter "*i*"[385] on each advertisement that was targeted to an individual online, upon which this person can click to inform himself about the targeted advertising practices of the entity who targeted that advertisement to him. While this does provide a certain level of disclosure, the user only receives it after the information has already been collected, thus not entirely satisfying the requirement of identifying the purposes prior to or at the moment of collection. Despite this, it has been recognized by the Office of the Privacy Commissioner as providing a level of transparency that follows the spirit of the disclosure requirement[386].

Thus, while this form of disclosure may be a step in the right direction it cannot be considered to be sufficient as it does not adequately fulfill the obligation required by law, and as such other solutions must be determined. With regards to the use of cookies, the only form of disclosure that would follow the precise letter of the law would require that each time a cookie is placed on an individual's computer by an entity, that entity inform the user of the purposes for which this cookie is being placed on his computer, the types of

---

[385] *See:* GOOGLE, "What are AdChoices?", 2012, online: <http://support.google.com/adsense/bin/static.py?hl=en&gl=CA&client=ca-pub-9310224305865624&ts=1631343&page=ts.cs&adU=www.crea-med.ca&rd=3&contact=abg_afc&url=http:%2F%2Fwww.listchallenges.com%2F100places%2FCompare%2F&adT=Private+Doctors> (site consulted on March 17, 2012).

[386] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, prev. cited, note 39, p. 26.

information it will aggregate and the manner in which that data will be utilized. This may not, however, be entirely practical and may in fact serve to annoy Internet users rather than make them grateful for the disclosure of privacy practices, as their use of the Internet will most probably constantly be interrupted by such pop ups.

While it is true that users can alter the security settings of their Internet browser to refuse to accept that cookies be placed on their browser, it must be pointed that not all users are aware of how to properly alter the security settings to achieve this[387]. Additionally, we cannot neglect to mention that some web pages may not function unless cookies are accepted[388]. In such cases, rather than the actual website appearing, a notification requiring that the user alter his cookie acceptance settings will show up so that he may ultimately be able to view the site in question. Thus, in the same manner as pop-ups informing users about the purposes for which their data is being collected through cookies may annoy them, their ability to limit the placement of cookies on their browser at the detriment of not being able to view websites would not be any more appealing. As a result, and despite the fact that the "*i*" button does not completely satisfy the disclosure requirement, we do believe that such an initiative is probably the most practical and user friendly manner in which to adequately disclose targeted advertising practices to users.

Furthermore, this may also be the only economically viable solution. Disclosing the purposes for the collection and use of an individual's personal information in such a manner that will negatively affect his experience of using the Internet will simply limit the use that individuals make of the Web, and ultimately the amount of behavioural information that will be available to marketers from this respect. The use of the "*i*" button as a form of disclosure, on the other hand, presents very interesting possibilities from an economic perspective. While it is true that there is a possibility that a person's data will be

---

[387] R. K. ZIMMERMAN, prev. cited, note 29, 445.
[388] APPLE, "iOS: Safari web settings", October 12, 2011, online: <http://support.apple.com/kb/HT1677> (site consulted on September 2, 2012); WINDOWS, "Cookies: frequently asked questions", 2012, online: <http://windows.microsoft.com/en-SG/windows-vista/Cookies-frequently-asked-questions> (site consulted on September 2, 2012).

collected prior to the point in time where he may decide to click on the "*i*" button to inquire about the manner in which his personal data is used, which may cause him to feel a certain lack of control, the "*i*" button presents a level of transparency that may assuage his fears, as it is out in the open and easily accessible thus demonstrating that marketers have nothing to hide, and allow him to properly assess the risks involved with his use of such websites.

Disclosure of the use of DPI practices, on the other hand, must come directly from ISPs. The best manner in which to ensure adequate disclosure in this respect is to include information regarding these practices in the service agreement and to ensure that all the information related to the use of this practice is explicitly articulated prior to the moment the contract is signed by the user.

When it comes to targeted advertising on mobile telephones, however, determining the form that such disclosure should take is even more complicated due to the fact that the screen of a cellular telephone is exponentially smaller than that of a desktop or laptop computer, and also presents certain limitations on the full functioning of websites[389]. Due to this, it would be both difficult and impractical for users to view lengthy privacy policies on such an undersized screen[390]. The form such disclosure should take therefore still presents us with certain issues that remain unresolved at present[391].

It has been suggested that meaningful disclosure with regards to mobile advertising could be established by adding a voice based disclosure, either by sending the consumer a text message containing a toll free number that they can call and which will activate a recording serving to properly inform the user, or by sending a hyperlink along with the text message upon which the individual can click to hear the audio message[392]. The problem with this solution, is that ever since the adoption of the new Canadian Anti-Spam

---

[389] E. B. CLEFF, prev. cited, note 369, 266; E. GRATTON , prev. cited, note 381, p. 60; E. GRATTON, prev. cited, note 369, 63.
[390] E. B. CLEFF, *Id.*; E. GRATTON , prev. cited, note 381, *Id.*; E. GRATTON, prev. cited, note 369, *Id*.
[391] E. GRATTON, prev. cited, note 369, *Id.*
[392] E. B. CLEFF, prev. cited, note 369, 267.

legislation[393] the sending of any electronic message (which is a message sent by means of telecommunication[394], including text, sound, voice or image messages) to an electronic address (which is any address used in connection with the transmission of an electronic message to any email, instant message or telephone account) is prohibited unless the person in question has consented to receiving it[395].

As such, the only solution that would both respect the laws in force while also allowing marketers to use the location data of individuals emanating from their mobile telephones is through disclosing the tracking practices used by each location-based advertiser the cellular telephone provider has agreements with, in the same manner as suggested above[396]. This would provide a level of transparency that would render individuals more inclined to consent to the use of their location information for advertising purposes, while at the same time allotting them with sufficient control over their personal data that will allow them to feel secure, thus furthering the goals of online marketers.

In order to ensure proper disclosure, several factors must therefore be taken into account, and these considerations are crucial to ensuring the complete enlightenment of the user with regards to the targeted advertising practices being used. Disclosure is doubly important when one considers that, without the user being informed about the reasons for the collection of his personal information in sufficient detail, the consent that he may ultimately provide would be moot. Thus, after having examined the element of disclosure in sufficient detail, we will now proceed to discuss the requirement of consent.

---

[393] *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act*, prev. cited, note 16.
[394] *Id.*, section 1.
[395] *Id.*, section 6(1).
[396] *Supra*, p. 79-80.

Paragraph 2 Consent

Both the PIPEDA and the ARPPIPS require that the consent of an individual must be acquired in order for his personal information to be validly used. Consent is essentially the response received from a given person once they have analyzed the risks involved with the provision of their personal data based on the information disclosed to them and have deemed that they are minimal[397]. This additional step of seeking an individual's consent to use his personal information is, however, crucial for several reasons. To begin with, acquiring their consent instills individuals with confidence in online marketers, which "is a necessary condition for their loyalty. This is truer than ever on the Web, where business is conducted at a distance and uncertainties are bigger because of impersonality in business relations"[398]. Loyalty directly translates into higher customer retention rates and makes it more likely for an individual to be forthcoming with his personal information[399] by nurturing society's inter-communication and ultimately ensuring that it is not impeded as a result of feelings of lack of safety arising from what individuals may view as invasions of privacy. This in turn heightens the ability for marketers to target these individuals with relevant ads, ultimately resulting in a higher turnover rate[400].

While acquiring consent increases profit margins, neglecting to do so could cause irreparable harm to a company's reputation that it may not be able to bounce back from, as is evidenced by the cases of Phorm and NebuAd[401], who used DPI technology to amass consumer information without acquiring prior consent causing them to lose their investors and partners and ultimately shut down. In other cases, failure to acquire consent may not

---

[397] *See:* K.-L. HUI, H. H. TEO and S.-Y. T. LEE, prev. cited, note 370.
[398] Dirk FROSCH-WILKE, "Are E-Privacy and E-Commerce a Contradiction in Terms? – An Economic Examination", (2001), p. 194, online: <http://www.informingscience.org/proceedings/IS2001Proceedings/pdf/FroschWilkeEBKAreEP.pdf> (site consulted on October 29, 2012); *See also:* Frederick F. REICHHELD and Phil SCHEFTER, "E-Loyalty: Your Secret Weapon on the Web", (2000), online: <http://www.pearsoned.ca/highered/divisions/text/cyr/readings/Reichheld_SchefterT2P1R1.pdf> (site consulted on October 29, 2012); *See also:* C. CHASSIGNEUX, prev. cited, note 47, p. 61-78.
[399] F. F. REICHHELD and P. SCHEFTER, *Id.*, p. 107.
[400] D. FROSCH-WILKE, prev. cited, note 398, p. 194-195.

be as detrimental, but will still have dire effects revolving around loss of customers and difficulty in gaining new ones, which, due to its rapid growth, holds more significance in online markets than traditional ones[402]. In these situations, companies will be required to invest more money into the acquisition of new customers, thus reducing their turnover rate. Furthermore, a loss of reputation could diminish the company's value in the stock market, as is demonstrated in the example of DoubleClick[403], where the enterprise used cookies to aggregate the personal data of individuals without their prior consent, who experienced a 15.27% drop in share value following the Federal Trade Commission's inquiry into their practices in February 2000[404].

On the other hand, there are those individuals that claim that the obligation to acquire an individual's consent prior to collecting and using his personal data creates an unnecessary strain on the free flow of information which in turn harms commerce as "better information leads to better markets"[405]. This position is often supported by the example of junk mail, which holds that if more data was known about an individual, the mail that would be sent to them would be tailored to their preferences and would in turn not be considered as "junk". Those who hold this position claim that it is privacy protection that inhibits this occurrence[406]. It is not, however, the protection itself that is the issue, but rather the general perception by the business sector of this protection, which

> "presumes that privacy necessarily entails information blockage. But this is not so. If individuals will truly benefit by releasing their personal data, e.g., by getting less junk […], they will rationally choose to do so. Information privacy does not mandate information quarantine; it merely requires that the individual exercise control within reasonable constraints over whether, and what type of, quarantine should exist. Accordingly, these arguments do not demonstrate that the individual should be deprived of information privacy.

---

[401] *See: Supra*, p. 21-23.
[402] *See:* Michael ROSEMANN, Michele ROCHEFORT, and Wolfgang BEHNCK, "Customer Relationship Management" (our translation), (1999) 36-208 *HMD-Praxis der Wirtschaftsinformatik* 105.
[403] *See: Supra*, p. 14-15.
[404] D. FROSCH-WILKE, prev. cited, note 398, p. 194.
[405] J. KANG, prev. cited, note 321, 1217.
[406] *Id.*, 1218.

> At most, they suggest that individuals should be open to information processing in exchange for commercial benefit and that society should make such exchanges feasible."[407]

By acquiring individual consent for the collection and use of personal data, businesses would be informing users of the benefits they will enjoy, while at the same time maintaining a level of transparency that will instill trust and thus make people more willing to share their personal information. It is therefore in this manner that the law "[makes] such exchanges feasible"[408]. In this light, the legal requirement that consent be acquired from individuals prior to the collection and use of their personal data is tremendously economically beneficial to marketers.

According to the PIPEDA, the consent of the individual whose private information is being collected must be acquired[409], the validity of which will be based upon the proper identification of the purposes for collection in such a manner that the person can reasonably understand how the data will be used[410], as discussed above. Furthermore, these people must have the choice of withdrawing their consent at any time subject to contractual or statutory limitations[411]. While consent does not necessarily need to be acquired at the moment of collection, it must at least be secured prior to the use of that data[412].

The ARPPIPS, on the other hand, obliges entities to obtain the consent of the individual whose information is being collected, used or communicated – meaning that consent must have already been acquired for any collection of data to be able to take place. Additionally, in order for this consent to be valid, it "must be manifest, free, and

---

[407] *Id.*; *See also:* Mary J. CULNAN, *Self-Regulation on the Electronic Frontier: Implications for Public Policy*, *in* National Telecomms. & Info. Admin., U.S. Dep't of Commerce, Privacy and Self-Regulation in the Information Age, ch. 1, § F (1997), online: < http://www.ntia.doc.gov/page/chapter-1-theory-markets-and-privacy#1F> (site consulted on October 31, 2012).
[408] J. KANG, *Id.*
[409] *Personal Information Protection and Electronic Documents Act*, prev. cited, note 16, Schedule 1, section 4.3.
[410] *Id.*, Schedule 1, section 4.3.2.
[411] *Id.*, Schedule 1, section 4.3.8.
[412] *Id.*, Schedule 1, section 4.3.1.

enlightened, and must be given for specific purposes"[413]. Nevertheless, an individual's consent may be implied when he provides certain personal information voluntarily[414]. Furthermore, the ARPPIPS describes certain exceptions to the consent provision in its sections 13 and 18 to 26, which permit an enterprise to disclose the personal information contained in a file on a person to a third-party, without the specific consent of the person, if it is for a reason which the person concerned has already consented to or for an object covered by the exceptions listed under those sections.

Consent can present itself in one of two different forms, namely opt-in and opt-out. Opt-in is the form of consent that allows users the most control over their information as they must consciously and explicitly provide their permission so that their personal data may be used. Opt-out consent, on the other hand, occurs in situations where an individual's personal information is automatically collected, effectively requiring him to specifically express his lack of consent to this compilation for it to cease.

In order for an enterprise to fulfill its obligation under the ARPPIPS, however, the only viable form of consent would be opt-in, as this law specifically requires that consent must be "manifest"[415]. The PIPEDA, on the other hand, states that the form of consent utilized must depend on the sensitivity of the information being collected, such as data regarding medical history or income. While opt-in consent is considered to be the form of consent that is most in harmony with the PIPEDA[416], according to the Office of the Privacy Commissioner, opt-out consent could be sufficient for an organization to fulfill its obligations under this Federal law[417]. Essentially, since behavioural information may not

---

[413] *Act respecting the Protection of Personal Information in the Private Sector*, prev. cited, note 15, section 14; In order for consent to be free and enlightened, it cannot be vitiated by error, fear or lesion (*See:* articles 1399-1406 C.C.Q. (*Civil Code of Quebec*, prev. cited, note 15)).
[414] *Lehman* v. *Heenan Blaikie*, [2005] CAI 433.
[415] *Act respecting the Protection of Personal Information in the Private Sector*, prev. cited, note 15, section 14.
[416] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA , prev. cited, note 39, p. 25.
[417] *Id.*

necessarily be considered as highly sensitive data[418], opt-out consent may be a legal option in such cases, even despite the preference for opt-in consent[419].

According to the Office of the Privacy Commissioner, certain conditions must be satisfied when opt-out consent is utilized, and these conditions will differ depending on whether the marketing purposes for which the personal information of an individual is obtained is secondary or primary. The use of opt-out consent for secondary marketing purposes, meaning that the information collected was aggregated for an initial reason but the use of that data for marketing is merely secondary, was examined by the Office of the Privacy Commissioner[420]. It was considered that certain requirements must be satisfied in order for opt-out consent to be legal in these situations, namely that the information in question cannot be considered to be sensitive in either its nature or context, the data being shared for secondary marketing purposes must be limited and the nature of the personal information used or disclosed as well as the extent of the intended use or disclosure must be clearly delineated, and finally the purposes for which this data is shared must be both limited and well-defined and described in clear and easily comprehensible language[421].

At the same time, however, it was considered by the Office of the Privacy Commissioner, in its report regarding Facebook's privacy practices, that due to the fact that Facebook offers its website freely to individuals, advertising is essential to its ability to provide these services, as without the revenue generated in such a fashion, it would be impossible to upkeep the site. As such, the Office of the Privacy Commissioner considered Facebook's targeted advertising practices to be a primary purpose and views it to be

---

[418] *See, Supra*, p. 68-73.
[419] *Id.*
[420] *Finding #243*, 2003 CanLII 38403 (P.C.C.); *Finding #244*, 2003 CanLII 38237 (P.C.C.).
[421] *Finding #77*, 2002, online: http://www.priv.gc.ca/cf-dc/2002/cf-dc_021016_7_e.cfm> (site consulted on March 17, 2012); *Finding #78*, 2002, online: <http://www.priv.gc.ca/cf-dc/2002/cf-dc_021016_6_e.cfm> (site consulted on March 17, 2012); *Finding #80*, 2002, online: <http://www.priv.gc.ca/cf-dc/2002/cf-dc_021016_4_e.cfm> (site consulted on March 17, 2012); *Finding #81*, 2002, online: <http://www.priv.gc.ca/cf-dc/2002/cf-dc_021016_3_e.cfm> (site consulted on March 17, 2012); *Finding #82*, 2002 CanLII 42385; *Finding #83*, 2002 CanLII 42324; *Finding #243*, *Id.*; *Finding #244*, *Id.*; *Finding #263*, 2004 CanLII 22905 (P.C.C.); *Finding #308*, 2005 CanLII 27670 (P.C.C.).

"reasonable that users are required to consent to Facebook Ads as a condition of service"[422]. By considering Facebook's targeted advertising practices in such a manner, the Office of the Privacy Commissioner is basically classifying primary marketing purposes as a legitimate purpose in light of the PIPEDA, thus preventing Facebook from being confronted with the violation set out in the PIPEDA[423], as well as the ARPPIPS[424], which prohibit organizations from refusing to supply an individual with a product or service simply because they have declined to consent to the collection, use or disclosure of their personal information, unless that data is essential to the transaction and is necessary to fulfill a legitimate purpose. The form of consent required, and ultimately whether or not a particular marketing purpose will be considered as primary or secondary, is therefore not entirely clear.

Despite this, we believe that the only viable solution rests in the form of opt-in consent. As previously mentioned[425], consumer trust is a necessary element in online marketing that will further promote the goals meant to be achieved. However, forcing these individuals to constantly seek the manner in which they may effectively demonstrate their lack of consent through opt-out procedures would place an onerous burden upon them that would not incite the confidence sought. It is rather opt-in consent that would accomplish this feat. Additionally, a company's institution of opt-in consent could serve to set it apart from its competitors and provide it with an advantageous edge that would better satisfy customers wants and needs and therefore attract both their attention and business[426]. While it is true that greater funds would need to be invested to employ an opt-in system of consent, this amount would be far less than what a company would lose should their method of acquiring consent inspire a lack of confidence in Internet users.

---

[422] *Finding #8*, July 16, 2009, par. 134, online: <http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm> (site consulted on March 25, 2012).
[423] *Personal Information Protection and Electronic Documents Act*, prev. cited, note 16, Schedule 1, section 4.3.3.
[424] *An Act Respecting the Protection of Personal Information in the Private Sector*, prev. cited, note 15, section 9.
[425] *Supra*, p. 85-86.
[426] D. FROSCH-WILKE, prev. cited, note 398, p. 194.

However, while opt-out consent may not be as viable a solution, it still remains a possibility in light of the PIPEDA and as such, consent must be achieved in one form or another when personal information is collected and used. This requirement is not, however, always respected in the practice of targeted marketing and therefore requires particular examination when it comes to acquiring consent in light of the use of (a) cookies, (b) DPI and (c) mobile tracking tools for targeted marketing purposes.

a. Cookies

To begin with, when cookies are used to collect information about individuals, their consent is never sought at the moment of collection[427]. The only form of consent acquired through the use of these tools, minimal as it may be, is opt-out, whereby a user can choose to delete the cookies stored on his browser – something which can only be considered as a form of consent in cases where the individual in question is actually knowledgeable about the practice whereby cookies are used to gather his personal data. However, in cases where Flash cookies are used to regenerate Web cookies, even when a person deletes the cookies from his browser thereby refusing to consent to the gathering of his personal data, such recreation circumvents the individual's refusal to provide his consent.

While it is true that a browser can be configured to warn individuals when a website is attempting to share a cookie with them, thus allowing users to reject such cookies should they so wish, the default settings of browsers are generally set to accept all cookies and users are not often made aware of the rejection mechanism in question[428]. Furthermore, it often occurs that sites require individuals to permit cookies to be stored on their browser so that they may be able to access the site in question, which violates the above discussed requirement of both the PIPEDA[429] and the ARPPIPS[430] that obliges organizations to have

---

[427] R. K. ZIMMERMAN, prev. cited, note 29, 443.
[428] *Id.*, 445.
[429] *Personal Information Protection and Electronic Documents Act*, prev. cited, note 16, Schedule 1, section 4.3.3.

a legitimate purpose in the event that they refuse to provide their services should a user decline to consent to any collection or use of his personal information. As mentioned above, the legitimacy of the purposes for which cookies aggregate data depends on whether the information is being collected for primary or secondary marketing purposes[431], as unless it is used for the former it cannot be considered as necessary for the fulfillment of a legitimate[432] purpose[433]. As such, when cookies are used to collect data for secondary marketing purposes, even if a user would be made aware of the browser setting allowing them to be notified about cookies and reject them, their inability to view the site should they refuse these cookies ultimately robs them of their choice.

The new Canadian Anti-Spam legislation[434], however, sheds a new light on the consent requirement regarding the use of cookies on one's computer, by stating that a person is considered to expressly consent to the installation of cookies on his computer if his conduct is such that it is reasonable to believe that he consents to the program's installation[435]. As such, acquiring the consent of individuals for the gathering of information through cookies may not be necessary for the purposes of Federal law. Regardless of this, however, their consent must still be procured prior to that information being used for any purposes whatsoever, in accordance with the PIPEDA.

Imputing the consent of individuals when it comes to the placement of cookies on their electronic devices is neither here nor there from an economic perspective. The manners in which the consent of individuals may be sought in this situation would all serve

---

[430] *An Act Respecting the Protection of Personal Information in the Private Sector*, prev. cited, note 15, section 9.
[431] *Finding #8*, prev. cited, note 422, par. 134.
[432] *Personal Information Protection and Electronic Documents Act*, prev. cited, note 16, Schedule 1, section 4.3.3; *An Act Respecting the Protection of Personal Information in the Private Sector*, prev. cited, note 15, art. 4.
[433] *Finding #162*, prev. cited, note 341.
[434] *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act*, prev. cited, note 16, section 10(8).

to hinder their use of the Internet by constantly harassing them with pop-ups demanding if they accept cookies or by simply preventing them from being able to access websites should they choose to limit the presence of cookies on their devices. These forms of seeking consent may therefore have the effect of limiting the use that people would make of the Internet as it would no longer be a simple and pleasant experience. At the same time, simply imputing their consent under such circumstances would have the result of inciting distrust in consumers, as previously discussed[436], which could lead to individuals being less forthcoming with their personal data. Such an outcome is illustrated by a recent survey conducted by TRUSTe, which signals that 90% of individuals employ browser controls to protect their privacy, which includes the deletion of cookies[437]. Such a limitation on the behavioural information available could thus be detrimental to the goals of marketers.

Nevertheless, there may be a middle ground between these two solutions. Essentially, when accessing a website, it is possible for the landing page to consist of a notification to users regarding that site's use of cookies and a demand of their acceptance. Once the user has made his choice, and whether or not he chooses to consent to the placement of a cookie on his computer, he will then be led to the home page of the site[438]. This solution would prevent the Internet from becoming a source of annoyance for individuals, thus ensuring that they do not cease using the Web, while at the same time instilling a certain level of trust that might cause them to be more open with their personal data. Furthermore, such an approach would also shield businesses from being subjected to negative publicity as a result of not acquiring consent, as they would be providing users with additional means of controlling their personal information.

---

[435] *Id.*
[436] *Supra*, p. 85-86.
[437] GIGAOM, "Survey: Percentage of users saying they opt out of targeted ads has nearly doubled", July 16, 2012, online: <http://gigaom.com/2012/07/16/percentage-of-users-saying-they-opt-out-of-targeted-ads-has-nearly-doubled-survey/> (site consulted on November 1, 2012).
[438] See, for example, the implementation of this solution on the Fasken Martineau website: FASKEN MARTINEAU, online: <http://www.fasken.com/> (site consulted on November 1, 2012).

b. Deep Packet Inspection

When the practice of DPI is used to collect personal information, on the other hand, the individuals affected by this practice generally remain uninformed and their consent is nearly never sought. A large number of ISPs "bury notices of their inspection practices in densely worded privacy policies [thus making it so that] consumers cannot reasonably be expected to know about, and protect themselves from, opaque practices"[439]. Furthermore, the only form of consent sought by such ISPs is in the form of an opt-out policy accessible online, but regarding which users are not clearly informed[440]. While this is not so for all ISPs, as some have pledged to the U.S. Senate Commerce Committee that they would only use DPI technology on their clients for targeted marketing purposes with their *explicit* consent[441], it is still a rather common practice of a good number of ISPs that ultimately serves to violate the privacy rights of their clients.

In the case of DPI, however, the lack of the acquisition of consent is not only a violation of both the PIPEDA and the ARPPIPS, but it is also a criminal act according to the Canadian *Criminal Code*[442]. In virtue of section 184(1) C.C., the willful interception, including listening to, recording or acquiring a communication or the substance, meaning or purport thereof[443], of a private communication, which consists of "any telecommunication […] that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it"[444], without the consent of the originator in question[445], is an indictable offence

---

[439] Nate ANDERSON, ".06% Opt Out: NebuAd hides link in 5,000-word Privacy Policy", July 24, 2008, online: <http://arstechnica.com/old/content/2008/07/06-opt-out-nebuad-hides-link-in-5000-word-privacy-policy.ars> (site consulted on February 20, 2012); OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "The Privacy Implications of Deep Packet Inspection", online: <http://dpi.priv.gc.ca/index.php/essays/the-privacy-implications-of-deep-packet-inspection/> (site consulted on February 20, 2012).
[440] N. ANDERSON, *Id.*; OFFICE OF THE PRIVACY COMMISSIONER, *Id.*
[441] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "The Greatest Threat to Privacy", online: <http://dpi.priv.gc.ca/index.php/essays/the-greatest-threat-to-privacy/> (site consulted on February 20, 2012).
[442] *Criminal Code*, prev. cited, note 16 (hereafter referred to as "C.C.").
[443] *Id.*, section 183.
[444] *Id.*
[445] *Id.*, section 183.1; *See: R.* v. *Goldman*, [1980] 1 S.C.R.. 976.

subject to an imprisonment for a term not exceeding five years[446]. This section does not, however, apply to individuals providing communications services to the public who intercept private communications in cases where interception is necessary to provide the service, or in cases where the service provider executes random checks to perform necessary monitoring for the purposes of mechanical or service quality control checks, or if the interception is necessary to ensure the protection of a person's rights or property directly related to providing the service[447].

Despite these exemptions, we do not believe that they could serve to protect ISPs exercising the practice of DPI. While it is true that DPI was originally created to protect individuals from various threats on the Internet that could harm their computers, and could thus be said to be used as a tool to protect their right to property, the ISPs who use this technology to reassemble email messages as they are being typed out by users or to gather data about their personal preferences, cannot be said to accomplish the aforementioned purpose. Furthermore, the collection of this type of information is not necessary for the provision of the service, especially since the Internet was constructed as an end-to-end service – meaning that any communications sent over the Internet are not meant to be intercepted until they reach their final destination. As such, unless the interception of email messages occurs due to the ISP's maintenance of services, it is an indictable offence.

The same position was taken in the case of *R.* v. *Weir*[448], where it was held that emails are deemed to be private communications for the purposes of section 184 C.C. and that any interception of such messages violates the reasonable expectance of privacy of the author of that message as well as his recipient. Furthermore, it was considered that ISPs are

---

[446] *Criminal Code*, *Id.*, section 184(1); *See:* François BLANCHETTE, *L'expectative raisonnable de vie privée et les principaux contextes de communications dans Internet*, Master's thesis, Montreal, Faculté des études supérieures, University of Montreal, 2001, p. 39-43.
[447] *Criminal Code*, *Id.*, section 184(2)(c).
[448] (1998) 59 Alta. L.R. (3d) 319 (B.R.), confirmed by (2001), 156 C.C.C. (3d) 188 (C.A.).

not permitted to access the contents of the email inbox of a client unless the consent of that person is obtained or if it is required by an officer who detains a warrant to this effect[449].

Considering the use of DPI as being a criminal offence is, we believe, an extremely economically viable solution. If the use of cookies to gather private data without individual consent could incite distrust, DPI technology would exponentially increase this lack of confidence, causing people to be less forthcoming with their personal information. Furthermore, because DPI renders ISPs privy to all the data viewed, received and emitted by a given user, and in view of the fact that the Internet has become one of the primary sources of communication between individuals, sometimes even holding voice conversation between them, the use of this technology may even cause individuals to cease using the Internet for inter-personal communications as they may feel as if their privacy is being invaded. While we might turn to the example of Facebook to counter this statement and demonstrate the number of individuals still using that SNW despite the privacy risks it may present, a recent survey conducted by the Princeton Survey Research Associates International demonstrated that 58% of individuals that use SNWs restrict access to their profiles[450]. The possibility that individuals will utilize the Internet differently is thus a risk that does exist. It is, however, upon the online interactions of individuals that Internet marketers depend for the success of their campaigns, and jeopardizing their ability to access such data would be detrimental to the achievement of their goals. Prohibiting the practice of DPI in an outright fashion is therefore crucial to ensuring the protection of the economic objectives that marketers seek to attain through the use of this practice, and it may therefore be most beneficial to them not to use it at all.

---

[449] *Id.*
[450] Mary MADDEN, "Privacy management on social media sites", February 24, 2012, online: <http://www.pewinternet.org/Reports/2012/Privacy-management-on-social-media/Summary-of-findings.aspx> (site consulted on November 8, 2012).

c. Mobile Tracking Tools

Mobile tracking tools also present their own issues with regards to the consent provisions of both the PIPEDA and the ARPPIPS. While it is true that Canadian mobile advertisers utilize opt-in consent prior to targeting individuals using location-based services[451], the various positioning systems used to track these individuals serve to track all those who possess a cellular telephone[452]. The only difference is that in the latter case, the location data aggregated is not used to target these individuals with location-based ads. While this does not change anything with regards to the obligation to acquire the consent of individuals in light of the ARPPIPS, which demands that an individual manifestly consent to the collection of his data[453], such instances may be exempt from the principle of consent with respect to the PIPEDA. While the PIPEDA states that consent should typically be acquired at the time of collection, it is possible for consent to be sought after the collection but prior to the use of the personal information[454]. Thus, in the event that the location data collected through the signals emitted by mobile phones is not utilized for advertising purposes, consent may not be necessary.

In cases where the information in question is used, however, the procurement of consent is necessary but may not be so easily obtained in the practice of mobile targeted marketing. As mentioned above[455], the new Canadian Anti-Spam legislation[456] requires that consent be acquired prior to any message being sent to an individual. At the same time, this law also considers any message sent requesting the consent of an individual to

---

[451] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, prev. cited, note 39, p. 25.
[452] *See:* A. CORPEL and M. LEMERCIER, prev. cited, note 141; Teresa SCASSA, "Information Privacy in Public Space: Location Data, Data Protection and the Reasonable Expectation of Privacy", (2009) 7-2 *C.J.L.T.*, 193, 194.
[453] *Act Respecting the Protection of Personal Information in the Private Sector*, prev. cited, note 15, section 14.
[454] *Personal Information Protection and Electronic Documents Act*, prev. cited, note 16, Schedule 1, section 4.3.1.
[455] *Supra*, p. 83-84.
[456] *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the*

send further messages to be an electronic message[457]. This means that the consent of the individual must be achieved in some other manner prior to sending him any messages whatsoever on his cellular telephone.

Furthermore, while this law considers that both explicit and implicit consent are acceptable[458], consent can only be implicit in very specific situations, namely when a business relationship already exists between the individual and the entity sending him a message, and if the individual has published his email address or disclosed his business card. In order to ensure express consent, on the other hand, the purposes for which consent is sought must be set out clearly and simply. As such, the proposition that disclosure, and thus consent, of the individual be performed by the carrier at the moment the service contract is signed may therefore be efficient, not only to provide disclosure but also to ensure that the consent to both the collection and use of the individual's personal information, and thus tracking data, be used to target him with advertisements[459] as sending him a message on his cellular telephone for the purpose of obtaining such consent is no longer permissible in light of Canada's new Anti-Spam legislation. In such cases, however, he must have the option of refusing to consent, as the wireless services being offered cannot depend on his acceptance of such a clause[460].

We believe that protecting individuals against receiving undesired messages on their mobile phones is a very economically sound position. If individuals were to receive messages from marketers with whom they have no relation, they are bound to feel a certain invasion of privacy and may even consider the receipt of such messages a nuisance. In this light, should individuals find mobile advertisements invasive, they may simply refuse to

---

Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act, prev. cited, note 16.
[457] *Id.*, section 1.
[458] *Id.*, section 6(1).
[459] E. B. CLEFF, prev. cited, note 369, 268.
[460] *Personal Information Protection and Electronic Documents Act*, prev. cited, note 16, Schedule 1, section 4.3.3 *Act Respecting the Protection of Personal Information in the private Sector*, prev. cited, note 15, section 9.

provide their consent to the sending of such messages so that they may live freely without such privacy invasions or may even limit the use they make of their cellular telephones to ensure that such data is unavailable to marketers.

This potential outcome has been illustrated by a recent survey conducted by the Pew Research Center, which demonstrated that 30% of individuals who downloaded apps on their cellular phones have uninstalled certain apps due to the fact that it had come to their attention that they were collecting information that the individuals did not wish to share[461] and 19% of cell holders have disabled the location tracking feature for fear that this data would be accessed by third parties. This sort of reaction on the part of individuals thus renders their personal information unavailable to marketers – an outcome which would be tremendously undesirable for them. Limiting the situations in which individuals can be contacted by businesses on their mobile telephones, in a manner that ensure that consent is properly acquired without invading an individual's privacy, is thus the only manner in which to ensure that this end result is avoided. While it may not be helpful to marketers immersed in the domain of mobile advertising, as it severely limits their ability to practice this form of marketing, this limit is far less than what they would suffer if consent was denied due to the invasiveness of their practices.

* * *

To conclude, it is clear that acquiring consent for the practice of targeted marketing presents many issues, regardless of which tracking tool is used to achieve this purpose. Several solutions have, however, been suggested with regards to the issue of consent, none of which have been implemented as of yet. The first solution to be proposed is that of a "Do Not Track List", which is similar to a "Do Not Call List" but applies to the use of technological tracking tools to aggregate information[462]. It has been considered, however,

---

[461] PEW INTERNET & AMERICAN LIFE PROJECT, "Privacy and Data Management on Mobile Devices", September 5, 2012, online: <http://www.pewinternet.org/Press-Releases/2012/Mobile-Privacy.aspx> (site consulted on November 1, 2012).
[462] *See*: J. LO, prev. cited, note 11.

that such a solution would result in more privacy issues than it would be able to mend, as it would function by creating a national database of consumers that have opted-out[463] which would allow the government to collect a significant amount of personally identifiable information to which they would not have otherwise had access and which they might misuse[464]. Furthermore, the fact that consumers would be required to opt-out rather than opt-in may also impose certain issues, aside from the fact that such a registry would be extremely costly to create and implement[465].

Another solution that has been proposed, and one that seems to be more viable than a "Do Not Track List", however, is one that would necessitate the creation of an opt-in program for targeted advertising[466] – a solution similar to the one which the European Commission intends to implement[467]. This solution would fundamentally attempt to protect consumers from the practice of targeted marketing by requiring marketers to develop a program, overseen by a government entity that would have the authority to impose significant fines should the enterprise not conform to its obligations, which would require consumers to choose to participate in targeted advertising strategies from a particular enterprise[468]. This program would also provide consumers with the choice of which information they would like to share, but prohibit them from volunteering any sensitive information, while requiring enterprises to provide these individuals with sufficient notice prior to beginning the collection of the information in question[469]. Finally, it is suggested that the data should only be used for the specific purposes for which it was

---

[463] H. OSBORN NG, prev. cited, note 24, 386.
[464] *Id.*, 386-387.
[465] J. LO, prev. cited, note 11, p. 73; *Id.*, 387.
[466] *See*: H. OSBORN NG, prev. cited, note 24.
[467] Jason LEWIS, "Facebook personal tracking hits snag", November 28, 2011, online: <http://www.smh.com.au/technology/security/facebook-personal-tracking-hits-snag-20111127-1o1k6.html> (February 21, 2012).
[468] H. OSBORN NG, prev. cited, note 24, 392.
[469] *Id.*

collected while limiting the period of time that enterprises may retain the information so as to prevent them from being in the position of creating very detailed consumer profiles[470].

For the reasons exposed above[471], we believe that this opt-in program would be the most beneficial as it would incite the trust of individuals by allowing them to exercise control over their personal data. However, regardless of whether or not such solutions are implemented, organizations are required to take steps to ensure that individual consent is acquired. While it is true that the issue of consent in targeted marketing is not clear cut, it is crucial to take all the elements regarding each type of tracking tool into account to determine which form of consent would be most appropriate, as well as economically viable, under the circumstances.

* * *

The above examination of the various privacy laws effectively outlines the provisions that present the greatest issues in the domain of targeted marketing, and the manner in which these issues can be best remedied. The protection of personal information, however, is merely one aspect of the right to privacy afforded to Canadian citizens. This right also serves to protect these individuals against any form of intrusion that would put the private nature of their lives at risk. The next section will therefore be dedicated to this second facet of privacy protection.

Section 2 The Protection Against Intrusion on Privacy and Personal Property and Its Application to the Practice of Targeted Marketing

In addition to protecting the personal information of individuals, as exposed in the previous section[472], the general right to privacy afforded to Canadian and Quebec citizens

---

[470] *Id.*, 392-393.
[471] *Supra*, p. 90.
[472] *Supra*, p. 68-101.

alike also serves to protect them against "intrusions upon [their] seclusion or solitude"[473]. Such a protection is provided in Quebec law through the action in civil liability enshrined in section 1457 C.C.Q.[474] which requires evidence of a fault, which in this case would be the intrusion in question, damages and a causal link between the two in order to establish a claim. This section will be dedicated to (1) outlining the fault arising from the act of intruding upon an individual's seclusion through the use of technological tracking tools for targeted marketing purposes and (2) illustrating the damages that may arise directly as a result of this faulty behaviour.

Subsection 1 The Fault of Intruding on Privacy and Personal Property

According to section 1457 C.C.Q., a fault is considered to be another's failure to "abide by the rules of conduct [...] according to the circumstances, usage or law". When it comes to privacy, the law holds that, not only do individuals have the right to the protection of their personal data, and therefore to their anonymity, as discussed above[475], but they also have the right to be guarded against any unjustified intrusions into their solitude[476] – a liberty which is accompanied by his right to physical isolation[477]. From this perspective,

---

[473] Charles J. HARTMANN and Stephen M. RENAS, "Anglo-American Privacy Law: An Economic Analysis", (1985) 5 *International Review of Law and Economics* 133, 140; *See also:* Jean-Louis BAUDOUIN and Patrice DESLAURIERS, *La Responsabilité Civile*, 7th ed., vol. 1, Cowansville, Les Éditions Yvon Blais, 2007, p. 225.

[474] *Civil Code of Quebec*, prev. cited, note 15.

[475] *Supra*, p. 68-101.

[476] *Cooperberg* c. *Buckam*, [1958] C.S. 427; *McIlwaine* c. *Equity Accounts Buyers Ltd.*, [1974] R.L. 115 (C.P.); *Auger* c. *Equity Account Buyers Ltd.*, [1976] C.S. 279; *Beaudoin* c. *Beaudoin*, [1986] R.R.A. 68 (C.P.); *Tousignant* c. *Bernier*, J.E. 87-1211 (C.S.); *Pasquale* c. *Descôteaux*, [1990] R.R.A. 574 (C.S.); *Pelletier* c. *Emery*, J.E. 97-1360 (C.S.); *Latreille* c. *Choptain*, J.E. 97-1475 (C.S.); *Savard* c. *All Tour Marketing*, [1998] R.R.A. 649 (C.Q.); *Olteanu* c. *Zellers inc.*, B.E. 99BE-1205 (Q.C.); *Choueke* c. *Coopératived'habitation Jeanne-Mance*, [2001] R.J.Q. 1441 (C.A.), infirmed J.E. 95-880 (C.S.) (leave to appeal to the Supreme Court refused); *Huot* c. *Martineau*, [2005] J.L. 75 (C.S.); *Wilkie* c. *Lapensée*, J.E. 2005-938 (C.S.); *Gariépy* c. *Naud*, EYB 2006-100784 (C.S.) (appeal refused EYB 2007-116806); J.-L. BAUDOUIN and P. DESLAURIERS, prev. cited, note 473, p. 225; C. J. HARTMANN and S. M. RENAS, prev. cited, note 473, 140.

[477] Édith DELEURY and Dominique GOUBAU, *Le droit des personnes physiques*, 4th ed., Cowansville, Les Éditions Yvon Blais, 2008, par. 172.

> "the protection of an individual's privacy takes on a geographic dimension. It recognizes a particular territory at whose frontiers another's power ends and at the heart of which reigns a small sovereignty. Guaranteed by section 7 of the Charter of Human Rights and Freedoms, the inviolability of the domicile is, for the person whom it protects, the right to prevent another's access to their home; more specifically, it is the right for each person to turn his domicile into a place of sanctuary and retreat where he can, if he desires, live alone and be protected from intrusions and interventions.
>
> [...]
>
> It is upon this basis that tribunals have sanctioned harassment, by telephone, to which certain individuals were victims […]."[478]

The Courts therefore recognize that intrusions into an individual's domicile need not necessarily be physical, but can consist of technological intrusions as well, such as through pestering an individual in his domicile by making constant telephone calls[479]. Considering that a telephone call consists of the sending of electronic signals, we believe that a parallel may be made when technological tracking tools are utilized to trace individuals throughout the Internet as the use of these tools inevitably implies the sending of an electronic signal to the devices of individuals so that they may effectively be tracked.

Considering the fact that physical intrusions into a person's home are no longer the only option of intruding upon his personal property in today's modern age, this is a reasonable stance to take as a means to properly ensure the protection of privacy. In essence, with the advent of the Internet, it is now possible to determine information about an individual's private life through intruding upon his personal electronic devices utilizing various technological tools such as the ones adopted for targeted marketing purposes, as

---

[478] *Id.*, par. 173.
[479] *Cooperberg* c. *Buckman*, prev. cited, note 476; *McIlwaine* c. *Equity Accounts Buyers Ltd.*, prev. cited, note 476; *Auger* c. *EquityAccount Buyers Ltd.*, prev. cited, note 476; *Beaudoin* c. *Beaudoin*, prev. cited, note 476; *Pasquale* c. *Descôteaux*, prev. cited, note 476; *Robbins* c. *Canadian Broadcasting Corp. (Québec)*, [1958] C.S. 152; *Lehouillier-Rail* c. *Visa Desjardins*, 2007 QCCQ 10123; *Plante* c. *Bisson*, 2006 QCCQ 3890.

discussed above[480]. In this light, and considering that harassment by telephone was sanctioned by the court as an intrusion into one's domicile, we believe that the use of such tools could potentially be considered as a form of intrusion as well.

The adoption of such a point of view would be tremendously beneficial to online targeted marketers. This is due to the fact that the protection of the solitude of individuals exists "not to bust people for trespass after it has been committed, [but] rather […] to encourage people to keep their doors relatively open in the first place"[481] because "[if] the government did not enforce laws against physical trespass, more potential victims would probably buy locks for their doors"[482]. Applying this perspective to our current situation, such a protection serves to promote a sense of safety that will allow individuals to feel sufficiently at ease to communicate openly and freely, rather than to erect barriers that would hinder communication because they are not properly protected against such privacy invasions. The laws safeguarding the right of individuals to their solitude therefore serve to promote the continued openness of individuals in their dealings on the Internet, and it is upon this that marketers rely for their advertising campaigns, thus making it impossible to deny the benefit of this protection to their cause.

While no Quebec court has ever been approached with a case regarding the possibility that the use of such tools may violate an individual's right to solitude, a recent case decided by the Ontario Court of Appeal[483] has chosen to recognize the collection of information in electronic format to be an intrusion into an individual's seclusion as an extension of his privacy, essentially stating that:

> "It is within the capacity of the common law to evolve to respond to the problem posed by the routine collection and aggregation of highly personal information that is readily accessible in electronic form. Technological change poses a novel threat to a right of privacy

---

[480] *Supra*, p. 10-31.
[481] N. K. KATYAL, prev. cited, note 322, at page 202.
[482] *Id.*
[483] *Jones* v. *Tsige*, 2012 ONCA 32.

> that has been protected for hundreds of years by the common law under various guises and that, since 1982 and the *Charter,* has been recognized as a right that is integral to our social and political order."[484]

We believe, however, that this outlook may be followed by Quebec courts should they be approached with such a matter. This belief is based on the opinion of the Superior Court of Quebec in the case of *Canadian Real Estate Assoc./Assoc. Canadienne d'immeuble* c. *Sutton (Quebec) Real Estate Services Inc.*[485] where they were approached to issue an interlocutory injunction to prohibit the unauthorized use of the plaintiff's website by the defendant. A website being a form of personal property, and the unauthorized nature of the visits being viewed as an intrusion, we believe that a parallel may be made between the two situations. As such, and despite the fact that the foundation of this case was ultimately never decided, the decision of the Court on this particular matter may shed some light on the manner in which Quebec Courts may treat the use of technological tracking tools for the purposes of intruding on an individual's solitude.

In this case, CREA was suing Sutton for having used a particular technology known as spiders[486], which are software agents that are designed to search, copy and retrieve elements on public websites[487] through multiple automated successive requests[488], to copy their real-estate listings, modify them slightly, and place them on their own site. In this case, the Court considered that Sutton was in bad faith due to the fact that it attempted to

---

[484] *Id.*, par. 68.
[485] 2003 CanLII 22519 (QC C.S.) (hereafter "*CREA* v. *Sutton*").
[486] *eBay, Inc.* v. *Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058 (N.D. Cal. 2000); *Register.com, Inc.* v. *Verio, Inc.*, 126 F. Supp. 2d 238 (S.D.N.Y. 2000), affirmed by 356 F.3d 393 (2004) (Ct. App. 2nd Cir.); *Ticketmaster Corp.* v. *Tickets.com, Inc.*, 2000 U.S. Dist. LEXIS 12987; 248 F.3d 1173, 2001 U.S. App. LEXIS 13598 (9th Cir. Cal., 2001); 2003 U.S. Dist. LEXIS 6483; 2005 U.S. App. LEXIS 6227 (9th Cir. Cal., Apr. 11, 2005).
[487] James MACDONALD, "Electronic Trespass in Canada: The Protection of Private Property on the Internet", (2006) 5-3 *C.J.L.T.* 163, 164; Stephen MIDDLEBROOK and John MULLER, "Thoughts on Bots: The Emerging Law of Electronic Agents", (2000) 56 *Bus. Law.* 341, 362.
[488] Richard RAYSMAN and Peter BROWN, "Software Robots and Unauthorized Access to Web Sites", in *New York Law Journal*, November 13, 2006, online: <http://www.thelenreid.com/resources/documents/1106_Computer%20Law.pdf> (site consulted on March 8, 2011).

bypass every technological deterrent that CREA put in its way to prevent it from accessing the site and thus issued the interlocutory injunction.

If we extend this reasoning to the use of technological tracking tools, the same logic could apply. For example, presently, the only real power an individual has over the use of his personal data gathered through cookies is to delete those cookies – the deletion being the technological deterrent meant to prevent his data from being used for targeted marketing purposes. Yet, as discussed above[489], Flash cookies simply re-create those Web cookies that an individual has deleted. Flash cookies are thus being used to overturn the technological deterrent meant to protect an individual's personal information. If we follow the logic of the case of *CREA* v. *Sutton*[490], the use of Flash cookies in this manner would therefore be considered faulty due to its unauthorized nature.

The same logic developed in *CREA* v. *Sutton*[491] can extend to the practice of DPI. It is common for individuals to take the pain to protect their computers from spyware by downloading software meant to detect such invasions and ultimately delete them. The use of DPI by ISPs, however, simply allows these entities to achieve precisely what this anti-spyware software is meant to protect individuals from by using technology that is undetected by the software in question. ISPs thus overturn the only technological deterrent available to users that could keep them at bay, and such behaviour may be considered both faulty and unauthorized if we follow the logic of *CREA* v. *Sutton*[492].

While *CREA* v. *Sutton*[493] could serve to exhibit the potentially illicit nature of the use of tracking tools, the Superior Court simply considers Sutton's use of CREA's website, despite CREA's objections, as an act of bad faith without going into further detail regarding what precisely constitutes an intrusion in the online world. Though it is evident that for the

---

[489] *Supra*, p. 16-17.
[490] *Canadian Real Estate Assoc./Assoc. Canadienne d'immeuble* c. *Sutton (Quebec) Real Estate Services Inc.*, prev. cited, note 485.
[491] *Id.*
[492] *Id.*
[493] *Id.*

use of another's property to be considered an intrusion such use must be unauthorized, we possess no criteria outlining what would constitute such an intrusion in the virtual world.

This element has, however, been extensively analyzed by the American courts in cases relating to trespass on technological devices[494]. While we may not be bound by American decisions, the opinions of the American courts on the manner in which this element ought to be defined are intriguing and, considering that Canadian case law in this domain is lacking, the potential for the Canadian courts to adopt a similar position remains a possibility. Essentially, when analyzing the definition of an "unauthorized intrusion", it is the approach taken by the Northern District Court of California in the case of *eBay* v. *Bidder's Edge*[495] that is most applicable to the issue at hand. In this case, Bidder's Edge possessed an auction site for which it would procure information regarding items available for auction by spidering other auction websites including eBay. The Court concluded that the transmission of these spiders was unauthorized as this type of use of their site was not granted under their terms and conditions[496]. Furthermore, eBay used certain technological barriers meant to stop spiders from accessing their site which were not heeded to by Bidder's Edge, who persisted in the impugned behaviour[497]. The Court thus concluded that the use of spiders on eBay's site was both intentional and unauthorized, essentially taking it a step further than the court in *CREA* v. *Sutton*[498] by taking eBay's terms and conditions into account.

---

[494] *CompuServe Incorporated* v. *Cyber Promotions, Inc.*, 962 F. Supp. 1015 (1997); *Hotmail Corp.* v. *Van$ Money Pie Inc.*, (No. C 98-20064 JW) 1998 WL 388389, *7 (N.D. Cal. 1998); *America Online, Inc.* v. *IMS*, 24 F. Supp. 2d 548, 550-551 (E.D. Va. 1998); *America Online, Inc.* v. *LCGM, Inc.*, 46 F. Supp. 2d 444, 451-452 (E.D. Va. 1998); *eBay, Inc.* v. *Bidder's Edge, Inc.*, prev. cited, note 486; *Register.com, Inc.* v. *Verio, Inc.*, prev. cited, note 486; *Ticketmaster Corp.* v. *Tickets.com, Inc.*, prev. cited, note 486; *Intel Corp.* v. *Hamidi*, 114 Cal. Rptr. 2d 244 (2001); 43 P.3d 587, 118 Cal. Rptr. 2d 546 (2002); 1 Cal. Rptr. 3d 32 (2003) 30 Cal. 4th 1342 71 P.3d 296.

[495] *eBay, Inc.* v. *Bidder's Edge, Inc.*, *Id.*

[496] *Id.*, 1070.

[497] *Id.*

[498] *Canadian Real Estate Assoc./Assoc. Canadienne d'immeuble* c. *Sutton (Quebec) Real Estate Services Inc.*, prev. cited, note 485.

If we transpose this reasoning into the situation whereby an individual's right to solitude is violated by the use of technological tracking tools, it can be said that through his use of various websites, an individual is aware that certain cookies must be placed on his computer for the site to work and could thus be said to accept this form of intrusion into his solitude. Such an authorization is, however, limited to the placement of these cookies on his browser so that he may utilize the site in question, and does not extend to permit the use of cookies to track his behaviour online. The use of cookies in such a manner goes beyond what was, in fact, permitted by the individual and could thus be considered unauthorized.

Similarly, in the case of DPI, individuals allow ISPs to send electronic signals to their personal devices to provide them with an Internet connection. Individuals do not, however, allow ISPs trace their behaviour online through these signals. The use of DPI to track individuals could therefore also be considered an unauthorized intrusion in this respect as the actions taken by ISPs exceed the authorization that was provided to them.

A similar logic could apply in the case of mobile tracking tools. Individuals permit their cellular telephone providers to send satellite signals to their mobile phones so that they may be able to have voice conversations and send text messages and so on. They do not, however, allow these signals to be sent so that their mobile service providers can track their geographic position and target them with ads based on this data. Thus, if we take the criterion established in the case of *eBay* v. *Bidder's Edge*[499], the use of technological tracking tools would consist of a use other than what was authorized by the individuals involved, and may therefore ultimately be considered an intrusion.

Establishing the unauthorized nature of the use of tracking tools through such an approach is intriguing. While this stance was taken in the case of *eBay* v. *Bidder's Edge*[500] with regards to trespass resulting from the unauthorized use of spiders, we believe that this logic should be extended to protect the right to solitude. If the courts were to hold that the

---

[499] *eBay, Inc.* v. *Bidder's Edge, Inc.*, prev. cited, note 486.
[500] *Id.*

simple use by individuals of the Internet or their cell phones establish their consent to the use of tracking tools to trace their behaviour, these individuals may behave in a manner that would serve to limit their use of these devices due to a lack of protection afforded to their right to solitude, as exposed above[501]. However, such an outcome may be avoided by holding that the use of technological tracking tools exceeds the extent of the authorization that individuals provided by allowing them to feel as if their consent was not merely imputed by their use of the Internet or their mobile phones, and would thus serve to ensure their continued use of these elements in a free and open manner.

Considering the economic benefits of such an outlook, we believe that it may be a practicable one for the intents and purposes of Quebec law. In view of the fact that an individual's right to privacy is a fundamental one, we do not believe that its protection would be properly assured by requiring an individual to act in order to exhibit a lack of consent that would establish the bad faith of the entity utilizing technological tracking tools, as would be required if we followed the approach developed in the case of *CREA* v. *Sutton*[502]. That case took place between two companies and we do not believe that adopting this position in the case of individuals whose privacy is being violated would be viable. While it may be useful in establishing the further bad faith of companies that may use technological tracking tools to trace individuals despite their lack of consent, it should not be the only criterion required to demonstrate the element of fault resulting from such unauthorized intrusions.

We therefore believe that the criterion established in *eBay* v. *Bidder's Edge*[503] would better serve to protect the right to solitude of individuals as it actually requires that the consent of individuals be acquired rather than merely imputed as a result of their use of the Internet or their mobile telephones. While this does place a greater obligation upon

---

[501] *Supra*, p. 103-104.
[502] *Canadian Real Estate Assoc./Assoc. Canadienne d'immeuble* c. *Sutton (Quebec) Real Estate Services Inc.*, prev. cited, note 485.
[503] *eBay, Inc.* v. *Bidder's Edge, Inc.*, prev. cited, note 486.

marketers to ensure that they receive authorization for the use of such tools, their respect of this requirement will ultimately benefit them, as exposed above[504].

While we are unsure as to whether or not Quebec law requires the establishment of any criteria other than an unauthorized intrusion, it is interesting to point out that American case law goes even further, essentially requiring a certain level of interference with another individual's possessory interest to establish the existence of an intrusion. There is, however, no consensus as to the degree of interference required. A certain trend in case law merely necessitates a level of interference that consist of simple intermeddling[505], while another demands a more substantial interference to establish such a claim[506].

The question of the degree of interference required, or whether such an element must be established at all, is an important one simply due to the fact that when it comes to

---

[504] *Supra*, p. 103-104.

[505] In the case of *CompuServe, Inc.* v. *Cyber Promotions, Inc.* (prev. cited, note 494), the Court only required proof simple intermeddling, stating that the simple act of sending electronic signals was a sufficient degree of intermeddling to constitute a claim in Trespass to Chattels, noting that substantial interference may not be necessary (*Id.*, 1021; *See:* Edward W. CHANG, "Bidding on Trespass: *eBay, Inc. v. Bidder's Edge, Inc.* and the Abuse of Trespass Theory in Cyberspace-Law", (2001) 29-4 *AIPLA Quarterly Journal* 445, 452; Laura QUILTER, "The Continuing Expansion of Cyberspace Trespass to Chattels", (2002) 17 *Berkeley Technology Law Journal* 421, 429-430; Michael R. SIEBECKER, "Cookies and the Common Law: Are Internet Advertisers Trespassing on Our Computers?", (2003) 76 *Southern California Law Review* 893, 924).

Similarly, in the case previously discussed (*Supra*, p. 107), that of *eBay* v. *Bidder's Edge* (prev. cited, note 486), on the other hand, the Court held that interference existed in this case due to the fact that eBay was able to demonstrate that Bidder's Edge effectively made use of their computer systems (*Id.*, 1070-1071) and that this degree of intermeddling was sufficient enough to establish a claim in trespass. This position was, however, very much criticized due to its general broadness that would essentially "allow a site to obtain an injunction against all unwanted visitors" (Maureen A. O'ROURKE, "Property Rights and Competition on the Internet: In Search of an Appropriate Analogy", (2001) 16 *Berkeley Tech. L.J.* 561, 597). Regardless of this point of view, however, several other cases followed the more liberal position taken in *CompuServe, Inc.* v. *Cyber Promotions, Inc.* (prev. cited, note 494) and in *eBay* v. *Bidder's Edge* (prev. cited, note 486) (*Register.com, Inc.* v. *Verio, Inc.*, prev. cited, note 486; *Oyster Software, Inc.* v. *Forms Processing, Inc.*, 2001 WL 1736382 (N.D. Cal. 2001); *American Airlines, Inc.* v. *Farechase*, *Inc.*, No. 067-194022-02 (67th Dist. Ct. Texas, March 8, 2003)).

[506] The Court in the case of *Intel Corp.* v. *Hamidi* (1 Cal. Rptr. 3d 32 (2003), prev. cited, note 494) required a more substantial level of interference, stating that "the tort does not encompass, and should not be extended to encompass, an electronic communication that neither damages the recipient computer system nor impairs its functioning" (*Id.*, 36) thus essentially maintaining that the level of interference required must be substantial for an intrusion to exist. This position was maintained in other cases as well (*Ticketmaster Corp.* v. *Tickets.com, Inc.*, prev. cited, note 486*; Sotelo* v. *Directrevenue, LLC, et al.,* 384 F. Supp.2d 1219 (N.D. Ill. 2005)).

technological tracking tools, the only tool that interferes *per se* in an individual's personal property are cookies as they are stored on the computer of an individual and are used to track them throughout the Internet. DPI and mobile positioning systems, on the other hand, do not interact with the device itself, but only with the electronic signals emitted from the device in question and such signals could only be a basis for an action in intrusion if the individual has possessory interest in said signals.

In the case of DPI, the packets of information emanating from an individual's computer are intercepted and, inasmuch as these packets contain data generated by this person, we believe that he could hold a possessory interest in these packets. While it is true that the ISP enables the sending of these packets, the individual in question pays for these services and, as such, we are of the opinion that it may be possible to consider any electronic signals originating directly from his computer as belonging to him.

With regards to mobile devices, on the other hand, it is not by any manifest action on the part of the owner of the cellular phone that signals are emitted and tracked, but rather as an inherent part of the technology in question. Whether the signals produced by a person's cellular phone can be considered as an extension of his possessory interest in the mobile device itself, as these signals originate from an item he owns and are necessary to his ability to use that item for its required purposes, on the other hand, is debatable.

This being said, we are not convinced that Quebec law would require any particular level of interference to establish the existence of a fault in light of an unauthorized intrusion on the right to solitude of individuals. The moment an unauthorized intrusion is established, the element of fault has been successfully proven as said intrusion violates the law, thus not requiring any further demonstration. However, we do foresee that a change in perspective may be necessary when it comes to intrusions of a technological nature.

If no threshold is emitted for the level of interference required to institute a claim of technological intrusion, such claims may be instituted by individuals in the event that an electronic signal is sent to their personal device for potentially frivolous reasons and

regardless of whether or not their right to solitude and the inviolability of their domicile is truly affected. Let us take, for example, the case of an individual who had a terrible argument with a friend that put an end to their relationship and this friend decides to send that person an e-mail. While, if we adopt the definition of intrusion that we have developed throughout this subsection, we would come to the conclusion that the act of sending this e-mail was an intrusion *per se*, we do not believe that this form of intrusion ought to be actionable. This is simply due to the fact that this would present an undue strain on the use of the Internet, causing every e-mail sent by a regular individual to be scrutinized and present the potential threat of legal action each time the "send" button is clicked. While it is true that the sending of an e-mail in this example would ultimately have to result in damages for it to be actionable, there are various reasons for which an individual can put forth that he or she has experienced suffering from the e-mail in question.

Thus, when viewing the level of interference required from a targeted marketing perspective it would not necessarily seem wise to have a threshold, as the use of technological tracking tools by marketers without the consent of the individual who are being traced may not always surpass the established threshold and would therefore render such privacy violations un-actionable, we cannot neglect the fact that the Internet is a tool used by nearly everyone and as such, any legal rules developed to regulate it must take the varying uses that are made of the Internet into account. We therefore believe that it would be wise to place a threshold on the level of interference required to establish a technological intrusion essentially making it high enough to exclude any claims that may arise from an intrusion that does not necessarily violate an individual's privacy and would ultimately result in a petty lawsuit that would waste both the time and money of the court system, while making it sufficiently low to ensure that their right to privacy is still adequately protected from true invasions thus maintaining their free and liberal use of the Internet for inter-personal communications[507].

---

[507] *See: Supra*, p. 103-104.

In light of the above analysis, we believe that it may be possible to consider the use of technological tools to track and target individuals with ads without their prior consent, as required by the PIPEDA and the ARPPIPS[508], as being an intrusion into their seclusion as well as their personal property, and therefore ultimately a fault. While it is true that the simple violation of the ARPPIPS by neglecting to acquire an individual's consent prior to collecting his personal information could constitute a fault in and of itself, and thus give rise to an action in civil liability, we believe that the analysis demonstrating that the use of technological tracking tools in Internet marketing could constitute an intrusion into one's solitude and personal property was necessary, simply so as to illustrate the various manners in which the use of such tools could violate an individual's right to privacy. What remains is therefore to determine whether or not said intrusion ultimately results in damages, in order to be capable of establishing an action under section 1457 C.C.Q. for these purposes.

Subsection 2 Damages Resulting From Intrusions on Privacy and Personal Property

In addition to demonstrating fault, it is also necessary to demonstrate the existence of damages to be successful in an action in civil liability in Quebec law. In this respect, damages need not be limited to an injury inflicted on the personal property that was intruded upon, but can extend to any form of damage that is a direct result of the fault that was committed. This makes a great deal of sense, because while the use of technological tracking tools to trespass onto someone's property to intrude into his private life could result in an injury onto that property – which would be actionable in Quebec law – this is not the only damage that is susceptible to occur and it is crucial for the law to recognize this fact. Under such circumstances, damages may also arise under the form of any consequences that may occur directly as a result of the acquisition and use of an individual's personal data that was aggregated at the moment of this trespass, which may result in distress, humiliation or anguish.

---

[508] *See: Supra*, p. 85-101.

The use of such tools renders a person's life an opened book, without it necessarily being desired, and makes it possible for others to discover facts about an individual's lifestyle and personality that he may rather keep confidential. The personal repercussions suffered as a result of this intrusion could therefore qualify as damages sufficient for the establishment of an action in civil liability, as it is a direct consequence of the violation of an individual's privacy achieved by intruding into his private life through trespassing onto his personal property.

* * *

This form of privacy protection follows the same grain as the protection afforded to the personal information of individuals by requiring their consent before their private lives are intruded upon. Intrusions on the solitude of individuals would, in fact, be non-existent if the requirements of both the PIPEDA and ARPPIPS regarding consent are respected. The existence of the fault of intrusion is based upon an individual intruding upon the solitude and personal property of another person *without authorization*. This means that a claim in civil liability for intrusion could no longer exist should the interference in question be consented to, as there could be no fault of trespass should the individual consent to intrusions into his personal life. As such, when it comes to using technological tools to intrude on the private lives of individuals, the proper respect of the requirement of both the PIPEDA and the ARPPIPS[509], obliging organizations to acquire the consent of individuals when such tools are utilized to gather their personal information, would ultimately serve to circumvent any claim a person could have with respect to trespass under such circumstances.

While the privacy issues that abound in the practice of targeted marketing are rather abundant, and the solutions to these problems are not always evident, consent is often times the key in such situations; it is the free and enlightened consent of individuals that will protect Internet marketers against pursuits for either the violation of personal information or

for trespass. Relying on the consent of individuals and respecting all the rules and regulations meant to protect both the personal information and personal property of individuals is the only economically sound position for marketers to take, as demonstrated throughout this chapter. Any other approach would ultimately circumvent the goal meant to be achieved by marketers by limiting the amount of behavioural information available to them, and it is upon their ability to aggregate this data that marketers depend to successfully target individuals with online or mobile advertisements.

While privacy law is very significant when it comes to targeted marketing, and it is crucial for marketers to pay sufficient heed to this area of the law in order to maintain their ability to perform this practice, this is not the only domain of law which may affect the practice of online marketing. There are certain other practices utilized in Internet marketing that may serve to violate competition law, trademark law and consumer protection law – issues which will all be discussed in further detail in the next chapter.

Chapter 2 Unfair Business Practices In Internet Marketing

SEM, the practice of using various techniques to increase a website's position in the search results appearing in online search engines[510], and SMM, the use of social media by companies to maintain a conversation with its consumers[511], are two forms of online marketing that sometimes utilize illicit methods to promote a company's product or service[512]. The use of such methods threatens both competitors, whose position in the market may be decreased as a result, as well as consumers, who tend to be deceived by these underhanded practices. As such, these practices present issues in three areas of the law that are meant to protect both competitors and consumers alike, namely competition law, trademark law and consumer protection law. This chapter will therefore be dedicated

---

[509] *See supra*, p. 85-101.
[510] *Supra*, p. 53-61.
[511] *Supra*, p. 43-52.
[512] *See : Supra*, p. 46-49 and 55-58.

to discussing the legal implications of both SEM and SMM (1) from a competition law and trademark law perspective, and (2) from a consumer protection law perspective.

Section 1 ***The Implications of Search Engine Marketing and Social Media Marketing From a Competition Law and Trademark Law Perspective***

Both SEM and SMM present certain issues with respect to the areas of competition law and trademark law. To begin with, (1) both of these forms of marketing are sometimes used in a manner that may consist of unfair competition. Additionally, there are times when (2) these forms of marketing make use of the trademarks of other companies that could ultimately fall under the gambit of trademark infringement.

Subsection 1 *Unfair Competition in Search Engine Marketing and Social Media Marketing*

The forms of unfair competition that are prominent in SEM and SMM surround (1) the use of certain SEM techniques to dishonestly diminish competition, and (2) the use of SMM to denigrate competitors in the hopes of adversely affecting their business – two issues which will be discussed in further detail below.

Paragraph 1 Unfair Trade Practices in Search Engine Marketing

The *Competition Act*[513] states its purpose to revolve around the "[maintenance] and [encouragement of] competition in Canada"[514] – a purpose which follows the economic basis for competition law, which holds that "the essential factor ensuring competition is the possibility for an entrepreneur to enter the market so as to compete against those that are already a part of it"[515] (our translation). In order to ensure this possibility, however,

---

[513] R.S.C., 1985, c. C-34 (Hereafter referred to as "CA").
[514] *Id.*, section 1.1.
[515] E. MACKAAY AND S. ROUSSEAU, prev. cited, note 22, p. 106.

enterprises must exercise honest business practices that render it possible for new companies to enter the market. As a result, the maintenance of competition depends on the use of such business practices while explicitly rejecting any form of behaviour that would, in any manner, diminish competition.

As discussed above, however, black hat SEM tactics[516], which are underhanded techniques used by companies to increase the ranking of a website, could be considered as an unfair trade practice. While no Canadian court of law has, up until the present, been approached with a case regarding this subject matter, an interesting parallel could be made with the case of *Chocolat Lamontagne Inc.* v. *Humeur Groupe Conseil Inc.*[517], which was decided regarding the use of the trademarks of competitors in the Google AdWords program[518]. The Superior Court judge in this case held that the use of trademarks in such a manner is acceptable and cannot be considered as constituting unfair competition because "[w]hen such an offer does not contain anything unfair [...] the advertiser cannot be held liable for having created the opportunity to be reached"[519]. The use of black hat SEM tactics is, however, considered to be "unfair" in the cyber-world. The analysis emitted by the Court in this case, while not prohibiting the Google AdWords program, may therefore possibly be extended to reason that the use of black hat techniques is illicit as such types of offers *do* contain unfair elements.

In this light, we believe that there is a strong likelihood that Canadian courts will consider this form of behaviour to consist of an unfair trade practice, more particularly because the use of such tactics violates the purpose of the CA. This is due to the fact that the ultimate goal of black hat SEM techniques is to attempt to unjustly and dishonestly exclude a competitor from the online market by lowering their position in the list of results and thus diminishing competition.

---

[516] *Supra*, p. 55-58.
[517] 2010 QCCS 3301.
[518] *See: Supra*, p. 59-61.
[519] *Chocolat Lamontagne Inc.* v. *Humeur Groupe Conseil Inc.*, prev. cited, note 518, par. 126.

The CA, however, confines itself to the regulation of a limited number of practices that may serve to diminish or eliminate competition, none of which could be viewed as including the type of unfair trade practice presented by black hat SEM techniques. It is rather the *Trade-marks Act*[520], at its section 7(e), that serves to regulate such behaviour by prohibiting companies from "[doing] any other act or [adopting] any other business practice contrary to honest industrial commercial usage in Canada"[521]. As such, individuals who use dishonest practices to negatively affect their competitors businesses can be sued for their actions. This section was, however, determined to be *ultra vires* by the Supreme Court of Canada in the case of *Macdonald et al.* v. *Vapor Canada Ltd.*[522], where the judges determined that the regulation of such forms of behaviour falls to provincial competence. As such, each province possesses its own system for regulating unfair trade practices[523], but we will concentrate solely on the one established in Quebec.

In Quebec, unfair trade practices are regulated by the action in disloyal competition which is based on the general regime of civil liability[524] engrained in section 1457

---

[520] R.S.C. 1985, c. T-13 (Hereafter referred to as "TMA").
[521] *Id.*, section 7(e).
[522] [1977] 2 S.C.R. 134.
[523] François GUAY, "Canada", in CENTER FOR INTERNATIONAL LEGAL STUDIES (dir.), *Unfair Trading Practices*, London, Kluwer Law International, 1996, 59, at page 59-60.
[524] *See : Demco Manufacturing Inc.* C. *Goyer d'artisanat Raymon inc.*, 2006 QCCA 52; *Groupe Pages Jaunes Cie.* c. *4143868 Canada Inc.*, 2009 QCCS 5398; 2011 QCCA 960; *Les Accessoires de Bagages Hudson Inc./Hudson Luggage Supplies Inc.* c. *Les Attaches Tri-Point Inc.*, 2003 CanLII 33320 (QC CS); *177197 Canada ltée* c. *J.a. Larue inc.*, 2005 CanLII 49339 (QC CS); *T-Rex Véhicules inc.* c. *6155235 Canada inc.*, 2008 QCCA 947; *Médias Transcontinental, s.e.n.c.* c. *Carignan*, 2009 QCCS 2848; *Husqvarna Corporation Inc.* c. *Service de jardin et forêt enr.*, 2009 QCCS 283; *Boulangerie St-Méthode inc.* c. *Boulangerie Canada Bread ltée*, 2012 QCCS 83; Pierre BOURBONNAIS, *L'action en concurrence déloyale en droit canadien et en droit québécois*, Master's thesis, Montreal, Faculté des études supérieures, Université de Montréal, 1979; Charles CAMIRAND, "Concurrence déloyale, les règles d'application de la responsabilité civile en matière d'imitation de marque de commerce", (1989) 4 R.J.E.U.L. 3, 19; Louis CARBONNEAU, "La concurrence déloyale au secours de la propriété intellectuelle" in Service de la formation permanent, Barreau du Québec, *Développements récents en droit de la propriété intellectuelle*, Cowansville, Éditions Yvon Blais, 1995, p. 239, at page 273-276; Mistrale GOUDREAU, "Concurrence déloyale en droit prive – commentaires d'arrêts", (1984) 15 *R.G.D.* 133, 135-136; Stefan MARTIN and Mélisa THIBAULT, "Le droit de la concurrence déloyale, substitut du droit d'auteur", in ALAI CANADA (dir.), *Un cocktail de droit d'auteur / A Copyright Cocktail*, Montreal, Éditions Thémis, 2007, 247, at page 247; André NADEAU and Richard NADEAU, *Traité pratique de la responsabilité civile*, Montreal, Wilson et Lafleur, 1971, no. 201, p. 219.

C.C.Q.[525], as outlined above[526]. In such cases, the fault would be the use of an unfair trade practice, but the question remains as to what exactly this constitutes. While such practices evidently consist of those which are explicitly prohibited by the law, unfair trade practices also consist of those behaviours "that are contrary to the "honest customs" of the industry and of commerce"[527] (our translation) regardless of the intention of the individual committing such acts[528].

In the case of SEM, the honest norms and customs solely permit the use of white hat techniques to increase ones ranking – all black hat techniques are severely frowned upon. Thus, in such cases, a fault could reasonably consist of the use of any black hat tactics as they cannot be considered to be honest practices. A similar position was upheld in the case of *Convectair NMT inc.* v. *Ouellet Canada*[529], where the issue at hand was the abusive use of meta-tags by the defendant to increase his rankings in online search engines. The Superior Court Judge in this case considered that the use of such underhanded methods by companies to appear higher up on the list of search results is both "dishonest and insidious"[530].

The consideration of dishonest commercial practices, and in this case the use of black hat SEM techniques to increase one's position in search results, as a fault for the intents and purposes of an action in disloyal competition makes complete sense from an economic analysis perspective as it serves to protect both components of the market, namely businesses as well as consumers. It protects businesses by obliging them to use honest practices and not manipulate their position in the market, while at the same time protecting consumers against being provided with false information by companies simply

---

[525] *Civil Code of Quebec*, prev. cited, note 15.
[526] *Supra*, p. 102.
[527] M. GOUDREAU, prev. cited, note 525, 147; *See also :* P. BOURBONNAIS, prev. cited, note 525, p. I; A. NADEAU and R. NADEAU, prev. cited, note 525, no. 205, p. 221; P. TRUDEL, F. ABRAN, K. BENYEKHLEF and S. HEIN, prev. cited, note 29, p. 17-25.
[528] P. BOURBONNAIS, *Id.*, p. 76; M. GOUDREAU, *Id.*, 151.
[529] (1999) R.J.Q. 1430 (C.S.).
[530] *Id.*, par. 5.

to attract their business. In the latter case, the use of black hat SEM tactics could lead a consumer to believe that the company that appears prior to another on the list of search results due to their use of these dishonest practices is more popular or comes more highly recommended when this may not necessarily be true.

In addition to demonstrating the existence of a fault, damages must also be proven to establish an action in disloyal competition. In these types of cases, however, judges often conclude that, once a fault is proven, there is a reasonable probability that damages will follow[531]. This is the only solution that would make sense from an economic analysis perspective as, rather than disturbing the market further by requiring actual evidence of damages, the faulty behaviour will have been stopped prior to its negatively affecting a

---

[531] *See*: *Demco Manufacturing Inc.* v. *Foyer d'artisanat Raymond inc.*, prev. cited, note 525; *Collectif Liberté Inc.* c. *Liberté-magazine Ltée et al*, C.S., Montreal, no. 500-05-0001615-814, February 28, 1980 (J. André Deslongchamps); *Ferland* c. *Larose*, [1982] C.S. 619; *Boutiques Dans un jardin inc.* c. *Société d'importation et de distribution L'art au quotidien inc.*, J.E. 94-959 (C.S.); M. GOUDREAU, prev. cited, note 525, 151-155; The damages that must be established in such cases generally revolve around the plaintiff's loss of clientele which resulted in or will most likely result in an ultimate decrease in his turnover rate. Often times, however, this proof is rather difficult to make, due to the fact that such actions are instituted prior to the occurrence of any damages as well as due to the fact that a company's clientele is generally unstable thus making it difficult to prove that it has, in fact, decreased (M. GOUDREAU, *Id.*, 152; *See for example : Desrosiers* c. *Dubuc Marketing inc.*, 2012 QCCQ 6114, par. 202-209 regarding proof of damages). It is due to this that judges generally infer damages from an existing fault. There are times where, even if the extent of the damages incurred upon the plaintiff are difficult to prove, judges will accord damage interests as well, but only if there is a reasonable establishment of damages in the first place (*See*: *Demco Manufacturing Inc.* c. *Foyer d'artisanat Raymond inc.*, *Id.*; *Collectif Liberté Inc.* c. *Liberté-magazine Ltée et al*, *Id.*; *Ferland* c. *Larose*, *Id.*; *Boutiques Dans un jardin inc.* c. *Société d'importation et de distribution L'art au quotidien inc.*, *Id.*; M. GOUDREAU, *Id.)*.

Contrary to traditional forms of disloyal competition however, damages resulting from disloyal competition occurring online, specifically with regards to SEM, may be easier to prove. Essentially, website owners are generally able to generate statistics that demonstrate the number of individuals that visit their website and whether or not these people reached their website through a search engine (*For example:* GOOGLE ANALYTICS, online: <http://www.google.com/analytics/> (site consulted on March 6, 2012)). As such, it would be possible to take these statistics prior to the use of black hat techniques by a competitor, and then compare them to the statistics generated following the commencement of the use of these tactics. If the statistics demonstrate a decrease in traffic to the website, this may serve as a demonstration of damages which may suggest a link between both the fault and that damages that may have been suffered, simply by demonstrating that the website's traffic lessened around the same time period as the competitor began using black hat techniques. Nevertheless, it must be pointed out that this decrease in traffic could be due to several factors other than the use of black hat techniques, such as a change in seasons or a plummeting of the economy, and it is due to this that such statistics may only act as a *suggestion* that the use of black hat techniques resulted in this decrease.

business thus avoiding any further affectation thereof. This approach serves to minimize the ultimate effect on the market and allow for the pursuit of honest business to continue.

* * *

Thus, when it comes to the use of black hat techniques in SEM, it is very likely that an action in disloyal competition could exist. SEM is not, however, the only form of online marketing in which an action in disloyal competition is an option; SMM also presents this possibility when social media forums are utilized to denigrate competitors – a practice commonly referred to as trade libel. The next paragraph will thus be dedicated to an in-depth discussion of the action in disloyal competition as a result of trade libel.

Paragraph 2 Trade Libel in Social Media Marketing

Various forms of social media, such as SNWs or blogs, are often used by companies to defame their competitors and harm their reputation[532] – behaviour which gives rise to a cause of action in trade libel. Trade libel, also referred to as denigration, is a tactic used to discredit one's competitor in the public eye by attacking either his reputation or his wares and services in the hopes of negatively affecting his business[533]. As discussed above[534], there are many instances in SMM where such actions are committed and tend to result in the plummeting of the competitor's sales. Such behaviour is, however, forbidden by the law – a prohibition which is enshrined in (a) section 7(a) of the TMA at federal law, as well as in (b) the action in disloyal competition for denigration at Quebec civil law, both of which will be discussed in further detail heretofore and applied to the occurrence of trade libel in SMM.

---

[532] *See : Supra*, p. 50-52.
[533] *Dominion Messenger & Signal Co. Ltd.* c. *Vaudrin*, (1924) 30 R.L.n.s. 336 (C.S.); *Sarrazin et al.* c. *Duquette*, (1935) 41 R. de J. 365 (C.S.); M. GOUDREAU, prev. cited, note 525, 136-137; *See also:* P. BOURBONNAIS, prev. cited, note 525, p. 61-71; Paul ROUBIER, *Le droit de la propriété industrielle*, t. 1, Paris, Librairie du Recueil Sirey, 1952, no. 104, p. 544-554.
[534] *Supra*, p. 50-52.

a. Section 7(a) of the Trade-marks Act

To begin with, section 7(a) of the TMA[535] is rather specific in its prohibition and states that "[n]o person shall […] make a false or misleading statement tending to discredit the business, wares or services of a competitor". According to the Supreme Court of Canada in the case of *S. & S. Industries Inc.* v. *Rowell*[536], this section requires the establishment of 3 criteria, namely (1) that the statement be false or misleading, (2) that it concern the business, wares or services of a competitor, and (3) that this competitor incur damages as a result, evidence of lost revenue being sufficient to fulfill this criterion[537].

An action under section 7(a)[538] presents a rather significant benefit[539] for businesses as, rather than solely being permitted to pursue if the statement in question is false, they may institute an action for any statement that is either false[540] *or* misleading[541]. The

---

[535] prev. cited, note 521.
[536] *S. & S. Industries Inc.* v. *Ross Frederick Rowell*, [1966] S.C.R. 419, 48 C.P.R. 193, 56 D.L.R. (2d) 501.
[537] H. R. R. BAIN, "The Law Affecting Comparative Advertising", (1974) 32 *U. Toronto Fac. L. Rev.* 109, 116; This section has its equivalent in Quebec law under section 222(b) of the *Consumer Protection Act* (prev. cited, note 15), which states that "[n]o merchant, manufacturer or advertiser may, falsely, by any means whatever, […] discredit goods or services offered by others". While this section only covers false statements, as opposed to both false and misleading ones, it is still more global than section 7(a) of the TMA (prev. cited, note 521) in that it does not require that the comment in question be made against a competitor. The CPA, however, only serves to regulate relations between merchants and consumers, and as such cannot be directly invoked by the company whose goods or services were discredited.
At the same time, the CPA does create legal obligations for businesses that, if not respected, can cause them to be pursued by other individuals through section 1457 C.C.Q. (*Civil Code of Quebec,* prev. cited, note 15). Section 1457 C.C.Q. imposes a duty upon each person, whether a physical or moral person, to respect the law. Since section 222(b) of the CPA (prev. cited, note 15.) is law, the moment a merchant, manufacturer or advertiser makes false statements that discredit the goods or services offered by another person, this person may therefore pursue the individual from whom said comments originated under section 1457 C.C.Q. In this respect, the transgression of section 222(b) (*Consumer Protection Act*, *Id.*) would consist merely of the fault – damages would still have to be proven in order to establish an action in civil liability. In such cases, the damages that would have to be established would essentially be similar to the damages that must be demonstrated in cases of disloyal competition, as discussed above (*Supra*, p. 120-121).
[538] *Trade-marks Act*, prev. cited, note 521.
[539] Manuel MORASCH, *Comparative Advertising: A comparative study of trade-mark laws and competition laws in Canada and the European Union*, Master's thesis, Toronto, University of Toronto, 2004, p. 15.
[540] In order for a statement to be considered false, it must be determined "whether a reasonable man would take the claim being made as being a serious claim or not […, or] whether the defendant has pointed to a specific allegation of some defect or demerit in the plaintiff's goods" (*De Beers Abrasive Products Ltd.* v. *International General Electric Co. of New York Ltd.*, [1975] 2 All E.R. 599, p. 605).

advantage that lies therein is twofold as, not only does it provide businesses with further opportunities to protect themselves against dishonest forms of competition and allow them to maintain their position in the market, but it also serves to preserve a healthy competitive environment that protects the market against any adverse effects it may suffer due to potentially dishonest trade practices.

Another possible benefit of an action under section 7(a) of the TMA[542] is that the malice or knowledge of the false nature of the statement by the individual from whom it emanates is not necessarily required. Unfortunately, however, while the Court in the case of *S. & S. Industries Inc.* v. *Rowell*[543] distinguished section 7(a) from this respect, future judgments on this section are divided as to whether or not such a distinction should be maintained[544]. Despite this division of the courts, we believe that the interpretation afforded to section 7(a) of the TMA by the Supreme Court in *S. & S. Industries Inc.* v. *Rowell*[545] is the correct one as nowhere does this section require that malicious intent or knowledge of falsehood be established, and as such, such a requirement should not merely be imputed. Furthermore, due to the fact that the TMA[546] is meant to protect trademarks and maintain competition, no other solution would be economically sound. Essentially, regardless of whether or not intent exists in the emission of such false or misleading statements, their effect on the market is often undeniable, and it is precisely against this

---

[541] A misleading statement is one that, while its content may be true, serves to mislead the public far beyond the extent of its veracity (M. MORASCH, prev. cited, note 540, p. 15). For example, if a study is conducted that serves to demonstrate that an individual's product is more efficient than that of his competitor, but merely by a very negligible amount, and the individual in question uses this information to allow the public to infer that his product is significantly better than that of his competitor, such a statement would be considered to be misleading (*Eveready Canada v. Duracell Canada Inc*. (1995), 64 C.P.R. (3d) 348, 352).

[542] prev. cited, note 521.

[543] prev. cited, note 537.

[544] The cases that follow the criteria established in *S. & S. Industries Inc.* v. *Ross Frederick Rowell*, *Id.*, include: *MacDonald et al.* v. *Vapor Canada Ltd.*, prev. cited, note 523; *Enterprise Rent-A-Car Co.* v. *Singer*, [1996] 2 FC 694; *Levi Strauss & Co.* v. *Timberland Company (Inc.) (The)*, 1997 CanLII 6012 (FC); *Almecon Industries Ltd.* v. *Anchortek Ltd.*, 2000 CanLII 16139 (FC); *Uview Ultraviolet Systems Inc.* v. *Brasscorp Ltd*., 2009 FC 58 (CanLII); The cases that equate section 7(a) to the action in libel include: *M & I Door Systems v. Indoco Industrial Door Co. Ltd*., (1989), 25 C.P.R. (3d) 477 (F.C.T.D.); *Sulco Industries Ltd.* v. *Jim Scharf Holdings Ltd.* (1996), 69 C.P.R. (3d) 316 (F.C.T.D., prothonotary).

[545] prev. cited, note 537.

[546] prev. cited, note 521.

effect that section 7(a)[547] is meant to protect businesses. Additionally, obliging companies to demonstrate the existence of malice would simply place an added burden upon them that would make it much more difficult for them to ultimately protect their reputation – an occurrence which would also not be sustainable from an economic perspective.

Thus, if we follow the three criteria established in the case of *S. & S. Industries Inc.* v. *Rowell*[548] and apply them to the various examples provided above[549] regarding the use of social media forums to discredit the business of competitors, we will reach varying results. To begin with, there is no doubt that the company Yili, the victim of the rumours spread by its direct competitor, Mengniu, regarding the fact that their children's milk products cause adolescents to go through puberty prematurely[550], would be successful in an action under section 7(a) of the TMA[551] against Mengniu as well as against the marketers this company paid to spread these falsehoods. Yili is one of Mengniu's largest competitors, and it was established that the rumours were both false and misleading and caused Yili's sales of that specific product to plummet almost immediately.

It may, however, be questionable if an action under section 7(a) of the TMA[552] would be available to Wild Oats Markets, for the attacking comments made by the CEO of its competitor, Whole Foods, in an online forum[553]. While the comments made by the CEO in question may have caused Wild Oats shares to decrease, if Wild Oats' business was, in fact, in trouble, then the comments at issue are not necessarily false. However, depending on the extent of the issues from which Wild Oats was suffering, the comments made by Whole Food's CEO could be considered to be misleading. It is therefore evident that such a situation requires an in-depth analysis of all the facts in question, and whether or not the

---

[547] *Trade-marks Act*, *Id.*
[548] prev. cited, note 537.
[549] *Supra*, p. 50-52.
[550] *Supra*, p. 50-51.
[551] prev. cited, note 521.
[552] *Id.*
[553] *Supra*, p. 50.

Courts would consider an action under section 7(a)[554] to be possible would be based on their examination of all the elements at hand.

The same concerns arise with the possible application of section 7(a)[555] to the situation in which Facebook hired a public relations firm to expose the privacy issues of Google's new feature, as discussed above[556]. Although Google can definitely be considered as one of Facebook's competitors, especially since Google has created its own social network for its users, the actual falsity or misleading nature of Facebook's claims against Google is questionable, in addition to the fact that it does not appear as if Google suffered any adverse effects as a result of Facebook's comments. Thus, while section 7(a)[557] does protect companies from being denigrated by their competitors, the application of this section is limited and the success of any action instituted under this section will be based wholly on the Court's interpretation of the facts of the case with which it is approached.

b. An Action in Disloyal Competition for Denigration Versus an Action in Defamation

The act of denigration is similar to the type of behaviour discussed in the previous section. Though no precise definition of the term has ever been provided in jurisprudence[558], it is generally considered to consist of comments being made to discredit the wares or services of a competitor so as to negatively affect his business[559]. There are

---

[554] *Trade-Marks Act*, prev. cited, note 521.
[555] *Id.*
[556] *Supra*, p. 51-52.
[557] *Trade-marks Act*, prev. cited, note 521.
[558] Marci PINET, *Le Droit de la concurrence déloyale en droit prive québécois*, Master's thesis, Ottawa, l'École des études supérieures, University of Ottawa, 1989, p. 35.
[559] P. BOURBONNAIS, prev. cited, note 525, p. 61 and on ; Rudolf KRASSER, *La répression de la concurrence déloyale dans les états membres de la Communauté Économique Européenne*, translated by Françoise URBAIN, t. 4, Paris, Dalloz, 1972, no.386, p. 282; Louis MERMILLOD, *Essai sur la notion de concurrence déloyale en France et aux États-Unis*, Paris, Pichon et Durand-Auzias, 1954, no. 61, p. 77; M. PINET, *Id.*, p. 34-35; P. ROUBIER, prev. cited, note 534, no. 110, p. 506 and no. 120, p. 544; Eugen ULMER, *La répression*

two actions that serve as a basis of protection against such maligning comments, namely the actions in denigration or defamation.

However, whether or not the latter action could, in fact, be used to protect legal persons from such maligning comments, is unclear. Some implicitly maintain a distinction between the two actions[560], essentially holding that the only one available to legal persons for such purposes is an action in denigration, while others sustain the position that legal persons possess a right to a reputation and, as such, an action in defamation should be available to them[561]. The reason for which this second position is supported is due to the

---

de la concurrence déloyale dans les états membres de la Communauté Économique Européenne, t. 1, Paris, Dalloz, 1967, no. 185, p. 115.

[560] L. CARBONNEAU, prev. cited, note 525, at page 275; M. GOUDREAU, prev. cited, note 525; A similar distinction was made by the Court in the case of *Ferland* c. *Larose*, prev. cited, note 532, where the defendant, an ambulance group, published denigrating comments in a brochure stating that the plaintiff refused to join their group and that this refusal can amount to a refusal to provide a better service essentially disadvantaging the population. In this case, the judge stated that "il est probablement discutable à savoir si cet acte constitue un cas de libelle diffamatoire, mais il tombe clairement dans la catégorie de ceux que les auteurs et la jurisprudence considèrent comme de la concurrence déloyale" (*Ferland* c. *Larose*, *Id.*, 620).

[561] *Price* c. *Chicoutimi Pulp Co.*, (1913) 22 B.R. 393; (1915) 51 R.C.S. 179; *Allure Sportswear inc.* c. *Beiner*, [1960] C.S. 628; *Vaudreil Enterprises Inc.* c. *Soulanges Paving Ltd.*, [1966] B.R. 35; *Magneto Auto Electric ltée* c. *Dubé*, [1966] B.R. 900; *Bélair Carpet Co.* c. *Maisonneuve Broadcasting Co.*, [1975] C.S. 645; *Mouvement Raëlien canadien* c. *Société Radio-Canada*, [1988] R.J.Q. 1662 (C.S.), EYB 1988-83451; *Radio Sept-Îles inc.* c. *Société Radio-Canada*, [1988] R.R.A. 552 (C.S.), EYB 1988-77752; *Saar Foundation Canada Inc.* c. *Baruchel*, [1990] R.J.Q. 2325 (C.S.), EYB 1990-83675; *Borenstein* c. *Eymard*, [1992] R.R.A. 491 (C.A.), EYB 1992-58883; *Damas* c. *Dauphin*, [1993] R.R.A. 357 (C.Q.); *Payette* c. *Beaulieu*, [1994] R.R.A. 267 (C.S.), EYB 1994-73311; *Aliments Ault ltée* c. *Investissements Mongeau inc.*, J.E. 95-1993 (C.S.), EYB 1995-75724; *Collège d'enseignement général et professionnel François-Xavier Garneau* c. *Logiciels Davos ltée*, [1996] R.R.A. 370 (C.S.), EYB 1996-84836; *Groupe R.C.M. inc.* c. *Morin*, [1996] R.R.A. 1005 (C.S.), EYB 1996-30449; B.E. 2000BE-266 (C.A.); *129675 Canada inc.* c. *Caron*, [1996] R.R.A. 1175 (C.S.), EYB 1996-85310; *Centre de psychologie préventive et de développement humain G.S.M. inc.* c. *Imprimerie populaire ltée*, [1997] R.R.A. 376 (C.S.), REJB 1997-00095; [1999] R.R.A. 17 (C.A.), REJB 1999-10604; *Lebeuf* c. *Association des propriétaires du Lac Doré*, [1997] R.R.A. 845 (C.S.), REJB 1997-01597; *Parlec Communication inc.* c. *Librairie Mona Lisait*, B.E. 98BE-709 (C.S.); *Publisystème inc.* c. *Québec (Procureur général)*, [1999] R.R.A. 335 (C.S.), REJB 1999-11356; B.E. 2002BE-184 (C.A.), REJB 2002-27911; *Racicot* c. *Boisvert*, B.E. 99BE-1304 (C.S.); *Barrou* c. *Microbutique éducative inc.*, [1999] R.J.Q. 2659 (C.S.), REJB 1999-14369; *Forget* c. *Cossette*, [2000] R.L. 1 (C.S.); *S.M.C. Pneumatiques (Canada) ltée* c. *Dicsa inc.*, B.E. 2003BE-208 (C.A.), REJB 2003-37817; *Gestion finance Tamalia inc.* c. *Breton*, [2001] R.R.A. 692 (C.S.), REJB 2001-25237; *Daigle* c. *Burniaux*, B.E. 2002BE-291 (C.S.), REJB 2001-26841; *Coutu* c. *Pierre-Jacques*, 2003 R.R.A. 309 (C.S.); *Buchwald* c. *2640-7999 Québec inc.*, J.E. 2003-1694 (C.S.), REJB 2003-47803; *Gilles E. Néron Communication Marketing inc.* c. *Chambre des notaires du Québec*, [2004] 3 S.C.R. 95, REJB 2004-68721; *Croix brisée du Québec* c. *Réseau de télévision TVA*, [2004] R.J.Q. 970 (C.S.), REJB 2004-54361; *Les entreprises Réjean Goyette inc.* c. *Monique Daigneault-Couillard et Hubert Couillard*, EYB 2005-83036 (C.Q.); *Université de Montréal* c. *Côté*, J.E.

fact that sections 3 and 35 C.C.Q.[562] and section 4 of the Quebec Charter[563] accord the right of reputation to "every person" and section 301 C.C.Q.[564] further holds that "[l]egal persons have full enjoyment of civil rights". Since an action in defamation is a corollary to the protection of a right to reputation, many come to the conclusion that this action should be available to legal persons as this right is a civil one that they therefore also enjoy.

In the event that both the actions in denigration and defamation would be available to legal persons, the benefit that such a choice would provide them with is undeniable, and this is for several reasons that on the one hand favour an action in defamation, and on the other hand support an action in denigration. To begin with, while no Canadian court has ever been approached with a case of online denigration, decisions have been rendered in cases of online defamation and it has been held that defamation is considered to exist regardless of the medium used to diffuse defamatory comments[565], including SNWs[566] and blogs[567], where the Courts have considered the same criteria of defamation to apply[568]. It was considered that defamatory comments made on SNWs such as Facebook are injurious[569] and "[attack] the dignity and integrity"[570] of the individual about whom such comments are made.

2006-485; *Rawdon (Municipalité de)* c. *Solo*, 2008 QCCS 4573; J.-L. BAUDOUIN and P. DESLAURIERS, prev. cited, note 473, p. 261; M. PINET, prev. cited, note 559, p. 101.

[562] *Civil Code of Quebec*, prev. cited, note 15.

[563] *Charter of Human Rights and Freedoms*, prev. cited, note 15.

[564] *Civil Code of Quebec*, prev. cited, note 15.

[565] *Société Radio-Canada* c. *Radio Sept-Îles inc.*, [1994] RJQ 1811 (QC CA); *Laforest* c. *Collins*, 2012 QCCS 3078; Bernard BRUN, "Le blogue : un équilibre délicat entre communication et responsabilité", in *Leg@l.TI, droit et technologies de l'information : devenir aujourd'hui l'avocat de demain*, Cowansville, Éditions Yvon Blais, 2007, 73, at page 79; Patrick GINGRAS and Nicolas W. VERMEYS, *Actes illicites sur Internet: Qui et comment poursuivre*, Cowansville, Éditions Yvon Blais, 2011, p. 7.

[566] *See: Thomas* c. *Brand-u Media inc.*, 2011 QCCQ 395; *Lévis (Ville)* c. *Lachance*, 2011 CanLII 2650.

[567] *See: Brassard* c. *Forget*, 2010 QCCS 1530; *National Bank of Canada* c. *Weir*, 2010 QCCS 402; *Corriveau* c. *Canoe inc.*, 2010 QCCS 3396; affirmed by 2012 QCCA 109.

[568] P. GINGRAS and N. W. VERMEYS, prev. cited, note 566, p. 7; *See : Société Radio-Canada* c. *Radio Sept-Îles Inc.*, prev. cited, note 566; *Gestion Finance Tamalia inc.* c. *Breton*, prev. cited, note 562; *Buchwald* c. *2640-7999 Quebec inc.*, prev. cited, note 562; *Abou-Khalil* c. *Diop*, 2008 QCCS 1921 (decision confirmed on appeal : *Diop* c. *Abou-Khalil*, 2010 QCCA 1988).

[569] *Lévis (Ville)* c. *Lachance*, prev. cited, note 567, par. 5.

[570] *Thomas* c. *Brand-u Media inc.*, prev. cited, note 567, par. 19.

Similarly, when the Superior Court of Quebec was approached with a case relative to defamatory comments made on blogs[571], not only did they conclude that the civil liability of the defendant was engaged, but they also noted "the distinctive capacity of the Internet to cause instantaneous, and irreparable, damage to the business reputation of an individual or corporation by reason of its interactive and globally all-pervasive nature of the characteristics of Internet communications"[572]. While, considering the general similarity between the two actions, it may be possible to create a parallel between online defamation and online denigration to establish that the courts would treat cases regarding the latter in the same manner as traditional denigration cases as well, it is impossible to be sure that the courts would establish the same parallel until they are approached with such a case.

Further benefits arising out of the possibility for legal persons to pursue in defamation as well as denigration revolve around the fact that the burden of proof placed upon them differs between the two actions, and depending on the evidence that they have at their disposal, it may be simpler for them to establish one action over the other. While both actions are governed by the general principles of civil liability[573], the manner in which the requisite elements that must be demonstrated to establish a case will differ between actions in denigration and actions in defamation.

To begin with, the action in denigration requires that bad faith be established on the part of the individual being pursued to successfully prove the element of fault[574] – a criterion which is meant to ensure the protection of the freedom of expression[575] but that is not easily proven nor makes much sense when applied to competitive environments. Essentially,

---

[571] *Prud'homme* c. *Rawdon (Municipalité de)*, 2010 QCCA 584; *National Bank of Canada* c. *Weir*, prev. cited, note 568; *Laforest* c. *Collins*, prev. cited, note 566.
[572] *National Bank of Canada* c. *Weir*, *Id.*, par. 46 (quoting *Barrick Gold Corp.* v. *Lopehandia*, [2004] O.J. No. 2329, par. 44); *See also: Laforest* c. *Collins*, *Id.*, par. 121.
[573] *See: Supra*, p. 102.
[574] *Ferland* c. *Larose*, prev. cited, note 484, p. 532; M. GOUDREAU, prev. cited, note 525, 149.
[575] P. TRUDEL, F. ABRAN, K. BENYEKHLEF and S. HEIN, prev. cited, note 29, p. 17-31.

> "every merchant is animated with the desire to acquire the largest possible clientele at the detriment of his competitors. The intention of competitors should therefore not be a criterion used to judge whether or not an act is disloyal. Only the means used to attract the clients of a competitor should be judged."[576] (our translation)

In the case of defamation, a similar stance is taken. Fault is considered to have occurred in the event that an individual voluntarily and with the intention to harm another person attacks the latter's reputation, causing a loss of respect towards that person and exposing him to hatred, contempt or ridicule, or when an individual behaves negligently and in his recklessness harms the reputation of another, thus leading to the same result, without necessarily intending on doing so[577]. It is much simpler to establish such a burden of proof than it is to illustrate the existence of bad faith. Essentially, all that would have to be demonstrated is that a maligning comment was made that ultimately harmed another's reputation to establish the element of fault. Superimposed into the case of denigration, such logic would require that a truly harmful comment be at cause, rather than one that is simply of an ungenerous nature, and such an outlook would ultimately lead to similar results without the difficult burden of proving bad faith[578].

From an economic analysis perspective, such a solution would be the most viable, simply due to the fact that a company's business options are generally based on its reputation. As such, companies should be provided with the tools that enable the protection of their reputation to the highest possible extent; requiring that the presence of bad faith be demonstrated when one of their competitors maligns them entirely defeats this purpose. The end result of any attack on a company's reputation, whether it be intentional or not, will still ultimately be the same and as such the legal recourses available to them ought to

---

[576] M. GOUDREAU, prev. cited, note 525, 151.
[577] *Société Radio-Canada* c. *Radio Sept-îles inc.*, prev. cited, note 566; *Prud'homme* v. *Prud'homme*, [2002] 4 S.C.R. 663, par. 32-37; J.-L. BAUDOUIN et P. DESLAURIERS, prev. cited, note 473, p. 262; Jean PINEAU and Monique OUELLETTE-LAUZON, *Théorie de la responsabilité civile*, 2nd ed., Montreal, Éditions Thémis, 1980, p. 62; A. NADEAU and R. NADEAU, prev. cited, note 525, p. 248.
[578] M. GOUDREAU, prev. cited, note 525, 151.

properly convey this fact and ensure protection and adequate remedies regardless of the intention of their competitor in such cases.

If we apply this obligation to demonstrate bad faith to the examples we provided above[579], we would be confronted with varying results. To begin with, in the case of Whole Foods, where the CEO of that company attacked its competitor, Wild Oats, in an online forum, we are not entirely positive that an action in denigration can be established. While it is true that the CEO in question did make comments that ultimately resulted in the devaluation of Wild Oats' shares, it may be difficult to prove bad faith in that, for all intents and purposes, considering the market at the time, the comments merely reiterated information that was already public. While bad faith may be able to be inferred in light of Whole Foods subsequent offer to purchase Wild Oats later on that year, this offer could only imply bad faith in the event that the decision to purchase Wild Oats was made prior to Whole Foods' CEO's comments being made online. Thus, considering the obligation to prove bad faith, a judge might not necessarily conclude denigration in such a case. Yet, in the same light, regardless of whether or not bad faith played a factor in these statements being made, Wild Oats' reputation still suffered a grave injustice that did ultimately have an effect on their placement in the market. It is thus clear that, in such cases, requiring proof of bad faith is not the most economically viable option as it inhibits companies from mending their reputation and ultimately repositioning themselves within the market.

The cases of Mengniu and Facebook, on the other hand, are both very similar to a case that was tried in the Superiour Court of Quebec entitled *Ferland* c. *Larose*[580]. In this case, the defendant, an ambulance group, published denigrating comments in a brochure stating that the plaintiff refused to join their group and that this refusal can amount to a refusal to provide a better service, thus disadvantaging the population. Considering these facts, the judge concluded to the existence of bad faith, noting that the behaviour of the defendant consisted of an act of disloyal competition in the form of denigration. Applied to

---

[579] *Supra*, p. 50-52.

the cases of Mengniu, where the aforementioned company spread abhorrent rumours about its competitor, and Facebook, where it simply exposed certain privacy issues that Google was experiencing with its new feature, we would reach the same results as the judge did in the case of *Ferland* v. *Larose*. This is mainly due to the fact that, regardless of whether or not the rumours Mengniu spread were false and the ones Facebook spread may have had some truth to them, both companies made such comments to

> "keep their competitor's clients at bay in the hopes that these consumers will resort to purchasing their own products or services. The means utilized are meant to create a doubt in the minds of consumers with regards to the quality of the products or services offered."[581] (our translation)

We therefore see that the requirement to prove bad faith has diverse results in different circumstances.

Another benefit of an action in defamation is that it may be taken against any person that is involved in its communication, whereas an action in denigration may only be taken against a competitor. At the same time, however, while a case in defamation may allow publishers of such comments to be pursued as well, the same might not necessarily be said in cases of *online* defamation. Contrary to traditional forms of communication of information, online publishers, known as intermediaries, simply harbor information, often without monitoring it or controlling it. As such, it is rather difficult to maintain the liability of an intermediary who does not possess the knowledge that defamatory comments may have been made on his website. It is precisely this position that was taken by the Superior Court of Quebec in the case of *Vaillancourt* c. *Lagacé*[582], where the judge stated that "none of the evidence indicates that one or several of the defendants possessed control over the information thereon, nor that they possess the technical capabilities to delete certain

---

[580] prev. cited, note 532.
[581] S. MARTIN and M. THIBAULT, prev. cited, note 525, at page 250-51; *Groupe Pages Jaunes CIE* c. *4143868 Canada Inc.*, prev. cited, note 525.
[582] 2005 CanLII 29333 (QC CS).

comments"[583] (our translation). This therefore demonstrates that the control of the information in question is necessary for an intermediary's liability to be engaged[584].

While not quoting the AELFIT[585], this case follows the regime of liability adopted by that law with regards to which actors may be held liable online, which differs slightly from the one established in virtue of section 1457 C.C.Q.[586] The regime of liability applicable to actors on the Internet in virtue of the AELFIT[587] will vary depending on the degree of control these individuals possess with regards to the content they disseminate. Those individuals that act as intermediaries and merely publish information without having any control over the content thereof will find themselves exempt from liability, unless there is evidence that the impugned content has somehow come to their attention[588]. This content

---

[583] *Id.*, par. 31.
[584] Vincent GAUTRAIS and Pierre TRUDEL, *Circulation des renseignements personnels et web 2.0*, Montreal, Éditions Thémis, 2010, p. 38-40.
[585] *An Act to Establish a Legal Framework for Information Technology*, prev. cited, note 15.
[586] *Civil Code of Quebec*, prev. cited, note 15.
[587] *An Act to Establish a Legal Framework for Information Technology*, prev. cited, note 15.
[588] While the AELFIT (*An Act to Establish a Legal Framework for Information Technology*, prev. cited, note 15) specifies four different types of intermediaries that could see their liability engaged, namely the transmitter, the intermediary that conserves documents for the sole purposes of ensuring the efficiency of their transmission, the intermediary offering referencing services to technological documents as well as the host, we will concentrate on the last two as we believe that they would be the most likely to be sued in such situations. The reason for this is because when a comment is made on a blogging website hosted by another person, this person is considered to be both a host and, due to the fact that blogs often contain hyperlinks to other content, an intermediary providing referencing services as well.

When it comes to these two actors, section 22 of the AELFIT provides a general exoneration by holding that these individuals are not responsible for the manner in which their services are utilized, which is essentially a logical extension of section 27 of the AELFIT which prevents intermediaries from having to perform any acts of surveillance over the content in their possession. As such, as long as the intermediary in question does not play an active role in the content being disseminated, he cannot be presumed to know what it consists of and therefore cannot be held liable for it.

There are, however, certain exemptions to this limitation on liability for both web hosts and intermediaries who provide referencing services which are outlined in section 22 paragraphs 2 and 3 of the AELFIT respectively. These paragraphs state that, although a web host or an intermediary providing referencing services cannot be considered liable for the activities engaged in by others who utilize their services, the moment they become aware of the illicit nature of the information in their possession, they *could* potentially engage their liability. Thus, according to this section, for web hosts or referencing intermediaries to be placed in the position of possibly incurring their liability, they must become aware that the documents in their possession are being used for an illicit activity.

However, due to the fact that these intermediaries are not obliged to actively monitor the information in their possession, the manners in which they can be made aware of the illicit content in their possession are minimal, and essentially limited to three circumstances. To begin with, if the illicit information emanates

must, however, first and foremost be considered to be illicit, meaning that it must contravene the law or constitute a fault[589], for their liability to potentially be engaged, and there is no doubt that defamatory comments fall under this category[590].

---

from the web host or the referencing intermediary itself, there can be no doubt as to their knowledge of this data and it will thus be imputed. Second, though these types of intermediaries are not obliged to actively monitor the documents in their possession, if they choose to do so then they will be presumed to have known that certain illicit information was in their possession. Finally, both a web host and a referencing intermediary will be considered to possess the knowledge that they are harbouring illicit content in the event that they are notified of this fact by a third person, thus rendering it impossible for them to ignore the existence of this information. In the case of a web host, however, section 22(2) of the AELFIT holds that it is also possible for him to incur his liability if he becomes aware of circumstances that make such a use apparent. This could occur, if, for example, the web host comes across certain information which could serve as a clue that would make it apparent that his services are being used for illicit purposes (Pierre TRUDEL, "La responsabilité civile sur Internet selon la Loi concernant le cadre juridique des technologies de l'information", p. 13-14, online : <http://www.chairelrwilson.ca/cours/drt6929f/Resp.%20civile-int.fpbq11-01.pdf> (site consulted on December 10, 2011).

Once the web host or the referencing intermediary receive knowledge that they are in possession of illicit information, they are required to seek the counsel of an objective third party, such as a legal professional, so as to determine whether or not the content in question is of a serious nature and could ultimately result in their liability should the matter be brought before a court of law (P. TRUDEL, *Id.*, p. 15-17; *See also:* P. TRUDEL, prev. cited, note 103, p. 220-222). Such a step is crucial to take because, should the data in question not be illicit, removing it from their website may ultimately result in their commission of a fault towards the individual from whom that information emanated by essentially limiting that person's freedom of expression (P. TRUDEL, *Introduction à la Loi concernant le cadre juridique des technologies de l'information*, *Id.*, p. 220-221).

As soon as the information is confirmed as being illicit by this objective third person, however, both the web host and the referencing intermediary are obliged to act immediately. In the web host's case, section 22(2) of the AELFIT requires him to "act promptly to block access to the documents or otherwise prevent the pursuit of the activity" to protect himself from incurring his liability. In the case of the referencing intermediary, on the other hand, section 22(3) of the AELFIT outlines his obligation to "act promptly to cease providing services to the persons known by the service provider to be engaging in such an activity". The immediate nature of these intermediaries' actions to this effect will be judged based on the amount of time it took them to act from the moment they were assured of the illicit nature of the information. They must, during this time, take the appropriate actions necessary to block all access to the documents or services in question and if they do not act accordingly their liability is very likely to be engaged (Pierre TRUDEL, "La responsabilité civile sur Internet selon la Loi concernant le cadre juridique des technologies de l'information", *Id.*, p. 17). Thus, when it comes to online defamation, the benefit of being in the position of pursuing publishers as well is lost unless the publisher is aware of the defamatory comments on his website and chooses to do nothing about it.

[589] Pierre TRUDEL, "La responsabilité sur internet en droit civil québécois", p. 11, online : <http://www.chairelrwilson.ca/documents/TRUDEL_resp_internet.pdf> (site consulted on December 13, 2011).

[590] Pierre TRUDEL and France ABRAN, "L'évaluation et la prise en charge des risques et enjeux", p. 8, online : <http://www.chairelrwilson.ca/cours/drt3808/prisechargerisquesenjeux.pdf> (site consulted on December 13, 2011).

Limiting the liability of intermediaries online is, effectively, the only solution that would make sense from an economic analysis perspective, especially considering the nature of the Internet. It was best said by Justice Abella in the case of *Crookes* v. *Newton*[591], where she stated that holding web hosts liable for information that does not originate from them and that they have no knowledge of would create a "potential "chill" in how the Internet functions [that] could be devastating"[592] not only to the Internet itself as a device, but also to the market which is beginning to rely more heavily upon the Internet as a mode of effective communication which would be stifled should individuals be held liable for statements that they have no knowledge of. Furthermore, "[if] ISPs were liable for [all the data] on their networks, they might more vigilantly police subscribers to the point where privacy would be eroded"[593] thus causing users to limit their use of this cyberarena and ultimately limit the behavioural data available to marketers, as exposed above[594]. Thus, limiting ISP liability is the only solution that would not hinder the Internet's use, and, while protecting those individuals who have had no active hand in diffusing the message, it does not prevent the pursuit of those that are truly responsible for the acts of defamation.

In light of this, however, the inability for companies to pursue any non-competitor for denigration would, in some circumstances, prevent them from being able to pursue entities that do hold a certain level of liability for the denigration in question. For example, in the cases of Mengniu and Facebook discussed above[595], where marketing firms were hired by these companies to spread rumours about their competitors, it would be unfair to the competitors affected by these rumours to only be able to pursue their direct competitors and not the marketing companies responsible for spreading these falsehoods. It is precisely for situations like these, where companies are denigrated by non-competitors, that we believe they should be entitled to pursue for defamation as well, as otherwise they would have no venue of protection under such circumstances.

---

[591] 2011 SCC 47.
[592] *Id.*, par. 36.
[593] N. K. KATYAL, prev. cited, note 322, at page 211.
[594] *See: Supra*, p. 64-66.

At the same time, however, there is a benefit to the action in denigration that is not present in the action in defamation, namely that the impugned comment or statement is not required to be publicized, whereas publication is considered to be the causal link between the fault and the damages in cases of defamation[596]. However, while it is crucial to identify at least one third person who has heard or read the impugned comment to establish a case in defamation, this may take less of an effort when it comes to online defamation rendering the absence of this requirement for the establishment of an action in denigration less beneficial under such circumstances. Essentially, this element may be established by turning to the statistics generated by websites to establish that the comments at issue have been viewed[597].

The possibility of using these statistics as evidence that the comments in question have, in fact, been read was brought forth by the dissenting judge in the case of *Crookes* v. *Newton*[598]. In this case, what was at issue was an article that contained certain hyperlinks leading to defamatory material. In light of this situation, the judge in question stated that, while proof regarding the number of times the article that contained the hyperlinks leading to the defamatory content had been read was established, there was no information demonstrating the number of times the actual defamatory content was read and whether or not it was accessed through the hyperlinks in question.

Thus, while the facts in this case do not establish the required evidentiary elements therein, this logic can be used to potentially employ website statistics and establish that the libelous comments published on a given website have, in fact, been read by a member of the public. As a result, when it comes to online defamation, the burden of proving that the impugned statements have been viewed by a third person may be much simpler. Thus, while the obligation to prove this element may be one that would normally, in cases of

---

[595] *Supra*, p. 50-52.
[596] *Laforest* c. *Collins*, prev. cited, note 566, par. 66.
[597] *See: Supra*, footnote 532, p. 120-121.
[598] prev. cited, note 592, par. 122.

traditional defamation, lean in favour of instating an action in denigration, the same cannot necessarily be said when it comes to cases of online defamation.

It must, however, be pointed out that while all that is required to be demonstrated in cases of denigration is that a statement was made by a competitor with the intention of ruining a company's reputation, thus not technically obliging proof that a third person had viewed the impugned comments, in order for the affected company to have suffered damages, the comment must have reached a third person and caused them to take their business elsewhere as a result of these statements. The action in denigration therefore does ultimately indirectly require that the comments at issue be viewed by another person so as to be successful.

It is at this point that the differences existing between the actions of denigration and defamation end. There are, however, certain similarities between the two actions that also play a role in the establishment of each type of claim. To begin with, it is crucial that the denigratory or defamatory comments in question be aimed at a specific business or entity, as denigration or defamation cannot exist if the statement at issue is a general one that is aimed at a large group of enterprises, none of which are individually criticized[599].

Furthermore, in order to be able to pursue an individual in either denigration or defamation, it is crucial to establish the identity of the defendant as the one who emitted the maligning statements at issue as it would be impossible to pursue an unknown defendant. When it comes to the publishing of such comments online, however, such a demonstration is not always so easily made. This is due to the fact that it may not be simple to identify the individual from whom the statements emanated as they often use pseudonyms or hire marketers or public relations firms to write them in their place. In the few examples we provided above[600], the identities of all the individuals who made defamatory comments were discovered. In the case of Mengniu, their identity was discovered due to a police

---

[599] *Ortenberg* c. *Plamondon*, (1915) 24 B.R. 385; *Goyer* c. *Duquette*, (1936) 61 B.R. 503; M. PINET, prev. cited, note 559, p. 36; *See also : Bou Malhab* c. *Diffusion Métromédia CMR inc.*, [2011] 1 S.C.R. 214.

investigation; in the case of Whole Foods Market, the identity of their CEO was determined by tracking the IP address to which his pseudonym was linked; and in the case of Facebook, their identity was discovered due to the fact that their publishing firm contacted many bloggers resulting in the issue ultimately going public. While it is true that determining the identity of an individual using a pseudonym is much simpler than determining the identity of an individual who hires other individuals to leak the defamatory comments, there is still no doubt that there are certain difficulties with the identification of individuals who initiate libelous comments online.

While we have, up until this point, exposed the various benefits that lean in favour of instating either an action in denigration or an action in defamation depending on the circumstances at hand, we cannot neglect the fact that a controversy still exists with regards to whether or not legal persons should be permitted to institute an action in defamation in the first place. If, however, we look at both the action in denigration and the action in defamation from an economic perspective, it may be possible to hold that legal persons should be in the position of instituting both.

As outlined above, it is much more difficult to establish an action in denigration, as the plaintiff must prove financial damages as well as malice, both of which are not required to be proven in cases of defamation, thus rendering the latter much easier to establish. The reason for the relative simplicity of instituting an action in defamation as opposed to an action in denigration can be explained using Economic Analysis of Law, which would hold that the adverse economic effects suffered by a company due to denigration will be significantly less than they would be in cases of defamation. Take the following example:

> "If firm A claims that firm B is owned by a devil worshipper, this will cost firm B money (in forgone sales) if customers believe the claim and prefer not to do business with devil worshippers. There may be no efficient way for consumers to ascertain the truth of the devil-worshipper claim, for it is a credence characteristic. In

---

[600] *Supra*, p. 50-52.

> contrast, if firm A claims that the product of firm B will not work well, then consumers can presumably determine the truth of this claim for themselves. Thus the relative ease with which a plaintiff may make out a case for defamation as compared with making out a case of [denigration], which appears mysterious when considered in terms used by courts, may be explicable in terms of the ability of consumers to determine truth and, hence, discount [denigration] more than defamation."[601]

As such, considering the relative effect defamation would have on a company's reputation and thus its economic stability, it is difficult for us to come to any conclusion that would not maintain the possibility for companies to pursue for defamation.

However, in light of the existing controversy, and considering that the action in denigration was created specifically for situations in which legal persons are defamed by their competitors, it might be wisest to simply opt for this course of action in cases where all the evidentiary elements required to establish such a case are present. Despite the fact that, under certain circumstances, an action in defamation might be more beneficial than an action in denigration, the latter still serves to adequately protect legal persons against any harm imposed upon their reputation by an unscrupulous competitor. However, in cases where an action in denigration may not be available to a business, as the entity from whom the maligning comments emanated is not a competitor or they are unable to establish one of the required evidentiary elements, the institution of an action in defamation remains a possibility. Whether or not such an action will be accepted by a court of law, however, will depend upon the position adopted by the court in question.

* * *

There are thus several different manners in which enterprises can protect themselves against trade libel at both federal and civil law, and all these actions can be successfully adapted to apply to the issue of trade libel online. While companies place a great deal of

---

[601] Ellen R. JORDAN and Paul H. RUBIN, "An Economic Analysis of the Law of False Advertising", (1979) 8 *J. Legal Stud.* 527, 537.

importance on protecting their reputation from harmful and false statements, their work at maintaining their company's image does not end there. They must also ensure the maintenance of any goodwill associated with their trademarks by preventing them from being infringed upon by third parties, which is a common eventuality online, as we will discuss in further detail in the next section.

Subsection 2 Trademark Infringement in Search Engine Marketing

Canadian law provides trademark protection for distinctive marks, certification marks, distinguishing guises, and proposed marks against those who appropriate the goodwill of the mark or create confusion between different vendors' wares and services or both[602], essentially considering any unauthorized use of such trademarks as a form of unfair competition. Such protection is provided statutorily under the Canadian TMA[603] by protecting a trademark against infringement or depreciation of goodwill, if the trademark in question is registered, and also at common law and civil law, through the action in passing off, whether the trademark is registered or not[604], and through the action in civil liability respectively.

Despite the protection afforded to trademarks in both Canadian and Quebec law, there are certain online practices whereby individuals utilize the trademarks of other entities for their own purposes. One such practice that has become very well-known is referred to as cybersquatting, which occurs when the domain name of a company's trademark is purchased by another individual. The legal implications of this practice have, however, been thoroughly analyzed by doctrine[605] and we will therefore concentrate on a topic that

---

[602] *Trade-marks Act*, prev. cited, note 421, section 2.
[603] *Id.*
[604] Mark J. FECENKO and Anita M. HUNTLEY, *E-Commerce: Corporate-Commercial Aspects*, Markham, LexisNexis Canada Inc., 2003, p. 171.
[605] *See:* Stacey KING, "The Law That It Deems Applicable: ICANN, Dispute Resolution, and the Problem of Cybersquatting", (1999-2000) 22 *Hastings Comm. & Ent. L.J.* 453; J. Thomas MCCARTHY, "Trademarks, Cybersquatters and Domain Names", (1999-2000) 10 *DePaul-LCA J. Art & Ent. L.* 231; Gregory D. PHILLIPS, "Necessary Protection for Famous Trademark Holders on the Internet", (1998-1999) 21 *Hastings Comm. & Ent. L.J.* 635.

has not been as widely discussed: the use of the trademarks of other companies in certain SEM practices by individuals to further promote their own business online, namely with regards to the practice of using trademarks in doorway pages or in keyword advertising, as discussed above[606]. The question of the hour is thus to determine whether or not this use of trademarks can be considered as infringement in light of both Canadian and Quebec law.

For trademark infringement to exist in the practice of SEM, however, an individual must utilize his competitor's trademark to "profit from the notoriety of this competitor to deceive consumers and invite them to frequent their site as a result of false representations"[607] (our translation). The elements that must be proven to establish a case in infringement will differ depending on whether the trademark in question is (1) registered or (2) unregistered. We will therefore set out the requirements for both causes of action heretofore.

Paragraph 1 Registered Trademarks

In order for the use of registered trademarks to be considered as infringement, an individual must (a) use the trademark of a competitor, and either (b) cause confusion in the minds of consumers, or (c) profit from this competitor's goodwill – conditions which will heretofore be explained in light of the use of trademarks for the purposes of SEM.

a. Use of a Competitor's Trademark

Sections 19, 20 and 22 of the TMA[608] all revolve around the "use" of an individual's trademark. The term "use" is defined by the TMA as "any use [...] in association with wares or services"[609] where the trademark "is marked on the wares themselves or on the packages in which they are distributed"[610] or where "it is displayed in

---

[606] *Supra*, p. 56 and 59-61.
[607] P. GINGRAS and N. W. VERMEYS, prev. cited, note 566, p. 23.
[608] prev. cited, note 521.
[609] *Id.*, section 2.
[610] *Id.*, section 4(1).

the performance or advertising of [...] services"[611]. In light of this definition afforded to the term "use", the question that must be answered is whether or not using a competitor's trademark for the purposes of doorway pages or keyword advertising can be considered as "use" with regards to the TMA[612].

There are two points of view regarding the manner in which the term "use" for the purposes of the TMA ought to be interpreted in light of trademark use on the Internet. One point of view holds that a very literal interpretation should be afforded to the term, and thus considers that only the reproduction of trademarks on wares or their packaging when they are sold from a site could be considering use, thus not taking into account the use of a mark in keyword advertising or doorway pages[613]. We find such an interpretation of the term "use" to be very limitative[614], especially since the Internet is increasingly being used to both promote and purchase products. If we maintain such a restrictive interpretation, the protection of trademarks in the online environment would be confined as all other use of a trademark on the Internet, aside from the affixation of a mark on the wares or their packaging, would fall into a legal void.

It is for this reason that we are of the opinion that it is the second interpretation generally held of the term "use" that ought to be retained for the purposes of online trademark infringement. In the case of *Playboy Enterprises* v. *Germain*[615], the Federal Court stated that it is possible for a "'mark' [to] be associated with the wares (and still be visible) otherwise than by being marked on the wares themselves or on the packages in which the wares are distributed"[616]. This interpretation suggests that the use of a trademark for the purposes of keyword advertising or doorway pages could consist of "use" in light of the definition afforded to the term by the TMA as, when an Internet user types in a

---

[611] *Id.*, section 4(2).
[612] *Id.*, section 2.
[613] Teresa SCASSA and Michael DETURBIDE, *Electronic Commerce and Internet Law in Canada*, Ontario, CCH Canadian Limited, 2004, p. 219.
[614] *Id.*
[615] (1987), 16 C.P.R. (3d) 517, par. 10 and 14.
[616] *Id.*, par. 14.

particular trademark, he will associate the search engine results that appear thereof with the mark in question[617].

We believe that such a definition of the term "use" follows the spirit of the law and serves to ensure that the TMA is economically efficient. In essence, the creation of a trademark relies heavily on the investment of a large sum of money to develop both the trademark as well as the reputation surrounding it. If another entity would be permitted to make use of a trademark in such a manner that may create confusion as to the origin of a ware or service, companies would not see the incentive of investing significant amounts of money into the creation of trademarks[618]. Thus, in order for companies to harbour a desire to invest such high sums of money into the formation of trademarks, they must be guaranteed a certain level of return which would not be able to be ensured should the trademark in question be "used" freely by another entity. As a result, preventing such unauthorized "use" serves to preserve the economic benefits of the TMA.

The form of "use" required to be established will, however, differ for the purposes of sections 19, 20 and 22 of the TMA[619]. To begin with, section 19[620] entitles the registered owner of a trademark to the exclusive right to use that trademark in respect to any wares or services to which their trademark is associated. This right is considered to

---

[617] R. W. TAUBNER, prev. cited, note 20, 309.
[618] William M. LANDES and Richard A. POSNER, "Trademark Law: An Economic Perspective", (1987) 30 *Journal of Law and Economics* 265, 270; A trademark essentially serves to trigger an association in the minds of consumers between a particular mark and a product or service to which it is related, which reduces the amount of research they must perform in order to find the product or service in question. For example, when a consumer wishes to purchase the product or service associated with a trademark, they need merely state that they wish to purchase "X" product of "Y" trademark and they will be able to easily find it and ultimately buy it. If, however, the same trademark is used by various entities for similar products or services, the differentiation that the trademark is meant to create will essentially be nonexistent and the ability for the consumer to easily find it will disappear. In such a circumstance, the return that a company will receive for its investment in a trademark will be minimal as, if a consumer is unable to either associate the trademark with the company's product or even find that product in the first place, the consumer will not end up purchasing the product in question. In maintaining that the trademark may only be effectively "used" by the company that developed it, the TMA is essentially protecting this consumer association as well as the purchase power that accompanies it and is thus effectively maintaining economic efficiency (*Id.*).
[619] *Trade-marks Act*, prev. cited, note 521.
[620] *Id.*

have been violated in the event that this mark is used by another party, for the purposes of similar wares and services, on the wares themselves, or on the packaging thereof, or if it is *used or displayed* in the performance or advertising of a service[621]. Inasmuch as keyword advertising is a form of advertising, regardless of the fact that it differs from traditional forms of advertising at which the TMA was aimed, the use of trademarks identical to the one registered[622] for such purposes could be considered as a violation of section 19[623].

It has, however, been considered by the Exchequer Court in the case of *Clairol International Corp.* v. *Thomas Supply & Equipment Co.*[624] that confusion must also be established for the purposes of section 19. In this case, the Court stated that a trademark is generally "used by a person for the purposes of distinguishing [...] wares or services [...] sold [...] by him from those [...] sold [...] by others"[625]. The adoption of such a definition therefore requires that the wares and services at issue be undistinguishable, thus demanding proof of confusion, for the use of another's trademark to be considered infringement[626]. Thus, while the use of a registered trademark for the purposes of keyword advertising may be considered as a *use or display* of the said trademark in the performance or advertising of a service, infringement for the purposes of section 19 of the TMA[627] will only exist if there is a likelihood of confusion – an element which will be discussed in further detail below[628].

According to the Federal Court[629], the definition of the term "use" applicable to section 20 of the TMA[630], on the other hand, is similar to the one adopted by the Court in

---

[621] *Id.*, art. 4; *Clairol International Corp.* v. *Thomas Supply & Equipment Co.* (1968), 55 C.P.R. 176 (Ex. Ct.).
[622] M. J. FECENKO and A. M. HUNTLEY, prev. cited, note 604, p. 171.
[623] T. SCASSA and M. DETURBIDE, prev. cited, note 614, p. 221.
[624] prev. cited, note 622, (hereafter referred to as "*Clairol"*); *See also:* R. W. TAUBNER, prev. cited, note 20, 309.
[625] *Clairol International Corp.* v. *Thomas Supply & Equipment Co.*, *Id*., 29.
[626] R. W. TAUBNER, prev. cited, note 20, 310.
[627] prev. cited, note 521.
[628] *Infra*, p. 146-152.
[629] *Compagnie générale des établissements Michelin-Michelin & Cie* v. *National Automobile, Aerospace, Transportation and General Workers Union of Canada (CAW-Canada)*, (T.D.), [1997] 2 F.C. 306 (hereafter referred to as "*Michelin*").
[630] prev. cited, note 521.

Clairol[631]. This is due to the fact that this section deals with the use of identical and similar trademarks with respect to *any* wares and services, rather than just registered ones as is required by section 19[632], in a manner that is likely to confuse consumers as to their origin[633]. This section thus also requires the existence of confusion for such "use" to be considered as infringement.

Differently from sections 19 and 20 of the TMA[634], section 22 of the TMA[635] protects the owners of registered trademarks against the depreciation of goodwill[636], rather than confusion, arising from the infringement of their mark in the event that it was used in a *commercial context*[637]. Though section 22 of the TMA[638] has not yet been brought before any Court of Appeal in Canada, and the manner in which it may apply to the Internet has not yet been entirely established[639], the definition upheld of the term "use" by the Courts in relation to this section may prove to aid us in determining the direction the Courts would take in this regard.

In the case of *Clairol*[640], the Court took the opportunity to state that, while it is prohibited to use a competitor's trademark on one's wares for the purposes of comparative advertising, it is possible to use their trademarks on other elements, such as brochures, for such purposes – an interpretation which was upheld by the Federal Court of Appeal in both the case of *Syntex Inc.* v. *Apotex Inc.*[641] and the case of *Michelin*[642]. Thus, it stands to

---

[631] prev. cited, note 622.
[632] *Id.*; M. J. FECENKO and A. M. HUNTLEY, prev. cited, note 605, p. 171; T. SCASSA and M. DETURBIDE, prev. cited, note 614, p. 223.
[633] Bradley J. FREEDMAN and Robert J.C. DEANE, "Trade-marks on the Internet: A Canadian Perspective" (2001) 34 *U.B.C.L. Rev.* 345, par. 15.
[634] *Id.*
[635] prev. cited, note 521.
[636] *Infra*, p. 152-153.
[637] *Compagnie générale des établissements Michelin-Michelin & Cie* v. *National Automobile, Aerospace, Transportation and General Workers Union of Canada (CAW-Canada)*, prev. cited, note 630; *Clairol International Corp.* v. *Thomas Supply & Equipment Co.*, prev. cited, note 622.
[638] prev. cited, note 521.
[639] M. J. FECENKO and A. M. HUNTLEY, prev. cited, note 605, p. 171-172.
[640] *Clairol International Corp.* v. *Thomas Supply & Equipment Co.*, prev. cited, note 622.
[641] [1984] 2 F.C. 1012 (Fed. C.A.).

reason that any *commercial use* of a competitor's trademark on items other than wares or services for the purposes of comparative advertising would not fall under the ambit of section 22 of the TMA[643] as it would not be considered to ultimately depreciate the goodwill of a competitor[644]. Considering the fact that keywords and doorway pages are neither wares nor services, this approach may render it difficult to establish a case under section 22[645] for these purposes. At the same time, however, this does not change the fact that the use of trademarks in the virtual world may depreciate goodwill, as will be discussed in further detail below[646].

Thus, with regards to sections 19 and 20[647], whether or not the use of trademarks in keyword advertising and doorway pages consists of infringement will depend on the existence of a likelihood of confusion, whereas, with regards to section 22[648], it will be based upon whether or not the use of trademarks in such manners can be considered as comparative advertising and, if not, whether the goodwill of one's competitor is depreciated as a result. We will therefore examine each of these elements in the following two sections.

b. Likelihood of Confusion

Confusion is a behaviour whereby a person, through his presentation of a product, creation of a similar trademark, and so on, creates confusion in the minds of consumers between his merchandise and that of another person[649]. As exposed above[650], the existence

---

[642] *Compagnie générale des établissements Michelin-Michelin & Cie* v. *National Automobile, Aerospace, Transportation and General Workers Union of Canada (CAW-Canada)*, prev. cited, note 630.
[643] prev. cited, note 521.
[644] R. W. TAUBNER, prev. cited, note 20, 311.
[645] *Id.*
[646] *Infra*, p. 152-153.
[647] *Trade-marks Act*, prev. cited, note 521.
[648] *Id.*
[649] *Ciba-Geigy Canada Ltd.* v. *Apotex Inc.* [1992] 3 S.C.R. 120; *République française* v. *S. Hyman Ltd.*, (1921) 31 B.R. 22; *Ferland* v. *Larose*, prev. cited, note 532; *Paramount Pictures Corp.* v. *Howley*, (1991) 39 C.P.R. (3d) 419; *Walt Disney Productions* v. *Fantasyland Hotel Inc.*, (1996) 67 C.P.R. (3d) 444; *Wrebbit Inc.* v. *Benoit*, [1998] R.J.Q. 3219; *Shewan* v. *Canada (P.G.)*, (1998) 87 C.P.R. (3d) 475; *Sport Maska Inc.* v. *Canstar Sports Group*, (1994) 57 C.P.R. (3d) 444; *Boutiques Dans un jardin inc.* v. *Société d'importation et de distribution L'art au quotidien inc.*, prev. cited, note 532.

of confusion would entirely circumvent the purposes meant to be achieved by enterprises when they invest in the creation of a trademark. Thus, in protecting trademark holders from situations in which confusion could be rendered possible, the TMA[651] is ensuring that companies continue to harbour the incentive to invest in the creation of trademarks and therefore in the ultimate flourishing of the market.

In order to continue in this economic spirit of the TMA[652], the definition of confusion must be interpreted broadly in its application to the Internet. In this grain, while confusion can generally only exist when the trademark in question is used in association with the same industry in the same geographic region, it has been held by the Supreme Court of British Columbia in the case of *British Columbia Automobile Association* v. *Office and Professional Employees International Union, Local 378*[653] that "the use of similar meta tags unconnected to a defendant's business or operation might indicate deception and might be a significant factor in determining if there is [confusion]"[654]. Meta-tags being the predecessor of keyword advertising, the same logic could apply in this case. Since it has been established by the Courts that there is a possibility of confusion in such cases, we must determine whether or not, based upon the criteria required for confusion to exist, this element can be established in light of keyword advertising.

The criteria upon which the existence of confusion is based are outlined in section 6(5) of the TMA[655] and include

> "(a) the inherent distinctiveness of the trade-marks [...] and the extent to which they have become known;
>
> (b) the length of time the trade-marks [...] have been in use;
>
> (c) the nature of the wares, services or business;
>
> (d) the nature of the trade; and

---

[650] *Supra*, p. 142-143.
[651] prev. cited, note 521.
[652] *Id.*
[653] 2001 BCSC 156.
[654] *Id.*, par. 129.
[655] prev. cited, note 521.

> (e) the degree of resemblance between the trade-marks [...] in appearance or sound or in the ideas suggested by them."[656]

While other factors may also be utilized to establish the existence of confusion[657], we will limit our analysis of the likelihood of confusion with regards to the use of trademarks in keyword advertising and doorway pages to the ones listed in section 6(5) of the TMA[658] aside from the last one, as the visual appearance of a trademark is not at issue when it comes to keyword advertising or doorway pages and this criterion is therefore not relevant to the topic at hand.

The first criterion of section 6(5) of the TMA[659] requires a determination of the extent to which the mark has become known – the more well-known a trademark is, the higher the likelihood of confusion[660]. When it comes to keyword advertising or doorway pages, the use of a trademark for these purposes will require a well-known mark that will often be queried by Internet users, as the goal meant to be achieved by such use is to obtain a higher placement in the search results[661]. One need merely observe the case law regarding the use of trademarks in keyword advertising to support this position. A few examples are the use of the Playboy trademark to promote other pornography websites[662], or the use of the Louis Vuitton trademark to promote the sale of counterfeit Louis Vuitton merchandise[663]. It can thus be considered that most cases in which a competitor's trademark will be used for the purposes of keyword advertising or doorway pages will fulfill the first criterion outlined in section 6(5) of the TMA[664].

---

[656] *Id.*, section 6(5).
[657] *Id.*
[658] *Id.*
[659] *Id.*
[660] R. NELSON ENG, prev. cited, note 20, 512-513.
[661] *Id.*, 512.
[662] *See : Playboy Enterprises, Inc.* v. *Frena*, 839 F. Supp. 1552 (M.D. Fla. 1993).
[663] *See: Google France SARL* v. *Louis Vuitton Malletier SA*, prev. cited, note 295.
[664] prev. cited, note 521.

The second criterion outlined in section 6(5) of the TMA[665] demands that the mark have been in use for a lengthy period of time. This criterion correlates with the first one, as the longer the mark has been integrated within the market, the more well-known that mark will be and the greater the chances are of establishing a likelihood of confusion[666]. Thus, in the event that the first factor is established, the chances that this second element will be fulfilled are quite high.

The third and fourth criteria outlined in section 6(5) of the TMA[667], regarding the nature of the wares, services, business or trade, can be treated together as both require a similarity between the products being offered, since the likelihood of confusion is significantly reduced when the wares or services in question are in wholly different categories[668]. The existence of this factor in the use of trademarks for the purposes of keyword advertising and doorway pages will differ with the facts of each case, but it "will generally lean towards a finding of likelihood of confusion because [it has been] affirmatively [suggested] that direct competitors use competitors' trademarks as keywords"[669] so that when an individual searches a business's name, a link to his competitor's site will appear in the list of results. At the same time, companies often also use the trademarks of businesses that are complimentary to their own, such as utilizing the trademark of an infamous camera company when the product being sold is camera cases[670]. The degree of similarity will therefore differ between cases, and as such, the examination of this element will depend greatly on the facts of the case being presented[671].

Thus, while it is true that the facts of each case will determine whether or not confusion exists when the trademark of a competitor is used for the purposes of keyword

---

[665] *Id.*.
[666] R. NELSON ENG, prev. cited, note 20, 513.
[667] *Id.*
[668] *See: Mr. Submarine Ltd.* v. *Amandista Investments Ltd.*, (1987), 19 C.P.R. (3d) 3; *Fonorala Inc.* v. *Motorola, Inc.*, (1998), 78 C.P.R. (3d) 509); *Provigo Distribution Inc.* v. *Max Mara Fashion Group SRL* [2005] F.C.J. No. 2162.
[669] R. NELSON ENG, prev. cited, note 20, 514.
[670] *Id.*

advertising or doorway pages, there is a strong likelihood that it would. This would therefore render it possible for trademark owners to pursue in virtue of sections 19 and 20[672], while also opening up an action in passing off, either in virtue of section 7 of the TMA[673] for registered marks or at common law for unregistered ones, as well as an action in civil liability, as will be discussed in further detail below[674].

This is the position that was indirectly adopted by the Superior Court in the case of *Convectair NMT inc.* v. *Ouellet Canada*[675]. While this case dealt with the use of a direct competitor's trademark in the meta-tags of a website, ultimately allowing this company to precede the competitor in question in the online search results, we have already established that meta-tags and keyword advertising are similar in nature and outcome[676], and we thus believe that a direct parallel may be made. The Superior Court in this case was, however, only called upon for the purpose of changing the district in which the case is tried, but the judge in question took this opportunity to make some interesting comments in this regard.

To begin with, the judge considered this practice to be "dishonest and insidious [as it] made Ouellet's website appear in the search results of the query "Convectair" with that company's right to do so"[677] and that this use of another's trademark was, in fact, illegal[678]. The judge then goes on to quote the sections of the TMA relative to the prohibition of causing confusion between the wares and services of a competitor, namely section 7(b) and section 20, and, while outlining the plaintiff's cause of action for confusion in order to decide upon which district the case arises from, the judge exudes his opinion that confusion does, in fact, exist in this case[679].

---

[671] *Id.*
[672] *Trade-marks Act*, prev. cited, note 521.
[673] *Id.*
[674] *Infra*, p. 153-156.
[675] prev. cited, note 481.
[676] *Supra*, p. 59.
[677] *Convectair NMT inc.* c. *Ouellet Canada*, prev. cited, note 530, par. 5.
[678] *Id.*, par. 6.
[679] *Id.*, par. 10.

In contrast to this decision, however, the more recent case of *Chocolat Lamontagne Inc.* v. *Humeur Groupe Conseil Inc.*[680] decided in regards to the use of Google AdWords maintains the opposite position. According to the Superior Court in this case

> "[t]he concept of competition must take into account the existence of new ways of interacting with consumers. There is nothing reprehensible with regard to Quebec civil law in the search method proposed by Google.
>
> According to the system used by consumers, [...] the response to the consumer's search request is such that it is up to the consumer to use or not use the information obtained in the results of a search.
>
> [...]
>
> In an economy of open competition, information meant to provide an alternative to other business cannot be prohibited.
>
> [...]
>
> In the Court's opinion, the use of Google Adwords, as the defendant did, to bill itself as the plaintiff's competitor to Web users looking for the plaintiff's site does not constitute unfair competition or passing off [...]."[681]

While it is true that the Google AdWords program is a new form of competition in the online market, and we believe that it is crucial to maintain an open spirit when it comes to regulating the Internet, we cannot support the position held by the Court in this case. Although a consumer does click on a link appearing in Google's search results of their own volition, it remains that it is highly possible that the fact that that particular link appears first in the list of search results may cause consumers to believe that the website to which that link leads is associated with the entity they were searching for[682]. It would ultimately be from this impression given to consumers that these consumers would end up on the website of the competitor of the company they initially searched for. Furthermore, while it

---

[680] *Chocolat Lamontagne inc.* c. *Humeur Group-conseil inc.*, prev. cited, note 518.
[681] *Id.*, par. 96-97, 100 and 125.
[682] *See: France SARL* v. *Louis Vuitton Malletier SA*, prev. cited, note 295.

is true that information meant to provide consumers with an alternative cannot be prohibited, it is the manner in which such information is sought to be provided that is in question in the case of the use of a competitor's trademark in keyword advertising[683]. There are other SEM tactics that could be used to provide this alternative information without necessarily utilizing the trademark of a competitor, as exposed above[684].

We therefore believe that, despite the decision in the case of *Chocolat Lamontagne inc.* c. *Humeur Group-conseil inc.*[685], and considering the above analysis, there may be a possibility of success in the event that actions under sections 19 or 20 of the TMA[686] are taken against the use of trademarks in keyword advertising. In the event, however, that a company wishes to invoke section 22 of the TMA[687] rather than sections 19 or 20[688], they must be in the position of demonstrating the deterioration of goodwill rather than confusion between wares or services, as will be illustrated in the next section.

c. Appropriating a Competitor's Goodwill

As previously exposed, the development of a company's goodwill is what provides companies with the incentive to invest in the creation of a trademark. If the ability to increase their goodwill and market value was non-existent, they would find no benefit in establishing trademarks. Thus, not only is it crucial to protect trademarks against the eventuality of confusion, but it is also important to ensure that their goodwill is protected as well, which is effectively what the TMA achieves through its section 22[689].

In order to establish an action under this section, an individual must prove

---

[683] *See: Id.*
[684] *Supra*, p. 53-55.
[685] prev. cited, note 518.
[686] prev. cited, note 521.
[687] *Id.*
[688] *Id.*
[689] *Id.*

> "(1) that its registered trade-mark was used by the defendant in connection with wares or services; (2) that its mark is sufficiently well known to have significant goodwill attached to it; (3) that its mark was used in a manner likely to have an effect on that goodwill (linkage); and (4) that the likely effect would be to depreciate the value of its goodwill (damage)."[690]

Thus, to determine whether or not an action under section 22[691] would be successful where a competitor's trademark is used in keyword advertising or doorway pages, it is crucial to establish that such use fulfills these four criteria. The criteria regarding the use of the registered trademark as well as the notoriety thereof have already been discussed above[692], so we will therefore concentrate on the latter two criteria which can, in light of the circumstances relating to SEM, be treated simultaneously.

The use of a competitors trademark in keyword advertising or doorway pages will, in most cases, affect the goodwill associated with that mark simply because, rather than the true owner of the mark appearing first in the list of search results, it is his competitor who will hold this position. It often occurs that consumers do not realize that the primary search result they receive is not necessarily linked to the product or service they are searching for, and those who do perceive that the products or services are not identical, are likely to be under the impression that they are related or that the owner of the trademark they searched for is endorsing the entity who appeared first on the list of results and will ultimately be deceived into clicking on the competitor's listing[693]. Thus, by steering consumers towards their own products or services in such a manner, it can be said that they are utilizing the trademark of a competitor in a manner that is likely to have an effect on their goodwill and will, in such a manner, depreciate the value of that goodwill. In this light, it is very likely

---

[690] *Veuve Clicquot Ponsardin* v. *Boutiques Cliquot Ltée*, [2006] 1 S.C.R. 824; *See also : Clairol International Corp.* v. *Thomas Supply & Equipment Co.*, prev. cited, note 622; *Compagnie générale des établissements Michelin-Michelin & Cie* v. *National Automobile, Aerospace, Transportation and General Workers Union of Canada (CAW-Canada)*, prev. cited, note 630.
[691] *Trade-marks Act*, prev. cited, note 521.
[692] *Supra*, p. 141-146 and 148.
[693] R. NELSON ENG, prev. cited, note 20, 512.

that an action under section 22 of the TMA[694] with regards to the use of a competitor's trademark in keyword advertising or in doorway pages would be successful.

Paragraph 2 Unregistered Trademarks

Considering the fact that the market relies heavily on trademarks to both increase competition and provide companies with the incentive to invest money in the creation of a trademark, the law extends its protection not only to registered trademarks, but to unregistered ones as well. The recourses available to individuals who possess unregistered trademarks are (a) the action in passing off at common law and (b) the action in civil liability for either confusion or ambush marketing at civil law.

a. The Tort of Passing Off

The elements required to be proven for the common law action in passing off are very similar to the ones exposed above for the purposes of sections 19, 20 and 22 of the TMA[695]. To begin with, the common law protection against passing off, "occurs when a person passes off their wares or services as those of another so as to take advantage of the goodwill of the other party"[696]. Thus, as opposed to protecting the trademark in and of itself, the action in passing off serves only to protect the goodwill associated with that trademark[697]. The elements required to prove a common law action in passing off are "the existence of goodwill, deception of the public due to a misrepresentation and actual or potential damage to the plaintiff"[698], in a similar manner as exposed above[699], the intentional nature of the misrepresentation not being required[700]. A similar action is available to owners of registered trademarks under section 7(b) and (c) of the TMA[701],

---

[694] prev. cited, note 521.
[695] *Id.*
[696] M. J. FECENKO and A. M. HUNTLEY, prev. cited, note 605, p. 172.
[697] T. SCASSA and M. DETURBIDE, prev. cited, note 614, p. 210.
[698] *Ciba-Geigy Canada Ltd.* v. *Apotex Inc.*, *Id.*, prev. cited, note 650, p. 15-16.
[699] *Supra*, p. 146-153.
[700] T. SCASSA and M. DETURBIDE, prev. cited, note 614, p. 209.
[701] prev. cited, note 521.

however in such cases no damages are required to be proven as the simple violation of their rights under the TMA is sufficient to establish a cause of action.

b. The Action in Civil Liability for Confusion or Ambush Marketing

In civil law, on the other hand, an action for trademark infringement is available under section 1457 C.C.Q.[702]. With respect to trademark infringement claims based on this section, a fault is considered to exist when one of two behaviours are present: confusion or ambush marketing. Confusion has already been exposed above[703]. The behaviour that goes by the name of ambush marketing, on the other hand, only recently emerged in doctrine[704]. It is essentially a type of behaviour whereby a company attempts to create a link between themselves and another company with a greater reputation with the goal of enticing people to purchase their products[705]. Ambush marketing is different from confusion in that there is clearly a distinction made between the two products, but, like a parasite, the link between the two permits one company to live off of the reputation of another[706].

In the event that confusion resulting from the use of trademarks in keyword advertising is not upheld, the possibility that it may consist of ambush marketing may be an interesting position to uphold. The use of a competitor's mark by a company for such purposes could be viewed as an attempt by that company to create a link between itself and its more infamous competitor in the hopes that this may attract consumers towards its own products or services. In such cases, there is clearly no existence of confusion in the minds of consumers, as a distinction is made between both companies, but it could still amount to

---

[702] *Civil Code of Quebec*, prev. cited, note 15; *See: Supra*, p. 102.
[703] *Supra*, p. 146-152.
[704] *See, for example :* Jean-Louis BAUDOUIN, "Le parasitisme", (2001) 31 R.G.D. 789; Jean Jacques BURST, *Concurrence déloyale et parasitisme*, Paris, Éditions Dalloz, 1993; Arnaud LECOURT, *La concurrence déloyale*, 2nd ed., Paris, L'Harmattan, 2004 ; Yves SAINT-GAL, "Concurrence déloyale et concurrence parasitaire ou agissements parasitaires", (1956) 25-26 *Revue internationale de la propriété industrielle et artistique* 19.
[705] *Groupe Pages Jaunes CIE* v. *4143868 Canada inc.*, prev. cited, note 525; *Éditions du Renouveau pédagogique Inc.* v. *Arbour*, [1991] J.Q. no 2573; *Compagnie Gervais Danone SA* v. *Aliments Ultima inc.*, [2006] J.Q. no 17288.
[706] *Éditions du Renouveau pédagogique Inc.* v. *Arbour*, *Id.*

a loss of goodwill on the part of the trademark owner. This would establish the element of damages necessary for such an action, which is analogous to what is required for a case in unfair competition[707], and can be proven in a similar manner as in an action under section 22 of the TMA[708].

The protection of companies against the advent of ambush marketing serves to guard the economic benefits of trademark development, similarly to the sections of the TMA that safeguard companies against confusion and insure their goodwill. In this case, however, what companies are being preserved from is the possibility that another entity could free-ride on both the mark and reputation in whose development they have invested significant funds. Protecting companies against ambush marketing will serve to ensure that they will continue to divest their money for the creation of marks, ultimately increasing competition and ensuring that the economic benefits of trademark law are maintained.

* * *

The protection of trademarks online is thus not nearly as clear cut as might be desirable, nor is it obvious as to the manner in which existing trademark laws ought to be interpreted in light of new technology. Despite this, if analyzed in an open minded manner, current trademark protection could serve to adequately protect trademark holders in this new virtual world. While trademark protection is a serious consideration for companies when it comes to online marketing, this same issue is also confronted with problems from a consumer protection perspective, and will be addressed in the next section.

Section 2 The Implications of Social Media Marketing From a Consumer Protection Law Perspective

Consumer protection laws, as a whole, are meant to shield consumers from the harsh nature of the market and ensure that they are not taken advantage of. One of the

---

[707] *Supra*, p. 120-121.

manners in which the law achieves this feat is by enacting protections meant to ensure that consumers are not subjected to false advertising. False or "[m]isleading advertising occurs when a claim about a product or service is materially false or misleading, in an attempt to persuade the consumer to buy it"[709]. The Internet, however, presents several opportunities for such backhanded forms of advertisements, many companies using blogs and SNWs to create false testimonials to attempt to engage a larger consumer audience, as discussed above in the cases of L'Oreal, Wal-Mart, Sony and Kohl's[710]. In doing so, not only are they deceiving and misleading consumers, but they are also serving to divert consumer purchases away from other competitors that deign to utilize honest business practices. The use of false advertising thus negatively affects the market, and as such, laws have been created to protect both consumers and competitors against this occurrence.

The only Canadian law that deals specifically with false advertising online, however, is the *Anti-Spam Act* which only covers false representations that are made by sending electronic messages to individuals or by including a false representation in a URL[711], therefore not covering the situation of false advertising in social media. As such, we must depend on already existing laws in the domain of false advertising in the traditional sense and extend their application to the case of the creation of false testimonials online. While many laws were enacted to protect consumers from false advertising[712], the principle ones are (1) the CA, on a Canadian level, and (2) the *Consumer Protection Act*, on

---

[708] prev. cited, note 521; *See: Supra*, p. 152-153.
[709] OFFICE OF CONSUMER AFFAIRS, "Canadian Consumer Handbook: Misleading Advertising", online: <http://www.consumerhandbook.ca/en/topics/consumer-protection/misleading-advertising> (site consulted on August 22, 2012).
[710] *Supra*, p. 46-50.
[711] *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act*, prev. cited, note 16, section 75.
[712] *Competition Act*, prev. cited, note 514; *Trade-marks Act*, prev. cited, note 521; *Consumer Packaging and Labelling Act*, R.S.C., 1985, c. C-38; *Textile Labelling Act*, R.S.C., 1985, c. T-10; *Consumer Protection Act,* prev. cited, note 15.

a Quebec level, both of which we will discuss heretofore in light of their possible application to the situation of false advertising in social media.

Subsection 1 The Competition Act

While the CA[713] protects consumers against several forbidden behaviours, it is the prohibition against making "a representation to the public that is false or misleading in a material respect"[714] regarding a particular product for the purposes of promoting any business interest that most applies to the situation of the creation of false testimonials by enterprises in online social media. The deceptive nature of the advertisement must be established by taking into account both "the general impression conveyed by a representation as well as its literal meaning"[715]. The general impression exuded by the creation of false testimonials by companies on online social media forums is that the testimonials in question were created by average consumers. In such cases, regardless of whether or not the testimonial literally makes the false statement that it is created by a consumer or not, the general impression would suffice to establish a claim.

Furthermore, the consideration that a representation is false or misleading in a material respect will be based on whether or not "the context in which it is made […] readily conveys an impression to the ordinary citizen which is, in fact, false or misleading and if that ordinary citizen would likely be influenced by that impression in deciding whether or not he would purchase the product being offered"[716]. Consumers will frequently turn to other individuals in their situation to acquire their opinion about a specific product

---

[713] prev. cited, note 514.
[714] *Id.*, sections 52 and 74.01(a).
[715] *Id.*, sections 52(4) and 74.03(5); *See also:* COMPETITION BUREAU CANADA, "Enforcement Guidelines: Application of the *Competition Act* to Representations on the Internet", October 2009, p. 3-4, online: <http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/vwapj/RepresentationsInternet2009-10-16-e.pdf/$FILE/RepresentationsInternet2009-10-16-e.pdf> (site consulted on April 16, 2012); Douglas J. SIMSOVIC, "i-advertising: the ways and the means", in Vincent GAUTRAIS (dir.), *Droit du commerce électronique*, Montreal, Les Éditions Thémis, 2002, 395, at page 406-407.
[716] *R.* v. *Kenitex Can. Ltd. et al.* (1980), 51 C.P.R. (2d) 103; *See also :* COMPETITION BUREAU CANADA, *Id.*, p. 3-4; D. J. SIMSOVIC, *Id.*, at page 406-407.

or service. The power of recommendation in the consumer world has long been known to be very influential, and as such, reading a false testimonial that is believed to emanate from a consumer will often influence another consumer to purchase the product in question.

While this power of one consumer to influence another may very well be a reason for which a company may create false testimonials, it is very difficult to support an enterprise's use of false advertising from an economic analysis perspective. The economic support for the purposes of advertising stems from the fact that "[n]o matter what kind of goods or services are involved, a decision to advertise conveys information: that the advertiser is willing to invest in his reputation and stands to lose if the customer is unhappy"[717]. When a significant investment is made by a company for advertising purposes, it also becomes clear that "[t]he seller who has invested in his reputation has more to lose by practicing deception than one which has not"[718]. In this light, it is very difficult to comprehend the reason for which a company would invest in advertising, with the ultimate goal of increasing its reputation, only to emit false ads which may only serve to hinder its reputation. Yet, regardless of whether or not the emission of false advertisements by enterprises makes economic sense or not, the reality of the matter is that companies do, as is evidenced by the examples we provided in the cases of L'Oreal, Wal-Mart, Sony and Kohl's[719], and as such, the law serves to protect both consumers and competitors against such an eventuality.

Once it has been established that an advertisement is false or misleading, an inquiry is instituted by the Commissioner of Competition. Such inquiries can result from "[complaints] against any organization that adopts business practices which may be in violation with the [CA]"[720] or from the Commissioner's own choice to investigate a matter

---

[717] E. R. JORDAN and P. H. RUBIN, prev. cited, note 602, 530.
[718] *Id.*, 531.
[719] *Supra*, p. 46-50.
[720] COMPETITION BUREAU CANADA, "How to File a Complaint", December 30, 2011, online: <http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/h_00130.html> (site consulted on: August 21, 2012)

due to his reason to believe that the CA[721] has been or will be violated[722]. It is ultimately based on this inquiry that the Commissioner of Competition will decide whether to pursue the company from whom the false advertisement emanated or not. At the same time, however, the CA does not eliminate the possibility for any individual affected by a violation of the CA to pursue in civil liability[723].

From an economic perspective, the system set up by the CA appears to be viable. While it is true that false advertising serves to mislead consumers into purchasing a product or service which may not live up to the advertisement in question, and such advertising also serves to harm competitors in that they will have experienced a loss of business as a result of the false advertisement that served to increase the flow of customers to the enterprise from whom the advertisement originated, it still remains that it may not be economically beneficial for either consumers or competitors to pursue for such purposes. In the case of consumers, the product or service they may have purchased will not often implicate enough of a loss for it to be beneficial for them to pay the legal fees of pursuit, whether this means simply paying the court fees in cases where a small claims pursuit is possible or paying both the court fees as well as for the services of a lawyer in other cases[724]. In the case of competitors, on the other hand, it is rare that any one company will lose a sufficient amount of profit for it to be economically beneficial for them to invest in a pursuit either, thus resulting in a lack of incentive to pursue under such circumstances[725].

Regardless of the lack of benefit such pursuits may provide in most cases, however, it is true that there are evidently certain situations in which the economic benefit of pursuit will be beneficial as the loss in question will have been high[726]. Despite this, these cases are not numerous enough to justify pursuit being the only option in cases of false

---

[721] prev. cited, note 514.
[722] *Id.*, section 10.
[723] *Id.*, sections 62 and 74.08.
[724] E. R. JORDAN and P. H. RUBIN, prev. cited, note 602, 531.
[725] *Id.*, 531 and 535.
[726] *Id.*, 536.

advertisement as it would not often be used by consumers and competitors alike and thus would not provide a sufficient level of protection against such underhanded forms of advertising[727]. As such, the creation of the system enshrined in the CA[728] serves to ensure that companies do not take advantage of the knowledge that they will often not be pursued when the amounts lost by consumers or competitors are minimal so as to emit false advertising, as they know that they will ultimately face the wrath of the law regardless of whether or not a consumer or competitor chooses to pursue them. Furthermore, while ensuring this protection, such a system does not exclude the possibility for those consumers or competitors who have directly been affected by a violation of the CA and have experienced a heavy loss to pursue in civil liability, thus allowing for the possibility of pursuit should an individual wish it[729].

Not only does the system provide the benefits outlined above, but it also possesses two separate regimes between which the Commissioner of Competition has a choice of pursuing: the civil regime[730] and the criminal regime[731]. While both the civil and criminal regimes prohibit the making of false or misleading representations in a material respect, they differ slightly in the consequences they foresee. The civil regime enables the court to order the enterprise to cease distributing false ads, to disseminate a notice to those individuals affected by the false or misleading representation notifying them of its existence and other details in that respect, and to oblige them to pay an amount of money not exceeding that which the enterprise amassed as a result of the advertisement in question[732]. The criminal regime, on the other hand, provides that the affected enterprise will be opened to severe sanctions which, when it is a conviction on indictment, includes a fine left up to the discretion of the Court or a prison sentence of up to 14 years, or both, and when it is on

---

[727] *Id.*, 531-532.
[728] prev. cited, note 514.
[729] *Id.*, sections 62 and 74.08.
[730] *Id.*, section 74.01(a).
[731] *Id.*, section 52.
[732] *Id.*, section 74.1.

summary conviction, includes a fine not exceeding 200,000$ or a prison sentence of up to 1 year, or both.

Considering the severe nature of the sanctions outlined in the criminal regime, the establishment of a cause of action under this system will require that the false or misleading representation in question be made knowingly or recklessly, thus demanding proof of the required element of *mens rea* for all criminal acts[733]. As such, it is considered by the Competition Bureau that this regime only applies in the most serious of cases[734], especially because it is often very difficult to establish the true intention of the enterprise that emitted the false advertisement[735], even though all that is required to demonstrate intent in such cases is that the ad in question had the ultimate effect of deceiving consumers[736].

As a result, certain criteria were developed by the Competition Bureau to determine the serious nature of a case, namely whether or not the prejudice suffered by both consumers and competitors is so substantial that the civil regime would not be sufficient to remedy it, the vulnerability and exploitation of the group of people subjected to the false advertisement such as children and the elderly, that no steps were taken to remedy the situation quickly and the false advertising persisted even after they discovered the falsity of its nature, and that this behaviour contravened either a previous engagement, a promise to take corrective measures against such forms of advertising, or an order of prohibition[737]. At the same time, however, the bureau will take certain attenuating factors into account[738] such as whether or not a criminal pursuit or a guilty sentence would be too severe considering

---

[733] Christophe MASSE, "La publicité trompeuse dans le commerce électronique", December 2000, p. 8, online : <http://www.juriscom.net/uni/etd/06/pub01.pdf> (site consulted on : August 22, 2012).
[734] COMPETITION BUREAU CANADA, "Information Bulletin, Misleading Representations and Deceptive Marketing Practices: Choice of Criminal or Civil Track Under the Competition Act", September 20, 1999, p. 2, par. 3, online: <http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/vwapj/ct01181e.pdf/$file/ct01181e.pdf> (site consulted on August 22, 2012).
[735] C. MASSE, prev. cited, note 734, p. 8.
[736] *R.* v. *Wholesale Travel Group*., [1991] 3 R.C.S. 154, 8 C.R. (4th) 145, 38 C.P.R. (3d) 451, 67 C.C.C. (3d) 193, 84 D.L.R. (4th) 161, 7 C.R.R. (2d) 36, 130 N.R. 1, 49 O.A.C. 161.
[737] COMPETITION BUREAU CANADA, prev. cited, note 735, p. 2, par. 3.
[738] C. MASSE, prev. cited, note 734, p. 8.

the circumstances or whether or not the enterprise concerned had established an efficient program to ensure its conformity to the law[739].

Requiring such conditions to be met prior to pursuing under the criminal regime is the only solution that ensures economic protection. If each time a different company caught emitting false advertisements were to be pursued under the criminal regime, it would be difficult for such companies to sustain themselves given the heavy consequences with which they would be faced. As such, competition would inevitably lessen and the market would suffer in turn. If, however, the Commissioner of Competition pursues under the civil regime, the consequences suffered by the company at fault would serve to both make amends for its error as well as allow the company enough latitude to rise in the market once again. Furthermore, considering the value of a reputation in a competitive market, the consequences foreseen under the civil regime, namely the requirement that a public statement be made regarding their violation of the CA[740], would appear to be a sufficient deterrent for companies. It therefore makes a great deal of sense from an economic perspective to limit criminal pursuits to only the most serious of cases.

Thus, while the creation of false testimonials on social media forums definitely falls under the description provided in the CA[741], the question is whether or not this form of false advertisement fulfills the criteria emitted by the Competition Bureau to be able to establish a criminal case in this respect. Unfortunately, it is impossible for us to provide a definitive answer with regards to this matter, as the establishment of the criteria provided by the Competition Bureau will differ on a case by case basis, but the possibility that the Competition Bureau will allow the criminal pursuit of enterprises who create false testimonials online most definitely exists.

---

[739] COMPETITION BUREAU CANADA, prev. cited, note 735, p. 2, par. 4.
[740] prev. cited, note 514.
[741] *Id.*, sections 52 and 74.01.

Subsection 2 The Consumer Protection Act

On the Quebec level, the *Consumer Protection Act*[742] holds that "[n]o merchant, manufacturer or advertiser may, by any means whatever, make false or misleading representations to a consumer"[743]. While the prohibitions under the heading of false advertisements are extensive and varied so as to cover several specific situations in which deceptive publicity might be an issue[744], the case of the creation of false testimonials would fall under the general prohibition against false representations which holds that a "representation includes an affirmation, a behaviour or an omission"[745]. In most cases of false testimonials, the individuals creating them on behalf of companies omit to point out that they are not the consumers that they give off the impression of being, but are rather representatives of the company being supported in the testimonial.

Furthermore, these testimonials make certain affirmations as to the general good quality of the product or service being offered by the company in question and, regardless of whether or not such affirmations may be true, they are made in light of the aforementioned omission thus causing them to be false representations by nature. Thus, in the examples we provided above[746] regarding the false testimonials created by L'Oreal Paris, Wal-Mart, Sony and Kohl's wherein company representatives provided positive comments regarding their products and services, we find ourselves in a situation of false representations as covered by the CPA[747].

In cases where false representations exist, it is not required to demonstrate that a consumer was, in fact, deceived, but simply rather that the possibility of deception exists[748]. Furthermore, considering that the creation of the testimonial by a company representative

---

[742] prev. cited, note 15 (Hereafter referred to as "CPA").
[743] *Id.*, section 219.
[744] *See : Id.*, sections 220-253.
[745] *Id.*, section 216.
[746] *Supra*, p. 46-50.
[747] prev. cited, note 15.
[748] *Id.*, section 217; Nicole L'HEUREUX, *Droit de la consommation,* 5th ed., Cowansville, Éditions Yvon Blais, 2000, p. 347; C. MASSE, prev. cited, note 734, p. 17.

could be considered an important fact[749], the consumer benefits from a presumption of fraud as "it is presumed that had the consumer been aware of such practice, he would not have agreed to the contract or would not have paid such a high price"[750]. When it comes to false testimonials, it is true that often times the recommendation of another consumer will steer an person towards purchasing a particular product or service. As such, in cases where the testimonial was created by a company representative, it can be presumed that a consumer would not have purchased that specific product or service had he been aware that the testimonial was, in fact, not created by a fellow consumer.

It is crucial to point out, however, that the CPA[751] only "applies to every contract for goods or services entered into between a consumer and a merchant in the course of his business,"[752] meaning that any action taken against a merchant in virtue of the CPA may only be taken by a consumer and not another merchant. As mentioned above[753], however, it is rare that a consumer will have suffered such a significant loss from false advertising that it would be economically viable for him to pursue. As such, and with analogous economic results, the Quebec CPA[754] has developed a solution similar to the one established in the CA[755]. The CPA essentially creates the *Office de la protection du consommateur* that is charged with ensuring that the provisions of the CPA are respected and whose president, or any consumer advocacy group that has existed as a legal person for a year or longer, "may apply to the court for an injunction ordering the person to cease engaging in the practice"[756] if a person has engaged or engages in false advertising or other practices prohibited by the second title of the CPA[757]. In such a manner, the law continues

---

[749] *Consumer Protection Act*, *Id.*, section 228.
[750] *Id.*, section 253.
[751] *Id.*
[752] *Id.*, section 2.
[753] *Supra*, p. 159-160.
[754] prev. cited, note 15.
[755] prev. cited, note 514.
[756] *Consumer Protection Act*, prev. cited, note 15, section 316.
[757] *Id.*

to protect consumers without necessarily expecting them to make an investment in a pursuit that may not ultimately be economically beneficial for them.

Ultimately, when a case for false representations is established against a company, the CPA foresees three different types of sanctions which entities guilty of false representations may suffer, namely ordinary contractual sanctions offered in civil law, administrative sanctions proffered by the *Office de la protection du consommateur* and penal sanctions against the advertiser or his directors[758].

* * *

The protection of consumers against the creation of online false testimonials by company representatives is therefore ample and serves to ensure that consumers are not taken advantage of, even in the event that it may not be economically reasonable for them to pursue the emitter of false advertising themselves. While leaving it up to the Commissioner of Competition or the President of the *Office de la protection du consommateur* to pursue for such contraventions may not have the ultimate result of reimbursing the consumers or competitors for their loss, such a solution serves to ensure that the corporations which emit false advertising ultimately face the wrath of the law in cases where they will not be pursued by consumers or competitors, so that they may cease to continue in both their deception of consumers as well as their diversion of business towards themselves due to false representations. In such a manner, negative effects on the market are reduced and an economic balance is maintained.

---

[758] C. MASSE, prev. cited, note 734, p. 17.

CONCLUSION

The Internet is an environment that is ripe with marketing opportunities and essentially facilitates the ability of marketers to appeal to consumers. It enables marketers to aggregate a significant amount of behavioural data regarding individuals with very little effort, while at the same time providing a forum upon which they may interact with consumers as well as be approached by them.

Prior to the emergence of the cyber world, the ability for marketers to achieve these feats required a great deal of effort on their part and, even then, did not allow them to attain their goals as easily and efficiently as is rendered possible by the advent of the Internet. The simplicity with which this virtual environment allows marketers to accomplish their objectives is thus undeniable, and the temptation of marketers to take advantage of these tools to their fullest possible extent is therefore entirely comprehensible.

At the same time, however, and as exposed throughout this thesis, often times, utilizing these tools to their maximum capacity, to ultimately increase the turnover rate of businesses as much as possible, does not necessarily take the legal rules protecting both individuals and businesses into account. While the Internet may be, for all intents and purposes, a marketing goldmine, utilizing it without paying heed to legal rules can prove to be tremendously destructive to both marketers as well as the market in general. This is true with regards to the use of technological tracking tools to invade the privacy of individuals without acquiring their consent, as while it allows for the aggregation of unprecedented amounts of behavioural data, neglecting to seek the approval of these individuals prior to the use of such tools could ultimately serve to limit their communications which would thus destroy the vast mine of data available to marketers.

This is also true when black hat SEM tactics are used to increase a business's visibility in online search engines as well as when businesses denigrate their competitors in online social media forums. Such behaviour would create a market founded on falsehoods

which would make it difficult for businesses to compete based on their true merits. This may ultimately result in the creation of a market that is not competitively proficient and may thus render it impossible for the pursuit of honest business to ensue. Furthermore, the knowledge that enterprises behave dishonestly and lie about their value or the worth of their competitors would ultimately create a doubt in the mind of consumers when they interact with businesses. This may place a strain on consumer-business relations and cause them to question the veracity of the information provided to them by companies – an outlook which could severely affect the efficiency of the market which depends greatly on consumers.

Finally, the use of the trademarks of competitors to increase a company's online presence would also present a strain on the market by eliminating the benefits for enterprises to invest in the creation of trademarks thus causing them to devote less of their budget to the conception of such marks and ultimately diverting this monetary influx from the market thus reducing its efficiency.

The destructive capability that may exist by using Internet marketing tools to their greatest capacity, without taking legal rules into consideration, can thus not be denied. However, as we have demonstrated throughout this thesis, it is neither necessary nor recommended for marketers to throw caution to the wind by utilizing this newfound playground of opportunities in any which way. It is possible for marketers to remain within the boundaries of the law and fulfill the purposes they seek – an approach which may, in fact, aid them in achieving their desired goals rather than hinder them in the process.

To begin with, the proper respect of privacy laws when aggregating consumer information, both online and in the physical world, for targeted marketing purposes would negate the destructive capacity of this form of marketing by making individuals feel safe in this virtual environment and thus not inhibiting their communications.

Similarly, ensuring the respect of competition laws and consumer protection laws would both serve to ascertain that the market remains efficient. Avoiding any behaviour that may consist of unfair competition would serve to maintain honest competition and

therefore guarantee the ability of new competitors to enter the market as well as require those already present to compete in a truthful manner. This flows with the respect of consumer protection laws, as it is only the respect of these laws as well as the use of honest business practices that would establish an honest market and thus ensure that consumers continue to have faith in businesses and the advertisements that are issued to them – an element upon which marketing efficiency depends.

In this light, it is evident that it is always the tactic that serves to respect the laws in force that will steer marketers in the right direction and ultimately allow them to achieve their goals to the utmost of their capacity. In essence, the nature of marketing requires marketers to strive for the most economically sound option, but it is not always the simplest route that will result in an immediate influx of revenue that is the best choice from an economic perspective. There are elements other than monetary incursions that must be taken into account to ensure that an approach is, in fact, truly beneficial from an economic perspective – one of these elements being the observance of legal rules and regulations.

While respecting the laws in force may require a certain investment that would otherwise be unnecessary, as we have exposed throughout this thesis, devoting a certain budget to this end would present marketers with significant long term benefits that may even surpass the immediate advantages they may experience by not observing the law. The consideration that must steer marketers is therefore whether or not their approach in marketing to individuals respects the laws in force – a consideration that we would stress going forward, as it is only such a perspective that would shed an epiphanic light on the best possible approach to be taken when it comes to marketing in both the virtual and physical worlds.

Keeping this consideration in mind is tremendously crucial. While this thesis outlines the legal implications of the use of various technologically enhanced marketing tools, the nature of the Internet is such that the relevance of these situations will lessen over time and it is only this consideration that will continue to serve marketers as well as legal

professionals by aiding them in adopting the most economically and legally sound approaches possible.

In this grain, there is already a relatively new virtual environment in which this consideration may prove useful: that of media sharing websites which are becoming very prominent in the online world. Such sites "[empower] users to upload multimedia content [such as] videos, images, podcasts and other forms of media"[759] the most popular one of which is YouTube, a video sharing site. This website unites all of the elements outlined throughout this thesis that allows for proficient online marketing. It enables marketers to aggregate a significant amount of information about users regarding their preferences by keeping track of the types of videos viewed by individuals. At the same time, it serves to publicize businesses, by allowing them to create their own channels "where a company can post and share content that is its own on its own customizable page [where users] can then watch the videos, rate them, and leave comments on them"[760], thus also providing them with a discussion forum upon which enterprises may converse with their clients. Furthermore, they may advertise their company as well, as when a user requests a video on YouTube, an advertisement will sometimes be imposed upon the user prior to the video beginning.

This one website is therefore a platform that allows for the combined accomplishment of Online Behavioural Advertising, SMM and SEM, effectively creating a prime marketing venue whose potential is only now beginning to be tapped into. In the same manner as this platform unites all the various forms of Internet marketing into one particular website, however, it is also accompanied by a combination of all the legal issues presented by the different types of Web marketing. It is the interaction of these legal issues on a single website that we believe to be an element of interest as, while it is entirely possible that the legal effects would be the same should the various forms of marketing remain separate, it is also a possibility that the common interaction of these legal issues in a

---

[759] D. J. PERDUE, prev. cited, note 197, p. 12.

single environment may serve to create a greater aura of complexity that could provide an interesting basis of analysis and may serve to raise more questions as to the manner in which such an environment ought to be treated.

Regardless of what ultimately ensues, however, what was true throughout this thesis and will continue to be true going forward is that foresight is never an asset in the business world and limiting one's goals to the achievement of immediate gratification may present dire consequences in future. This statement rings true particularly with respect to the practice of online marketing as, while the greatest monetary influx would result from the use of Internet marketing tools to their highest possible capacity, the failure to assume a global outlook that takes the law into account would ultimately serve to achieve less in the long run, as exposed throughout this thesis. It is thus crucial to adopt an approach that takes economic viability into account – both from a monetary as well as a legal perspective – which would serve to increase the turnover rate of a company, not just in the immediate future, but in the distant one as well.

While the future may be unforeseeable to us, we are of the belief that this will always remain true simply due to the fact that human interaction is the basis for marketing, and it is thus this interaction that must be encouraged to maintain a fruitful market. In order to efficiently promote such inter-personal relations, one must cater to human nature which disposes people to only trust what they know and balk at what they do not. The only manner in which to acquire and maintain the trust of individuals, however, is by respecting the laws in force – laws that were created to rule the society in which we live by protecting all the people that reside in it and ultimately promoting trust as a basis for societal interactions.

---

[760] H. WINN, prev. cited, note 223, 17.

TABLE OF LEGISLATION

Constitutional

Canadian Charter of Rights and Freedoms, part 1 of the *Constitution Act of 1982*, [schedule B to the *Canada Act 1982*, 1982, c. 11 (U.K.)]

Federal

An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act, S.C. 2010, c. 23

Competition Act, R.S.C., 1985, c. C-34

Consumer Packaging and Labelling Act, R.S.C., 1985, c. C-38

Criminal Code, R.S.C. 1985, c. C-46

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

Textile Labelling Act, R.S.C., 1985, c. T-10

Trade-marks Act, R.S.C. 1985, c. T-13

Provincial

An Act Respecting the Protection of Personal Information in the Private Sector, L.R.Q., c. P-39.1

An Act to establish the Legal framework for information technology, R.S.Q., c. C-1

Charter of Human Rights and Freedoms, L.R.Q., c. C-12

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

Consumer Protection Act, R.S.Q., c. P-40.1

TABLE OF JUDGMENTS

Canadian Jurisprudence

Canada (Information Commissioner) v. *Canada (Commissioner of the Royal Canadian Mounted Police*), [2003] 1 S.C.R. 66

Canada (Information Commissioner) v. *Canada (Transportation Accident Investigation and Safety Board)*, 2006 F.C.A. 157

Canadian Real Estate Assoc./Assoc. Canadienne d'immeuble c. *Sutton (Quebec) Real Estate Services Inc.*, 2003 CanLII 22519 (QC C.S.)

Centre de psychologie préventive et de développement humain G.S.M. inc. c. *Imprimerie populaire ltée*, [1997] R.R.A. 376 (C.S.), REJB 1997-00095; [1999] R.R.A. 17 (C.A.), REJB 1999-10604

Centre local de services communautaires de l'érable c. *Lambert*, [1981] C.S. 1077

Chocolat Lamontagne Inc. v. *Humeur Groupe Conseil Inc.*, 2010 QCCS 3301

Choueke c. *Coopérativ ed'habitation Jeanne-Mance*, [2001] R.J.Q. 1441 (C.A.), infirmed J.E. 95-880 (C.S.)

Ciba-Geigy Canada Ltd. v. *Apotex Inc.* [1992] 3 S.C.R. 120

Clairol International Corp. v. *Thomas Supply & Equipment Co.* (1968), 55 C.P.R. 176 (Ex. Ct.)

Collectif Liberté Inc. c. *Liberté-magazine Ltée et al*, C.S., Montreal, no. 500-05-0001615-814, February 28, 1980

Collège d'enseignement général et professionnel François-Xavier Garneau c. *Logiciels Davos ltée*, [1996] R.R.A. 370 (C.S.), EYB 1996-84836

Compagnie générale des établissements Michelin-Michelin & Cie v. *National Automobile, Aerospace, Transportation and General Workers Union of Canada (CAW-Canada)*, (T.D.), [1997] 2 F.C. 306

Compagnie Gervais Danone SA v. *Aliments Ultima inc.*, [2006] J.Q. no 17288

Convectair NMT inc. v. *Ouellet Canada*, (1999) R.J.Q. 1430 (C.S.)

Cooperberg c. *Buckam*, [1958] C.S. 427

Corriveau c. *Canoe inc.*, 2010 QCCS 3396; affirmed by 2012 QCCA 109

Coutu c. Pierre-Jacques, 2003 R.R.A. 309 (C.S.)

Croix brisée du Québec c. *Réseau de télévision TVA*, [2004] R.J.Q. 970 (C.S.), REJB 2004-54361

Crookes v. *Newton*, 2011 SCC 47

Dagg v. *Canada (Minister of Finance)*, [1997] 2 S.C.R. 403

Daigle c. *Burniaux*, B.E. 2002BE-291 (C.S.), REJB 2001-26841

Damas c. *Dauphin*, [1993] R.R.A. 357 (C.Q.)

De Beers Abrasive Products Ltd. v. *International General Electric Co. of New York Ltd.*, [1975] 2 All E.R. 599

Demco Manufacturing Inc. C. *Goyer d'artisanat Raymon inc.*, 2006 QCCA 52

Deschamps c. *Renault Canada*, [1977] 18 C. de D. 1937

Desrosiers c. *Dubuc Marketing inc.*, 2012 QCCQ 6114

Dominion Messenger & Signal Co. Ltd. c. *Vaudrin*, (1924) 30 R.L.n.s. 336 (C.S.)

E. c. *Office de la protection du consommateur*, [1987] C.A.I. 350

Éditions du Renouveau pédagogique Inc. v. *Arbour*, [1991] J.Q. no 2573

Enterprise Rent-A-Car Co. v. *Singer*, [1996] 2 FC 694

Eveready Canada v. Duracell Canada Inc. (1995), 64 C.P.R. (3d) 348

Ferland c. *Larose*, [1982] C.S. 619

Field c. *United Amusement Co.*, [1971] C.S. 283

Finding #13, 2009 CanLII 74730 (P.C.C.)

Finding #162, 2003 CanLII 37655 (P.C.C.)

Finding #2009-010, September 2009, online: <http://www.priv.gc.ca/cf-dc/2009/2009_010_rep_0813_e.cfm> (site consulted on March 16, 2012)

Finding #243, 2003 CanLII 38403 (P.C.C.)

Finding #244, 2003 CanLII 38237 (P.C.C.)

Finding #25, 2001 CanLII 21526 (P.C.C.)

Finding #263, 2004 CanLII 22905 (P.C.C.)

Finding #308, 2005 CanLII 27670 (P.C.C.)

Finding #315, 2005 CanLII 37355 (P.C.C.)

Finding #319, 2005 CanLII 50763 (P.C.C.)

Finding #77, 2002, online: http://www.priv.gc.ca/cf-dc/2002/cf-dc_021016_7_e.cfm> (site consulted on March 17, 2012)

Finding #78, 2002, online: <http://www.priv.gc.ca/cf-dc/2002/cf-dc_021016_6_e.cfm> (site consulted on March 17, 2012)

Finding #8, July 16, 2009, online: <http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm> (site consulted on March 25, 2012)

Finding #80, 2002, online: <http://www.priv.gc.ca/cf-dc/2002/cf-dc_021016_4_e.cfm> (site consulted on March 17, 2012)

Finding #81, 2002, online: <http://www.priv.gc.ca/cf-dc/2002/cf-dc_021016_3_e.cfm> (site consulted on March 17, 2012)

Finding #82, 2002 CanLII 42385

Finding #83, 2002 CanLII 42324

Fonorala Inc. v. *Motorola, Inc.*, (1998), 78 C.P.R. (3d) 509)

Forget c. *Cossette*, [2000] R.L. 1 (C.S.); *S.M.C. Pneumatiques (Canada) ltée* c. *Dicsa inc.*, B.E. 2003BE-208 (C.A.), REJB 2003-37817

Gariépy c. *Naud*, EYB 2006-100784 (C.S.) (appeal refused EYB 2007-116806)

Gauthier c. *Syndicat des employés de la Bibliothèque de Québec*, [1997] C.A.I 1

Gestion finance Tamalia inc. c. *Breton*, [2001] R.R.A. 692 (C.S.), REJB 2001-25237;

Gilles E. Néron Communication Marketing inc. c. *Chambre des notaires du Québec*, [2004] 3 R.C.S. 95, REJB 2004-68721

Gordon v. *Canada (Health)*, 2008 F.C. 258

Goyer c. *Duquette*, (1936) 61 B.R. 503

Groupe Pages Jaunes Cie. c. *4143868 Canada Inc.*, 2009 QCCS 5398; 2011 QCCA 960

Groupe R.C.M. inc. c. *Morin*, [1996] R.R.A. 1005 (C.S.), EYB 1996-30449; B.E. 2000BE-266 (C.A.)

Hunter v. *Southam*,[1984] 2 S.C.R. 145

Huot c. *Martineau*, [2005] J.L. 75 (C.S.)

Husqvarna Corporation Inc. c. *Service de jardin et forêt enr.*, 2009 QCCS 283

Institut d'assurance du Canada c. *Guay*, J.E. 1998-141 (C.Q.)

James Richardson & Sons v. *Ministry of Nat'l Revenue*, [1984] 1 S.C.R. 614

Jones v. *Tsige*, 2012 ONCA 32

Laforest c. *Collins*, 2012 QCCS 3078

Latreille c. *Choptain*, J.E. 97-1475 (C.S.)

Lebeuf c. *Association des propriétaires du Lac Doré*, [1997] R.R.A. 845 (C.S.), REJB 1997-01597

Lehman v. *Heenan Blaikie*, [2005] CAI 433

Lehouillier-Rail c. *Visa Desjardins*, 2007 QCCQ 10123

Les Accessoires de Bagages Hudson Inc./Hudson Luggage Supplies Inc. c. *Les Attaches Tri-Point Inc.*, 2003 CanLII 33320 (QC CS)

Les entreprises Réjean Goyette inc. c. *Monique Daigneault-Couillard et Hubert Couillard*, EYB 2005-83036 (C.Q.)

Levi Strauss & Co. v. *Timberland Company (Inc.) (The)*, 1997 CanLII 6012 (FC)

Lévis (Ville) c. *Lachance*, 2011 CanLII 2650

M & I Door Systems v. Indoco Industrial Door Co. Ltd., (1989), 25 C.P.R. (3d) 477 (F.C.T.D.)

Macdonald et al. v. *Vapor Canada Ltd*, [1977] 2 S.C.R. 134

Magneto Auto Electric ltée c. *Dubé*, [1966] B.R. 900

McIlwaine c. *Equity Accounts Buyers Ltd.*, [1974] R.L. 115 (C.P.)

Médias Transcontinental, s.e.n.c. c. *Carignan*, 2009 QCCS 2848

Mouvement Raëlien canadien c. *Société Radio-Canada*, [1988] R.J.Q. 1662 (C.S.), EYB 1988-83451

Mr. Submarine Ltd. v. *Amandista Investments Ltd.*, (1987), 19 C.P.R. (3d) 3

National Bank of Canada c. *Weir*, 2010 QCCS 402

Olteanu c. *Zellers inc.*, B.E. 99BE-1205 (Q.C.)

Ortenberg c. *Plamondon*, (1915) 24 B.R. 385

Paramount Pictures Corp. v. *Howley*, (1991) 39 C.P.R. (3d) 419

Parlec Communication inc. c. *Librairie Mona Lisait*, B.E. 98BE-709 (C.S.)

Pasquale c. *Descôteaux*, [1990] R.R.A. 574 (C.S.)

Payette c. *Beaulieu*, [1994] R.R.A. 267 (C.S.), EYB 1994-73311

Pelletier c. *Emery*, J.E. 97-1360 (C.S.)

Plante c. *Bisson*, 2006 QCCQ 3890

Playboy Enterprises v. *Germain*, (1987), 16 C.P.R. (3d) 517

Price c. *Chicoutimi Pulp Co.*, (1913) 22 B.R. 393; (1915) 51 R.C.S. 179

Provigo Distribution Inc. v. *Max Mara Fashion Group SRL* [2005] F.C.J. No. 2162

Prud'homme c. *Rawdon (Municipalité de)*, 2010 QCCA 584

Prud'homme v. *Prud'homme*, [2002] 4 S.C.R. 663

Publisystème inc. c. *Québec (Procureur général)*, [1999] R.R.A. 335 (C.S.), REJB 1999-11356; B.E. 2002BE-184 (C.A.), REJB 2002-27911

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

R. v. *Duarte*, [1990] 1 S.C.R. 30

R. v. *Goldman*, [1980] 1 S.C.R.. 976

R. v. *Kenitex Can. Ltd. et al.* (1980), 51 C.P.R. (2d) 103

R. v. *Weir*, (1998) 59 Alta. L.R. (3d) 319 (B.R.), confirmed by (2001), 156 C.C.C. (3d) 188 (C.A.)

R. v. *Wholesale Travel Group*., [1991] 3 R.C.S. 154, 8 C.R. (4th) 145, 38 C.P.R. (3d) 451, 67 C.C.C. (3d) 193, 84 D.L.R. (4th) 161, 7 C.R.R. (2d) 36, 130 N.R. 1, 49 O.A.C. 161

Racicot c. *Boisvert*, B.E. 99BE-1304 (C.S.); *Barrou* c. *Microbutique éducative inc.*, [1999] R.J.Q. 2659 (C.S.), REJB 1999-14369

Radio Sept-Îles inc. c. *Société Radio-Canada*, [1988] R.R.A. 552 (C.S.), EYB 1988-77752

Rawdon (Municipalité de) c. *Solo*, 2008 QCCS 4573

Reeves c. *Fasken Martineau DuMoulin*, [2001] C.A.I 322

Reibeiro c. *Shawinigan Chemicals*, [1973] C.S. 389

Reid c. *Belzile*, [1980] C.S. 717 (C.S. Q.C.)

République française v. *S. Hyman Ltd.*, (1921) 31 B.R. 22

Robbins c. *Canadian Broadcasting Corp. (Québec)*, [1958] C.S. 152

Robbins c. *Canadian Broadcasting Corporation*, [1958] C.S. 152

S. & S. Industries Inc. v. *Ross Frederick Rowell*, [1966] S.C.R. 419, 48 C.P.R. 193, 56 D.L.R. (2d) 501

Saar Foundation Canada Inc. c. *Baruchel*, [1990] R.J.Q. 2325 (C.S.), EYB 1990-83675

Sarrazin et al. c. *Duquette*, (1935) 41 R. de J. 365 (C.S.)

Savard c. *All Tour Marketing*, [1998] R.R.A. 649 (C.Q.)

Ségal c. *Centre de services sociaux de Québec*, [1988] C.A.I. 315

Shewan v. *Canada (P.G.)*, (1998) 87 C.P.R. (3d) 475

Société Radio-Canada c. *Radio Sept-Îles inc.*, [1994] RJQ 1811 (QC CA)

Sport Maska Inc. v. *Canstar Sports Group*, (1994) 57 C.P.R. (3d) 444

Sulco Industries Ltd. v. *Jim Scharf Holdings Ltd.* (1996), 69 C.P.R. (3d) 316 (F.C.T.D., prothonotary)

Syntex Inc. v. *Apotex Inc.*, [1984] 2 F.C. 1012 (Fed. C.A.)

The Gazette c. *Valiquette*, [1997] R.J.Q. 30 (C.A.)

Thomas c. *Brand-u Media inc.*, 2011 QCCQ 395

Tousignant c. *Bernier*, J.E. 87-1211 (C.S.)

T-Rex Véhicules inc. c. *6155235 Canada inc.*, 2008 QCCA 947

Université de Montréal c. Côté, J.E. 2006-485

Uview Ultraviolet Systems Inc. v. *Brasscorp Ltd*., 2009 FC 58 (CanLII)

Vaillancourt c. *Lagacé*, 2005 CanLII 29333 (QC CS)

Vaudreil Enterprises Inc. c. *Soulanges Paving Ltd.*, [1966] B.R. 35

Veuve Clicquot Ponsardin v. *Boutiques Cliquot Ltée*, [2006] 1 S.C.R. 824

Walt Disney Productions v. *Fantasyland Hotel Inc.*, (1996) 67 C.P.R. (3d) 444

Wilkie c. *Lapensée*, J.E. 2005-938 (C.S.)

Wrebbit Inc. v. *Benoit*, [1998] R.J.Q. 3219

American Jurisprudence

America Online, Inc. v. *IMS*, 24 F. Supp. 2d 548, 550-551 (E.D. Va. 1998)

America Online, Inc. v. *LCGM, Inc.*, 46 F. Supp. 2d 444, 451-452 (E.D. Va. 1998)

American Airlines, Inc. v. *Farechase, Inc.*, No. 067-194022-02 (67th Dist. Ct. Texas, March 8, 2003)

CompuServe Incorporated v. *Cyber Promotions, Inc.*, 962 F. Supp. 1015 (1997)

eBay, Inc. v. *Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058 (N.D. Cal. 2000)

Hotmail Corp. v. *Van$ Money Pie Inc.*, (No. C 98-20064 JW) 1998 WL 388389, *7 (N.D. Cal. 1998)

Intel Corp. v. *Hamidi*, 114 Cal. Rptr. 2d 244 (2001); 43 P.3d 587, 118 Cal. Rptr. 2d 546 (2002); 1 Cal. Rptr. 3d 32 (2003) 30 Cal. 4th 1342 71 P.3d 296

Oyster Software, Inc. v. *Forms Processing, Inc.*, 2001 WL 1736382 (N.D. Cal. 2001)

Playboy Enterprises, Inc. v. *Frena*, 839 F. Supp. 1552 (M.D. Fla. 1993)

Re DoubleClick Inc. Privacy Litigation, *154 F. Supp. 2d 497, online:* <http://cyber.law.harvard.edu/is02/readings/doubleclick.html> (site consulted on October 22, 2012).

Register.com, Inc. v. *Verio, Inc.*, 126 F. Supp. 2d 238 (S.D.N.Y. 2000), affirmed by 356 F.3d 393 (2004) (Ct. App. 2nd Cir.)

Sotelo v. *Directrevenue, LLC, et al.,* 384 F. Supp.2d 1219 (N.D. Ill. 2005)

Ticketmaster Corp. v. *Tickets.com, Inc.*, 2000 U.S. Dist. LEXIS 12987; 248 F.3d 1173, 2001 U.S. App. LEXIS 13598 (9th Cir. Cal., 2001); 2003 U.S. Dist. LEXIS 6483; 2005 U.S. App. LEXIS 6227 (9th Cir. Cal., Apr. 11, 2005)

French Jurisprudence

Google France SARL v. *Louis Vuitton Malletier SA*, Joined Cases C-236/08, C-237/08 & C-238/08, 2010 ECJ EUR-Lex LEXIS 119 (Mar. 23, 2010)

BIBLIOGRAPHY

Monographs and Collective Works

ANDERSON, C., *The Long Tail: Why the Future of Business is Selling Less of More*, New York, Hyperion, 2006

BAUDOUIN, J. L., *La Responsabilité Civile*, 4th ed., Cowansville, Yvon Blais, 1994

BAUDOUIN, J.-L. and P. DESLAURIERS, *La Responsabilité Civile*, 7th ed., vol. 1, Cowansville, Les Éditions Yvon Blais, 2007

BLANCHETTE, F., *L'expectative raisonnable de vie privée et les principaux contextes de communications dans Internet*, Master's thesis, Montreal, Faculté des études supérieures, University of Montreal, 2001

BOURBONNAIS, P., *L'action en concurrence déloyale en droit canadien et en droit québécois*, Master's thesis, Montreal, Faculté des études supérieures, Université de Montréal, 1979

BURST, J. J., *Concurrence déloyale et parasitisme*, Paris, Éditions Dalloz, 1993

CHASSIGNEUX, C., *Vie privée et commerce électronique*, Montreal. Éditions Thémis, 2004, p. 24-44

CLAY, B. and S. ESPARZA, *Search Engine Optimization: All-in-One For Dummies*, Hoboken, Wiley Publishing, 2009

CLAY, B. and S. ESPARZA, *Search Engine Optimization All-in-One for Dummies*, New Jersey, John Wiley & Sons, 2012

COLE, E., *Network Security Bible*, 2nd ed., 2009, Indianapolis, Wiley Publishing

DELEURY, É. and D. GOUBAU, *Le droit des personnes physiques*, 4th ed., Cowansville, Les Éditions Yvon Blais, 2008

ERBSCHLOE, M., *Trojans, Worms, and Spyware: A Computer Security Professional's Guide to Malicious Code*, Oxford, Elsevier Butterworth-Heinemann, 2005

FANELLI-ISLA, M., *Guide pratique des réseaux sociaux: Twitter, Facebook…des outils pour communiquer*, Paris, Dunod, 2010

FECENKO, M. J. and A. M. HUNTLEY, *E-Commerce: Corporate-Commercial Aspects*, Markham, LexisNexis Canada Inc., 2003

GAUTRAIS, V. and P. TRUDEL, *Circulation des renseignements personnels et web 2.0*, Montreal, Éditions Thémis, 2010

GINGRAS, P. and N. W. VERMEYS, *Actes illicites sur Internet: Qui et comment poursuivre*, Cowansville, Éditions Yvon Blais, 2011

GOLLMANN, D., *Computer Security*, New York, John Wiley & Sons, 1999

GRATTON, E., *Internet and Wireless Privacy: A Legal Guide to Global Business Practices*, Toronto, CCH Canadian, 2003

GRATTON, E., *Wireless Privacy and Personalized Location-based Services: The Challenge of Translating the Legal Framework into Business Practices*, Master's thesis, Montreal, Faculté des études supérieures, University of Montreal, 2002

HURLEY, C., F. THORNTON, M. PUCHOL and R. ROGERS, *Wardriving: Drive, Detect, Defend: A Guide to Wireless Security*, Rockland, Syngress Publishing, 2004.

INDUSTRY CANADA, *La protection de la vie privée et l'autoroute canadienne de l'information: une nouvelle infrastructure de l'information et des télécommunications*, Ottawa, Industry Canada, 1994

KARR, D. and C. FLANNERY, *Corporate Blogging for Dummies*, Indianapolis, Wiley Publishing, 2010

KISSELL, J., *Mac Security Bible*, Indianapolis, Wiley Publishing, 2010

KRASSER, R., *La répression de la concurrence déloyale dans les états membres de la Communauté Économique Européenne*, translated by Françoise URBAIN, t. 4, Paris, Dalloz, 1972

KURAN, T., *Private Truths, Public Lies: The Social Consequences of Reference Falsification*, Cambridge, Harvard University Press, 1995

L'HEUREUX, N., *Droit de la consommation,* 5th ed., Cowansville, Éditions Yvon Blais, 2000

LECOURT, A., *La concurrence déloyale*, 2nd ed., Paris, L'Harmattan, 2004

LOTT, J., D. SCHALL, and K. PETERS, *Actionscript 3.0 Cookbook*, Sebastopol, O'Reilly, 2006

MACKAAY, E. and S. ROUSSEAU, *Analyse économique du droit*, 2nd ed., Montreal, Éditions Thémis, 2008

MERMILLOD, L., *Essai sur la notion de concurrence déloyale en France et aux États-Unis*, Paris, Pichon et Durand-Auzias, 1954

MORASCH, M., *Comparative Advertising: A comparative study of trade-mark laws and competition laws in Canada and the European Union*, Master's thesis, Toronto, University of Toronto, 2004

NADEAU, A. and R. NADEAU, *Traité pratique de la responsabilité civile*, Montreal, Wilson et Lafleur, 1971, no. 201

ODELL, D., *Pro JavaScript RIA Techniques: Best Practices, Performance, and Presentation*, Berkeley, Apress, 2009

PERDUE, D. J., *Social Media Marketing: Gaining a Competitive Advantage by Reaching the Masses*, Virginia, Center for Computer and Information Technology, Liberty University, 2010

PINEAU, J. and M. OUELLETTE-LAUZON, *Théorie de la responsabilité civile*, 2nd ed., Montreal, Éditions Thémis, 1980

PINET, M., *Le Droit de la concurrence déloyale en droit prive québécois*, Master's thesis, Ottawa, l'École des études supérieures, University of Ottawa, 1989

REBOUL, P. and D. XARDEL, *Le Commerce électronique: Techniques et Enjeux*, Paris, Éditions Eyrolles, 1997

RISSOAN, R., *Les réseaux sociaux – Facebook, Twitter, LinkedIn, Viadeo, Google+: Comprendre et maîtriser ces nouveaux outils de communication*, St-Herblain, Éditions ENI, 2011

ROGNERUD, J., *Ultimate Guide to Search Engine Optimization: Drive Traffic, Boost Conversion Rates and Make Tons of Money*, 2nd ed., Irvine, Entrepreneur Press, 2011

ROUBIER, P., *Le droit de la propriété industrielle*, t. 1, Paris, Librairie du Recueil Sirey, 1952

SCASSA, T. and M. DETURBIDE, *Electronic Commerce and Internet Law in Canada*, Ontario, CCH Canadian Limited, 2004

SHERSON, G. W., *Internet Marketing and Society*, Master's thesis, Wellington, Faculty of Commerce and Administration, Victoria University of Wellington, 2000

SOLOVE, D. J., *The Digital Person: Technology and Privacy in the Information Age*, New York, New York University Press, 2004

STROUT, A. and M. SCHNEIDER, *Location Based Marketing for Dummies*, Hoboken, John Wiley & Sons, 2011

TRUDEL, P., F. ABRAN, K. BENYEKHLEF and S. HEIN, *Droit du cyberespace*, Montreal, Éditions Thémis, 1997

TRUDEL, P., *Introduction à la Loi concernant le cadre juridique des technologies de l'information*, Cowansville, Éditions Yvon Blais, 2012

ULMER, E., *La répression de la concurrence déloyale dans les états membres de la Communauté Économique Européenne*, t. 1, Paris, Dalloz, 1967

VICENTE, A. I., "La convergence de la sécurité informatique et de la protection des renseignements personnels : Vers une nouvelle approche juridique", 2003, p. 9, online : <http://www.lex-electronica.org/docs/articles_114.pdf> (site consulted on October 18, 2012)

WESTIN, A. F., *Privacy and Freedom*, New York, Athenum, 1967

YIN, H., *Web Search Context Management Using Javascript/Cookie and JSP/Database Technologies*, Master's thesis, Auburn, Faculty of Computer Science and Software Engineering, Auburn University, 2011

ZUZE, H., *The Crossover Point Between Keyword Rich Website Text and Spamdexing*, Master's thesis, Cape Town, Faculty of Business, Cape Peninsula University of Technology, 2011

Journal Articles and Studies From Collective Works

ALBERT, M. A. and R. L. BOCCHINO JR., "Trade Libel: Theory and Practice Under the Common Law, The Lanham Act, and the First Amendment", (1999) 89 *Trademark Rep.* 826

BAIN, H. R. R., "The Law Affecting Comparative Advertising", (1974) 32 *U. Toronto Fac. L. Rev.* 109

BAUDOUIN, J.-L., "Le parasitisme", (2001) 31 R.G.D. 789

BENYEKHLEF, K., "Les dimensions constitutionnelles du droit à la vie privée", in P. TRUDEL and F. ABRAN (dir.), *Droit du public à l'information et vie privée. Deux droits irréconciliables?*, Montreal, Éditions Thémis, 1992

BLOUSTEIN, E. J., "Privacy Is Dear at Any Price: A Response to Professor Posner's Economic Theory", (1978) 12 *Ga. L. Rev.* 429, 445

BOYD, D. M. and N. B. ELLISON, "Social Network Sites: Definition, History, and Scholarship", (2008) 13 *Journal of Computer-Mediated Communication* 210

BRESLIN, J. and S. DECKER, "The Future of Social Networks on the Internet: The Need for Semantics", (2007) 11-6 *IEEE Internet Computing* 86

BRUN, B., "Le blogue : un équilibre délicat entre communication et responsabilité", in *Leg@l.TI, droit et technologies de l'information : devenir aujourd'hui l'avocat de demain*, Cowansville, Éditions Yvon Blais, 2007, 73

CAMIRAND, C., "Concurrence déloyale, les règles d'application de la responsabilité civile en matière d'imitation de marque de commerce", (1989) 4 R.J.E.U.L. 3

CANNON, A. W., "Regulating AdWords: Consumer Protection in a Market Where the Commodity is Speech", (2009) 39-1 *Seton Hall Law Review* 291

CARBONNEAU, L., "La concurrence déloyale au secours de la propriété intellectuelle" in Service de la formation permanent, Barreau du Québec, *Développements récents en droit de la propriété intellectuelle*, Cowansville, Éditions Yvon Blais, 1995

CHANG, E. W., "Bidding on Trespass: *eBay, Inc. v. Bidder's Edge, Inc.* and the Abuse of Trespass Theory in Cyberspace-Law", (2001) 29-4 *AIPLA Quarterly Journal* 445

CHANG, H. P., "Return to Confusion: Call for Abandonment of the Initial Interest Confusion Doctrine", (2008) 12 *Intell. Prop. L. Bull.* 131

CHEN G. and F. RAHMAN, "Analyzing privacy designs of mobile social networking applications", in *Proceedings of the IEEE/IFIP International Symposium on Trust, Security and Privacy for Pervasive Applications (TSP)*, Shanghai, China, 2008, 83

CHING, W., R. J. TEH, B. LI, C. RIZOS, "Uniwide WiFi Based Positioning System", *IEEE International Symposium on Technology and Society*, Shanghai, China, 2010, 180

CIARLONE JR., T. G. and E. W. WIECHMANN, "Cybersmear May Be Coming to a Website Near You: A Primer for Corporate Victims", (2003) 70 *Def. Counsel J.* 51

CLEFF, E. B., "Mobile advertising regulation: Implementing the legal criteria of meaningful consent in the concept of mobile advertising", (2007) 23 *Computer Law & Security Report* 262

EDMUNDSON, K. E., "Global Position System Implants: Must Consumer Privacy Be Lost in order for People to Be Found?", (2005) 38 *Ind. L. Rev.* 207

FEASBY, J. T., "Who Was That Masked Man? Online Defamation, Freedom of Expression, and the Right to Speak Anonymously", (2002) 1-1 *C.J.L.T*, online: <http://cjlt.dal.ca/vol1_no1/articles/01_01_Feasby_defam.pdf> (site consulted on January 20, 2011)

FLAHERTY, D. H., "On the Utility of Constitutional Rights to Privacy and Data Protection", (1991) 41 *Case Western Reserve Law Review* 831

FREEDMAN, B. J. and R. J.C. DEANE, "Trade-marks on the Internet: A Canadian Perspective" (2001) 34 *U.B.C.L. Rev.* 345

FREEMAN, E. H., "Wardriving: Unauthorized Access to Wi-Fi Networks", (2006) 15-1 *Information Systems Security* 11

GAVISON, R., "Privacy and the Limits of Law", (1980) 89-3 *The Yale Law Journal* 421

GOUDREAU, M., "Concurrence déloyale en droit prive – commentaires d'arrêts", (1984) 15 *R.G.D.* 133

GRATTON, E., "M-commerce: The Notion of Consumer Consent in Receiving Location-Based Advertising", (2002) 1-2 *C.J.L.T.* 59

GRIMMELMANN, J., "The Structure of Search Engine Law", (2007) 93 *Iowa Law Review* 1;

GUAY, F., "Canada", in CENTER FOR INTERNATIONAL LEGAL STUDIES (dir.), *Unfair Trading Practices*, London, Kluwer Law International, 1996, 59

HARDING, W. T., A. J. REED and R. L. GRAY, "Cookies and Web Bugs: What They Are and How They Work Together", in Harold F. TIPTON and Micki KRAUSE (dir.),

Information Security Management Handbook, 6th ed., vol. 1, Boca Raton, Auerback Publications, 2007, 2133

HARTMANN, C. J. and S. M. RENAS, "Anglo-American Privacy Law: An Economic Analysis", (1985) 5 *International Review of Law and Economics* 133

HASHEMI, Y., "Note – Facebook's Privacy Policy and its Third-Party Partnerships : Lucrativity and Liability", (2009) 15 *B. U. J. Sci. & Tech. L.* 140

HAYTHORNTHWAITE, C., "Social Networks and Internet Connectivity Effects", (2005) 8-2 *Information, Communication & Society* 125

HOEDL, C., "How to Market Services: Advertising Consumer Protection and Personal Data", (1998) 3 *Int'l Bus. L.J.* 285

HUI, K.-L., H. H. TEO and S.-Y. T. LEE, "The Value of Privacy Assurance: An Exploratory Field Experiment", (2007) 31-1 *MIS Quarterly* 19, 26

JACOBY, J. and M. SABLEMAN, "Keyword-Based Advertising: Filling in Factual Voids (*GEICO v. Google*)", (2007) 97-3 *Trademark Rep.* 681

JORDAN, E. R. and P. H. RUBIN, "An Economic Analysis of the Law of False Advertising", (1979) 8 *J. Legal Stud.* 527

JUELS, A., "Targeted Advertising…And Privacy Too", in David NACCACHE (dir.), *Topics in Cryptology: The Cryptographers' Track at the RSA Conference 2001*, Berlin, Springer, 2001, 408

KANG, J., "Information Privacy in Cyberspace Transactions", (1998) 50 *Stanford Law Review* 1193, 1218-1219

KATYAL, N. K., "The Dark Side of Private Ordering: The Network/Community Harm of Crime", in M. F. GRADY and F. PARISI (dir.), *The Law and Economics of Cybersecurity*, New York, Cambridge University Press, 2006, 193

KEEN, P. C., "Anonymity and the Supreme Court's Model of Expression: How Should Anonymity be Analyzed Under Section 2(b) of the Charter?", (2005) 2-3 *C.J.L.T* 167

KIM, W., O.-R. JEONG and S.-W. LEE, "On Social Web Sites", (2010) 35-2 *Information Systems Journal* 215

KING, N. J., "Direct Marketing, Mobile Phones, and Consumer Privacy: Ensuring Adequate Disclosure and Consent Mechanisms for Emerging Mobile Advertising Practices", (2007) 60-2 *Federal Communications Law Journal* 239

KING, S., "The Law That It Deems Applicable: ICANN, Dispute Resolution, and the Problem of Cybersquatting", (1999-2000) 22 *Hastings Comm. & Ent. L.J.* 453

KUESTER, J. R. and P. A. NIEVES, "Hyperlinks, Frames and Metatags: An Intellectual Property Analysis", (1997) 38 *I.D.E.A.* 243

LADOUCEUR, N., "Calibrating the Electronic Scales: Tipping the Balance in Favour of a Vigorous and Competitive Electronic Market for Consumers", (1999) 25 *Can.-U.S. L.J.* 295

LANDES, W. M. and R. A. POSNER, "Trademark Law: An Economic Perspective", (1987) 30 *Journal of Law and Economics* 265

LIN, D. and M. C. LOUI, "Taking the Byte Out of Cookies: Privacy, Consent and the Web", (1998) *Computers and Society* 39

LOCKWOOD, S., "Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators", (2004) 18 *Harv. J. L. & Tech.* 307

MACDONALD, J. "Electronic Trespass in Canada: The Protection of Private Property on the Internet", (2006) 5-3 *C.J.L.T.* 163

MAGGS, G. E., "Internet Solutions to Consumer Protection Problems", (1997) 49 *S. C. L. Rev.* 887

MALAGA, R., "Worst Practices in Search Engine Optimization", (2008) 51-12 *Communications of the ACM* 147

MARTIN, S. and M. THIBAULT, "Le droit de la concurrence déloyale, substitut du droit d'auteur", in ALAI CANADA (dir.), *Un cocktail de droit d'auteur / A Copyright Cocktail*, Montreal, Éditions Thémis, 2007, 247

MCADAMS, R. H., "The Origin, Development and Regulation of Norms", (1997) 96 *Mich. L Rev.* 338,419-424

MCCARTHY, J. T., "Trademarks, Cybersquatters and Domain Names", (1999-2000) 10 *DePaul-LCA J. Art & Ent. L.* 231

MIDDLEBROOK, S. and J. MULLER, "Thoughts on Bots: The Emerging Law of Electronic Agents", (2000) 56 *Bus. Law.* 341

MILNE, G. R. and M. J. CULNAN, "Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices", (2004) 18-3 *Journal of Interactive Marketing* 15

MOSKIN, J., "Virtual Trademark Use – The Parallel World of Keyword Ads", (2008) 98-3 *Trademark Rep.* 873

NELSON ENG, R., "A Likelihood of Infringement: The Purchase and Sale of Trademarks as Adwords", (2009) 18-2 *Alb. L.J. Sci. & Tech* 493

NOTE: "Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators", (2004) 18-1 *Harv. J.L. & Tech.* 307

O'ROURKE, M. A., "Property Rights and Competition on the Internet: In Search of an Appropriate Analogy", (2001) 16 *Berkeley Tech. L.J.* 561

OHM, P., "The Rise and Fall of Invasive ISP Surveillance", (2009) 5 *University of Illinois Law Review* 1417

OSBORN NG, H., "Targeting Bad Behavior: Why Federal Regulators Must Treat Online Behavioral Marketing as Spyware", (2009) 31 *Hastings Comm. & Ent. L.J.* 369, 371

OTTENBERG, A. A., "GPS Tracking Technology: The Case for Revisiting Knotts and Shifting the Supreme Court's Theory of the Public Space Under the Fourth Amendment", (2004) 46-3 *B. C. L. Rev.* 661

PASQUALE, F., "Rankings, Reductionism and Responsibility", (2006) 54 *Cleveland St. L. Rev.* 115

PELLETIER, B., "La protection de la vie privée au Canada", (2001) 35 *R.J.T.* 485

PERSON, A. N., "Behavioral Advertisement Regulation: How the Negative Perception of Deep Packet Inspection Technology May be Limiting the Online Experience", (2010) 62-2 *Federal Communications Law Journal* 435

PFEFFERKORN, R., "Liability for Search Engine Triggering of Trademarked Keywords after Rescuecom", (2008) 5 *Shidler J.L. Com. & Tech.* 2

PHILLIPS, G. D., "Necessary Protection for Famous Trademark Holders on the Internet", (1998-1999) 21 *Hastings Comm. & Ent. L.J.* 635

POITRAS, D. and L. DESBIENS, "Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et Loi sur la protection des renseignements personnels dans le secteur privé, textes annotés", S.O.Q.U.I.J., 1996

POSNER, R. A., "John A. Sibley Lecture: The Right of Privacy", (1978) 12-3 *Georgia Law Review* 393

POSNER, R. A., "The 1978 James McCormick Mitchell Lecture: Privacy, Secrecy, and Reputation", (1978) 28 *Buffalo Law Review* 1

QUILTER, L., "The Continuing Expansion of Cyberspace Trespass to Chattels", (2002) 17 *Berkeley Technology Law Journal* 421

RAMOS, A., "Deep Packet Inspection Technologies", in H. F. TIPTON and M. KRAUSE (dir.), *Information Security Management Handbook*, 6th ed., vol. 3, New York, Auerbach Publications, 2009, 2195

RAYNAL, F. and F. GASPARD, "Small treatise about e-manipulation for honest people", (2010) 6-2 *Journal in Computer Virology* 143

ROHANI, V. A. and O. S. HOCK, "On Social Network Web Sites: Definition, Features, Architectures and Analysis Tools", (2010) 2 *Journal of Advances in Computer Research* 41

ROSEMANN, M., M. ROCHEFORT and W. BEHNCK, "Customer Relationship Management" (our translation), (1999) 36-208 *HMD-Praxis der Wirtschaftsinformatik* 105

ROSSI, J. A., "Protection for Trademark owners: The Ultimate System of Regulating Search Engine Results", (2001) 42 *Santa Clara L. Rev.* 295, 321;

RUSTAD, M. L. and T. H. KOENIG, "Cybertorts and Legal Lag: An Empirical Analysis", (2003) 13 *S. Cal. Interdisc. L.J.* 77

SAINT-GAL, Y., "Concurrence déloyale et concurrence parasitaire ou agissements parasitaires", (1956) 25-26 *Revue internationale de la propriété industrielle et artistique* 19

SAUNDERS, K. M., "Confusion is the Key: A Trademark Law Analysis of Keyword Banner Advertising", (2002) 71 *Fordham Law Review* 543

SCASSA, T., "Information Privacy in Public Space: Location Data, Data Protection and the Reasonable Expectation of Privacy", (2009) 7-2 *C.J.L.T.* 193

SCHWARTZ, P. M., "Internet Privacy and the State", (1999-2000) 32 *Conn. L. Rev.* 815, 840

SEN, R., "Optimal Search Engine Marketing Strategy", (2005) 10-1 *International Journal of Electronic Commerce* 9

SHEA, G., "Trademarks and Keyword Banner Advertising", (2002) 75 *Southern California Law Review* 529

SIEBECKER, M. R., "Cookies and the Common Law: Are Internet Advertisers Trespassing on Our Computers?", (2003) 76 *Southern California Law Review* 893

SIMSOVIC, D. J., "i-advertising: the ways and the means", in Vincent GAUTRAIS (dir.), *Droit du commerce électronique*, 395

SINGH, T., L. VERON-JACKSON and J. CULLINANE, "Blogging: A New Play in Your Marketing Game Plan", (2008) 51 *Business Horizons* 281

SPULBER, D. F., "The Map of Commerce: Internet Search, Competition, and the Circular Flow of Information", (2009) 5-4 *Journal of Competition Law and Economics* 633

TAN, A., "Google Adwords: Trademark Infringer or Trade Liberalizer?", (2010) 16 *Michigan Telecommunications and Technology Law Review* 473

TAUBNER, R. W., "Google AdWords and Canadian Trademark Law", (2010) 7-2 *C.J.L.T.* 289;

VILLOCH III, A., "Europe's Mobile Opportunity: Can the European Union Legislate Consumer Trust and Compete in the E-Commerce Market with the United States?", (2002) 20 *Penn. St. Int'l L. Rev.* 439

VON ARX, K., "LitOral: A New Form of Defamation Consciousness", (2002) 1-2 *C.J.L.T* 63

WAITE, D., "Consumer Protection Issues in Internet Commerce", (1999) 32 *Can. Bus. L.J.* 132

WALLER, S. W., "In Search of Economic Justice: Considering Competition and Consumer Protection Law", (2004) 36 *Loy. U. Chi. L.J.* 631

WERBACH, K., "Breaking the Ice: Rethinking Telecommunications Law for the Digital Age", (2005) 4 *J . Telecomm. & High Tech. L.* 59

WINN, H., "Internet Marketing: Using New Forms of Internet Media to Market to Today's Generation", (2010) 8 *Liberty Business Review* 11

ZECK, K., "Referential Fair Use & Keyword advertising: The Necessity of Product Placement to our Domestic System of Free-Market Enterprise, (2008) 44-3 *Gonzaga Law Review* 519

ZIMMERMAN, R. K., "The Way the "Cookies" Crumble: Internet Privacy and Data Protection in the Twenty-First Century", (2000-2001) 4 *Legislation and Public Policy* 439

Electronic Articles

ABOUT.COM, "Packet", 2012, online: <http://compnetworking.about.com/od/networkprotocols/l/bldef_packet.htm> (site consulted on November 7, 2012)

ANDERSON, N., ".06% Opt Out: NebuAd hides link in 5,000-word Privacy Policy", July 24, 2008, online: <http://arstechnica.com/old/content/2008/07/06-opt-out-nebuad-hides-link-in-5000-word-privacy-policy.ars> (site consulted on February 20, 2012)

ANDERSON, N., "Deep packet inspections meets 'Net neutrality, CALEA", July 26, 2007, online: <http://arstechnica.com/hardware/news/2007/07/Deep-packet-inspection-meets-net-neutrality.ars> (site consulted on January 20, 2012)

ANDERSON, N., "NebuAd loses CEO, business model in wake of tracking furor", September 5, 2008, online: http://arstechnica.com/techpolicy/news/2008/09/nebuad-loses-ceo-business-model-in-wake-of-tracking-furor.ars (site consulted on October 23, 2012)

APPLE, "iOS: Safari web settings", October 12, 2011, online: <http://support.apple.com/kb/HT1677> (site consulted on September 2, 2012);

ARGENTON, C. and J. PRÜFER, "Search Engine Competition with Network Externalities", April 11, 2011, online: <http://www.tilburguniversity.edu/webwijs/files/center/prufer/search_engines.pdf> (site consulted on January 25, 2012)

ATHEY, S. and J. S. GANS, "The Impact of Targeted Technology on Advertising Markets and Media Competition", January 11, 2009, online: <http://works.bepress.com/joshuagans/39/> (site consulted on June 4, 2011)

BENDRATH, R. and M. MUELLER, "The End of the Net as we know it? Deep Packet Inspection and Internet Governance", August 4, 2010, online: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1653259> (site consulted on September 7, 2012)

BENDRATH, R., "Global technology trends and national regulation: Explaining Variation in the Governance of Deep Packet Inspection", February 2009, online: http://userpage.fu-berlin.de/bendrath/ISA09_Paper_Ralf%20Bendrath_DPI.pdf> (site consulted on September 6, 2012)

BEYE, M., A. JECKMANS, Z. ERKIN, P. HARTEL, R. LAGENDIJK and Q. TANG, "Literature Overview - Privacy in Online Social Networks", 2010, online: <http://doc.utwente.nl/74094/1/literaturereview.pdf> (site consulted on January 29, 2012)

BONNEAU, J., F. STAJANO, J. ANDERSON and R. ANDERSON, "Eight Friends Are Enough: Social Graph Approximation via Public Listings", 2009, online: <http://www.cl.cam.ac.uk/~jcb82/doc/BASA09-SNS-eight_friends.pdf> (site consulted on January 29, 2012)

CAMERON, A., "Facebook, Streetview, and What's Next: Navigating Your Way Through New Issues in Privacy Law", April 23, 2010, online: <http://www.fasken.com/files/Publication/78b5cf7e-31cf-4654-b6a0-5fd2adea69fb/Presentation/PublicationAttachment/9d6f81cb-f178-4bc3-b302-5fd4b4c87e63/Alex_Cameron_LSUC_2010_Paper.pdf> (site consulted on February 20, 2012)

CAMERON, K. and A. CAVOUKIAN, "Wi-Fi Positioning Systems: Beware of Unintended Consequences Issues Involving Unforeseen uses of pre-existing Architecture", June 2011, online: <http://www.ipc.on.ca/images/Resources/wi-fi.pdf> (site consulted on January 20, 2012)

CANADIAN RADIO-TELEVISION AND TELECOMMUNICATIONS COMMISSION, "Telecom Regulatory Policy CRTC 2009-657: Review of the Internet traffic management practices of Internet service providers", October 21, 2009, online: <http://www.crtc.gc.ca/eng/archive/2009/2009-657.htm> (site consulted on February 18, 2012)

CARON, D., "Privacy, Social Networking Sites, and the Canadian Approach: Protecting a Pluralistic Conception of Privacy Through Principle-Based Regulation", May 20, 2010, online: <http://www.priv.gc.ca/speech/2010/sp-d_20100520_dc_e.cfm> (site consulted on August 8, 2011)

CAVOUKIAN, A. and M. GURSKI, "Privacy in a wireless world", January 1, 2002, online: <http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=334> (site consulted on March 21, 2002)

CBC NEWS, "Facebook use drops in Canada, U.S.", June 13, 2011, online: <http://www.cbc.ca/news/technology/story/2011/06/13/facebook-users-drop.html> (site consulted on January 20, 2012)

CHAABANE, A., M. A. KAAFAR and R. BORELI, "Big Friend is Watching You: Analyzing Online Social Networks Tracking Capability", August 17, 2012, online: <http://conferences.sigcomm.org/sigcomm/2012/paper/wosn/p7.pdf> (site consulted on September 7, 2012)

CHASSIGNEUX, C., "La protection des informations à caractère personnel", in Eric LABBÉ, Daniel POULIN, François JACQUOT and Jean-François BOURQUE (dir.), *Le guide juridique du commerçant électronique*, online : <http://www.jurisint.org/pub/05/fr/guide_final.pdf> (site consulted on March 21, 2012)

CHAUDHARY, A., "Nimbuzz to Offer Location Based Advertising On Mobile App", April 20, 2012, online: <http://www.medianama.com/2012/04/223-nimbuzz-location-based-ads/> (site consulted on October 23, 2012)

CHIANG, O., "Twitter Hits Nearly 200M Accounts, 110M Tweets Per Day, Focuses On Global Expansion", January 19, 2011, online: <http://www.forbes.com/sites/oliverchiang/2011/01/19/twitter-hits-nearly-200m-

users-110m-tweets-per-day-focuses-on-global-expansion/> (site consulted on January 20, 2012)

CITRON, D. K., "The Privacy Implications of Deep Packet Inspection", online: http://dpi.priv.gc.ca/index.php/essays/the-privacy-implications-of-deep-packet-inspection/> (site consulted on September 6, 2012)

CLAYTON, R., "The Phorm "Webwise" System", May 18, 2008, online: <http://www.cl.cam.ac.uk/~rnc1/080518-phorm.pdf> (site consulted on October 22, 2012)

CNN.COM, "Google blacklists BMW Web site", February 7, 2006, online: <http://www.cnn.com/2006/BUSINESS/02/07/google/> (site consulted on October 25, 2012)

COMPETITION BUREAU CANADA, "Enforcement Guidelines: Application of the *Competition Act* to Representations on the Internet", October 2009, online: <http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/vwapj/RepresentationsInternet2009-10-16-e.pdf/$FILE/RepresentationsInternet2009-10-16-e.pdf> (site consulted on April 16, 2012)

COMPETITION BUREAU CANADA, "How to File a Complaint", December 30, 2011, online: <http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/h_00130.html> (site consulted on: August 21, 2012)

COMPETITION BUREAU CANADA, "Information Bulletin, Misleading Representations and Deceptive Marketing Practices: Choice of Criminal or Civil Track Under the Competition Act", September 20, 1999, online: <http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/vwapj/ct01181e.pdf/$file/ct01181e.pdf> (site consulted on August 22, 2012)

CONSTANDACHE, I., R. R. CHOUDHURY and I. RHEE, "Towards Mobile Phone Localization without War-Driving", online: <http://synrg.ee.duke.edu/papers/compAcc.pdf> (site consulted on September 8, 2012)

CONSTINE, J., "Facebook Celebrates the Like Button's 1st Birthday By Showing Off Its Footprint", April 21, 2011, online:

<http://www.insidefacebook.com/2011/04/21/like-button-birthday/> (site consulted on January 29, 2012)

CONSTINE, J., "Facebook Says "Likers" Click Links To External Websites 5.4x More", September 29, 2010, online: <http://www.insidefacebook.com/2010/09/29/facebook-stats-likers/> (site consulted on January 20, 2012)

CORPEL, A. and M. LEMERCIER, "Traces numériques des smartphones: De l'investigation à la protection de la vie privée", 2001, online : <http://www.lifl.fr/ict/fichiers/1.pdf> (site consulted on September 7, 2012)

CULNAN, M. J., *Self-Regulation on the Electronic Frontier: Implications for Public Policy*, *in* National Telecomms. & Info. Admin., U.S. Dep't of Commerce, Privacy and Self-Regulation in the Information Age, ch. 1, § F (1997), online: <http://www.ntia.doc.gov/page/chapter-1-theory-markets-and-privacy#1F> (site consulted on October 31, 2012)

DAILY RESEARCH NEWS ONLINE, "Phorm Approaches 'Defining Moment'", October 1, 2012, online: <http://www.mrweb.com/drno/news16166.htm> (site consulted on October 22, 2012)

DALY, A., "The Legality of Deep Packet Inspection, June 17, 2010, online: <http://ssrn.com/abstract=1628024 or doi:10.2139/ssrn.1628024> (site consulted on January 19, 2012)

DAVIS, W., "Case Close: NebuAd Shuts Down", May 18, 2009, online: <http://www.mediapost.com/publications/article/106277/> (site consulted on October 23, 2012)

DAVIS, W., "NebuAd Settles Lawsuit Over Behavioral Targeting Tests", August 16, 2011, online <http://www.mediapost.com/publications/article/155980/> (site consulted on October 23, 2012)

DELWAIDE, K. and A. AYLWIN, "Learning From a Decade of Experience: Quebec's Private Sector Privacy Act", 2005, online: <http://www.priv.gc.ca/information/pub/dec_050816_e.pdf> (site consulted on March 17, 2012)

DEVILLARD, A., "Affaire Phorm: Bruxelles demande des comptes au Royaume-Uni, La Commission européenne a ouvert une procédure d'infraction, à l'origine de laquelle se trouve une technologie de ciblage comportemental appelée Phorm", April 15, 2009, online: <http://www.01net.com/editorial/501173/affaire-phorm-bruxelles-demande-des-comptes-au-royaume-uni/> (site consulted on October 22, 2012)

DUGGAN, M., and J. DEVENEY, "How to Make Internet Marketing Simple", 2003, online: <http://www.deveney.com/public/userfiles/5_internet20marketing2.pdf> (site consulted on January 23, 2012)

EDRI-GRAM, "UK: Phorm Targeted Advertising Practices – Under Pressure", March 26, 2008, online: <http://www.edri.org/edrigram/number6.6/phorm-uk-ifpr> (site consulted on October 22, 2012)

EFRAIT, A., "Google Penalizes Overstock for Search Tactics", February 24, 2011, online: <http://searchenginewatch.com/article/2049969/Overstock.com-Lands-in-Googles-Penalty-Box-Over-Links-for-Discounts-Deal> (site consulted on October 25, 2012)

EICHELBERGER, L., "The Cookie Controversy: Cookies and Internet Privacy", online: <http://www.cookiecentral.com/ccstory/cc3.htm> (site consulted on September 6, 2012)

EMARKETER, "New Ways to Target Your Customer", April 20, 2006, online: <http://www.emarketer.com/Article.aspx?id=1003937&R=1003937> (site consulted on September 9, 2012)

ENGE, E., "11 Guidelines for getting Authoritative Links", February 23, 2007, online: <http://searchenginewatch.com/article/2056780/11-Guidelines-for-Getting-Authoritative-Links> (site consulted on October 27, 2012)

ERNESTAD, V. and R. HENRIKSSON, "Social media marketing from a bottom-up perspective – the social media transition", online: <http://umu.diva-portal.org/smash/get/diva2:325207/FULLTEXT01> (site consulted on January 21, 2012)

ESTEVES, J., "France Vichy Cosmetics: Blog or Not To Blog?", May 9, 2008, online: <http://openmultimedia.ie.edu/openproducts/vichy_i/vichy_i/pdf/teaching_case_vichy.pdf> (site consulted on August 25, 2012)

EUROPEAN UNION, "Telecom: Commission launches case against UK over privacy and personal data protection", April 14, 2009, online: <http://europa.eu/rapid/press-release_IP-09-570_en.htm?locale=en.> (site consulted on October 22, 2012)

FACEBOOK DEVELOPERS, "Like Button", 2012, online: <http://developers.facebook.com/docs/reference/plugins/like/> (site consulted on September 7, 2012)

FACEBOOK DEVELOPERS, "Social Plugins", 2012, online: <http://developers.facebook.com/docs/plugins/> (site consulted on September 10, 2012);

FEDERAL TRADE COMMISSION, "FTC Staff Revises Online Behavioral Advertising Principles", February 2009, online: <http://www.ftc.gov/opa/2009/02/behavad.shtm> (site consulted on September 9, 2012)

FEDERAL TRADE COMMISSION, "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers", December 2010, online: <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf> (site consulted on January 20, 2011)

FEDERAL TRADE COMMISSION, BUREAU OF CONSUMER PROTECTION, "Online Profiling: A Report to Congress", 2000, online: <http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf> (site consulted on November 25, 2011).

FOURSQUARE BLOG, "The real world, now in real-time! Say hi to foursquare Radar!", October 12, 2011, online: <http://blog.foursquare.com/2011/10/12/the-real-world-now-in-real-time-say-hi-to-foursquare-radar/> (site consulted on October 24, 2012).

FROSCH-WILKE, D., "Are E-Privacy and E-Commerce a Contradiction in Terms? – An Economic Examination", (2001), online: <http://www.informingscience.org/proceedings/IS2001Proceedings/pdf/FroschWilkeEBKAreEP.pdf> (site consulted on October 29, 2012)

GABE, G., "The Long Tail of SEO, How Long Tail Keywords Impact Natural Search Traffic, Bounce Rate and Conversion",

<http://www.hmtweb.com/blog/2008/08/long-tail-of-seo-how-long-tail-keywords.html> (site consulted on January 23, 2012)

GAUTRAIS, V., "Introduction générale : Le défi de la protection de la vie privée face aux besoins de circulation de l'information personnelle", June 5, 2003, online : <http://www.lex-electronica.org/docs/articles_107.pdf> (site consulted on March 22, 2012)

GIGAOM, "Survey: Percentage of users saying they opt out of targeted ads has nearly doubled", July 16, 2012, online: <http://gigaom.com/2012/07/16/percentage-of-users-saying-they-opt-out-of-targeted-ads-has-nearly-doubled-survey/> (site consulted on November 1, 2012)

GINGRAS, M., "Quand *Big Brother* fait du pouce sur l'inforoute", 1997, online: <http://commposite.org/index.php/revue/article/view/109/87> (site consulted on March 18, 2012)

GOGOI, P., "Wal-Mart's Jim and Laura: The Real Story", October 9, 2006, online: <http://www.businessweek.com/stories/2006-10-09/wal-marts-jim-and-laura-the-real-storybusinessweek-business-news-stock-market-and-financial-advice> (site consulted on August 27, 2012)

GOLDMAN, J., Z. HUDSON, and R. M. SMITH, "Privacy: Report on the Privacy Policies and Practices of Health Web Sites", January 2000, online: <http://www.chcf.org/~/media/MEDIA%20LIBRARY%20Files/PDF/P/PDF%20privacyexecsummary.pdf> (site consulted on September 5, 2012)

GOODWIN, D., "Overstock.com Lands in Google's Penalty Box Over Links-for-Discounts Deal", February 24, 2011, online <http://searchenginewatch.com/article/2049969/Overstock.com-Lands-in-Googles-Penalty-Box-Over-Links-for-Discounts-Deal> (site consulted on October 25, 2012)

GOOGLE, "AdWords Trademark Policy", 2012, online: <http://support.google.com/adwordspolicy/bin/answer.py?hl=en&answer=6118> (site consulted on October 18, 2012)

GOOGLE, "Choose an ad format", December 21, 2011, online: <http://support.google.com/adwords/bin/answer.py?hl=en&answer=1722124&topic=1713898&ctx=topic> (site consulted on January 23, 2012)

GOOGLE, "Duplicate Content", November 17, 2011, online: <http://support.google.com/webmasters/bin/answer.py?hl=en&answer=66359> (site consulted on January 23, 2012)

GOOGLE, "What are AdChoices?", 2012, online: <http://support.google.com/adsense/bin/static.py?hl=en&gl=CA&client=ca-pub-9310224305865624&ts=1631343&page=ts.cs&adU=www.crea-med.ca&rd=3&contact=abg_afc&url=http:%2F%2Fwww.listchallenges.com%2F100places%2FCompare%2F&adT=Private+Doctors> (site consulted on March 17, 2012)

Graeme MCMILLAN, "Google blacklists sites run by a family of British politician", September 7, 2012, online: <http://www.digitaltrends.com/web/google-blacklists-sites-run-by-family-of-british-politician/> (site consulted on October 24, 2012)

GROSS, G., "Senators Question NebuAd, Targeted Ad Privacy", July 9, 2008, online: <http://www.pcworld.com/businesscenter/article/148136/senators_question_nebuad_targeted_ad_privacy.html> (site consulted on January 20, 2012)

HA, A., "JiWire Aims to Improve Mobile Ad Targeting With Its New Location Graph", August 14, 2012, online: <http://techcrunch.com/2012/08/14/jiwire-location-graph/> (site consulted on October 24, 2012)

HALL, E., "U.K.'s o2 Works With Marks & Spencer, Starbucks, L'Oreal on Location-Based Marketing: Mobile Phone Operators Text Marketers' Deals to Customers; Orange Will Be Next to Add Service", (January 20, 2011, online: <http://adage.com/article/global-news/02-location-based-marketing-m-s-starbucks-l-oreal/148343/> (site consulted on October 18, 2012); Sarah Shearman, prev. cited, note 164

HALLIDAY, J., "Facebook paid PR firm to smear Google", May 12, 2011, online: <http://www.guardian.co.uk/technology/2011/may/12/facebook-pr-firm-google> (site consulted on August 27, 2012)

HANSELL, S., "NebuAd Observes 'Useful, but Innocuous' Web Browsing", April 7, 2008, online: <http://bits.blogs.nytimes.com/2008/04/07/nebuad-observes-useful-but-innocuous-web-browsing/> (site consulted on January 20, 2012)

HARLAN, C., "China pushing back against online smear campaigns", January 27, 2011, online: <http://www.washingtonpost.com/business/china-pushing-back-against-online-smear-campaigns/2011/01/27/ABMY93Q_story.html> (site consulted on January 25, 2012)

HEIDEMANN, J., M. KLIER and F. PROBST, "Identifying Key Users in Online Social Networks: A PageRank Based Approach", December 2010, online: <http://www.wi-if.de/paperliste/paper/wi-301.pdf> (site consulted on January 29, 2012)

HEPBURN, A., "Facebook Statistics, Stats & Facts for 2011", January 18, 2011, online: <http://www.digitalbuzzblog.com/facebook-statistics-stats-facts-2011/> (site consulted on January 20, 2012)

HEPBURN, A., "Facebook: Facts and Figures for 2010", March 22, 2010, online: <http://www.digitalbuzzblog.com/facebook-statistics-facts-figures-for-2010/> (site consulted on January 20, 2012)

HIGGINBOTHAM, S., "NebuAd Bites The Dust", May 19, 2009, online: <http://gigaom.com/2009/05/19/nebuad-bites-the-dust/> (site consulted on October 23, 2012)

HILLS, T., "Deep Packet Inspection", December 14, 2006, online: http://www.lightreading.com/document.asp?doc_id=111404> (site consulted on September 6, 2012)

HONG, J. I., G. BORIELLO, J. A. LANDAY, D. W. MCDONALD, B. N. SCHILIT and J. D. TYGAR, "Privacy and Security in the Location-enhanced World Wide Web", online: <http://www.seattle.intel-research.net/pubs/100220061021_335.pdf> (site consulted on September 8, 2012)

HOWARD, F. and O. KOMILI, "Poisoned search results: How hackers have automated search engine poisoning attacks to distribute malware", March 2010, online: <http://www.sophos.com/security/technical-papers/sophos-seo-insights.pdf> (site consulted on January 23, 2012)

HOWARD, J., "Wagging the Tail", July 20, 2006, online: <http://jonhoward.typepad.com/livingbrands/2006/07/wagging_the_tai.html> (site consulted on July 6, 2011)

HUBSPOT, "The 2011 State of Inbound Marketing", February 2011, online: <http://www.hubspot.com/Portals/53/docs/ebooks/the%20state%20of%20inbound%20marketing%20final%20v3-2.pdf> (site consulted on January 21, 2012)

INTERACTIVE ADVERTISING BUREAU, "Platform Status Report: User Generated Content, Social Media, and Advertising – An Overview", April 2008, online: <http://www.slideshare.net/AutomotiveSocial/2008-ugc-platform-2931455> (site consulted on January 21, 2012)

JAVA, A., T. FININ, X. SONG and B. TSENG, "Why We Twitter: Understanding Microblogging Usage and Communities", 2007, online: <http://ebiquity.umbc.edu/_file_directory_/papers/369.pdf> (site consulted on January 21, 2012)

JIWIRE, "JiWire's Location Graph: Because where you've been says more about you than the websites you visit", 2012, online: <http://www.jiwire.com/locationgraph> (site consulted on October 24, 2012)

JOHNSON, J. P., "Targeted Advertising and Advertising Avoidance", July 28, 2009, online: <http://www.econ.as.nyu.edu/docs/IO/12543/Johnson_20091027.pdf> (site consulted on November 24, 2011)

KAFFASH, J., "Wall's and O2 target ice cream ads around weather", August 9, 2012, online: <http://www.marketingweek.co.uk/news/walls-and-o2-target-ads-around-weather/4003193.article> (site consulted on October 23, 2012)

KAPLAN, P., "John Mackey panned Wild Oats on Web", July 12, 2007, online: <http://www.reuters.com/article/2007/07/12/us-wholefoods-ftc-idUSN1133440820070712> (site consulted on January 25, 2012)

KAPLOW, L. and S. SHAVELL, "Economic Analysis of Law", February 1999, online: <http://lsr.nellco.org/harvard_olin/251> (site consulted on February 20, 2012)

KARCH, M., "Don't Make 'Click Here' Links – Why Hyperlink Names Matter to Google", 2012, online:

<http://google.about.com/od/searchengineoptimization/qt/hyperlinkqt.htm> (site consulted on January 23, 2012)

KARCH, M., "How to Improve Your Website's Google Ranking", 2012, online: <http://google.about.com/od/searchengineoptimization/qt/improverank.htm> (site consulted on January 23, 2012)

KARCH, M., "What Is PageRank and How Do I Use It?", 2012, online: <http://google.about.com/od/searchengineoptimization/a/pagerankexplain.htm> (site consulted on January 23, 2012)

KARCH, M., "Why Titles Matter – How to Get More People to See Your Pages in Google", 2012, online: <http://google.about.com/od/searchengineoptimization/qt/titleseoqt.htm> (site consulted on January 23, 2012)

KRISHNAMURTHY, B. and C. E. WILLS, "On the Leakage of Personally Identifiable Information Via Online Social Networks", August 17, 2009, online: <http://www2.research.att.com/~bala/papers/wosn09.pdf> (site consulted on September 10, 2012)

KROTOSKI, A., "New Sony viral marketing ploy angers consumers: Sony has generated ire with another alleged viral marketing campaign posing as real Web 2.0", December 11, 2006, online: <http://www.guardian.co.uk/technology/gamesblog/2006/dec/11/newsonyviral> (site consulted on January 25, 2012)

LANDAU STEINMAN, M. and M. HAWKINS, "When Marketing Through Social Media, Legal Risks Can Go Viral", May 2010, online: <http://www.venable.com/files/Publication/b4f467b9-0666-4b36-b021-351540962d65/Presentation/PublicationAttachment/019f4e5f-d6f8-4eeb-af43-40a4323b9ff1/Social_Media_white_paper.pdf> (site consulted on September 9, 2012)

LEWIS, J., "Facebook personal tracking hits snag", November 28, 2011, online: <http://www.smh.com.au/technology/security/facebook-personal-tracking-hits-snag-20111127-1o1k6.html> (February 21, 2012)

LI, N. and G. CHEN, "Analysis of a Location-based Social Network", online: <http://rio.ecs.umass.edu/~lgao/ece697_10/Paper/LocationBasedSocialNetwork.pdf > (site consulted on January 20, 2012)

LO, J., "A 'Do Not Track List' for Canada?", December 3, 2009, online: <www.piac.ca/files/dntl_final_website.pdf> (site consulted on November 24, 2011)

LYONS, D., "Facebook Busted in Clumsy Smear on Google", May 11, 2011, online: <http://www.thedailybeast.com/articles/2011/05/12/facebook-busted-in-clumsy-smear-attempt-on-google.html> (site consulted on August 27, 2012)

MACLEAN, C., "Social Media Deception…Warning to Ad-Agencies and Clients", June 30, 2009, online: <http://clivemaclean.wordpress.com/2009/06/30/social-media-warning-to-ad-agencies-and-their-clients/> (site consulted on January 25, 2012)

MADDEN, M., "Privacy management on social media sites", February 24, 2012, online: <http://www.pewinternet.org/Reports/2012/Privacy-management-on-social-media/Summary-of-findings.aspx> (site consulted on November 8, 2012).

MANORS, G., "Phorm jumps after Turkey trial", October 16, 2012, online: <http://www.ifamagazine.com/news/phorm-jumps-after-turkey-trial/26159/> (site consulted on October 22, 2012)

MARTIN, K. E., "Facebook (A): Beacon and Privacy", <http://www.darden.virginia.edu/corporate-ethics/pdf/Facebook%20_A_business_ethics-case_bri-1006a.pdf> (site consulted on September 7, 2012)

MASSE, C., "La publicité trompeuse dans le commerce électronique", December 2000, online : <http://www.juriscom.net/uni/etd/06/pub01.pdf> (site consulted on : August 22, 2012)

MCENTEGART, J., "Facebook Hires PR Firm to Smear Google", May 12, 2011, online: <http://www.tomsguide.com/us/Facebook-Burson-Marsteller-Smear-Campaign-Anti-Google-Social-Circle,news-11171.html> (site consulted on August 27, 2012)

MCGEHEARTY, E., "Overstock.com Busted Against – Using Black Hat SEO", August 31, 2011, online: <http://globerunnerseo.com/overstock-com-busted-again-using-black-hat-seo> (site consulted on October 24, 2012)

MCKINLEY, K., "Cleaning Up After Cookies Version I.0", December 31, 2008, online: <https://www.isecpartners.com/files/iSEC_Cleaning_Up_After_Cookies.pdf> (site consulted on September 4, 2012)

MEGA GAMES, "Sony Fake PSP Blog Busted", December 14, 2006, online: <http://megagames.com/news/sony-fake-psp-blog-busted> (site consulted on August 27, 2012)

MINISTRY OF ECONOMIC DEVELOPMENT AND TRADE, "Increasing Traffic to Your Website Through Search Engine Optimization (SEO) Techniques", 2011, online: <http://www.ontariocanada.com/ontcan/1medt/smallbiz/sb_downloads/ebiz_Search_Engine_en.pdf> (site consulted on September 9, 2012)

MINISTRY OF ECONOMIC DEVELOPMENT AND TRADE, "Social Media Marketing", 2011, online: <http://www.ontariocanada.com/ontcan/1medt/smallbiz/sb_downloads/ebiz_social_media_marketing_en.pdf> (site consulted on September 9, 2012)

MSNBC.COM, "Whole Foods CEO's anonymous online life: Postings on financial forums attacked a rival company trying to buy", July 12, 2007, online: <http://www.msnbc.msn.com/id/19718742/ns/business-us_business/t/whole-foods-ceos-anonymous-online-life/ > (site consulted on January 25, 2012)

NAIK DESAI, A., "Nimbuzz Reveals Insights About Mobile Based Advertising", July 30, 2012, online: <http://www.watblog.com/2012/07/30/nimbuzz-reveals-insights-about-mobile-based-advertising/> (site consulted on October 23, 2012)

NEATE, R., "Google blacklists websites run by family of Grant Shapps", September 7, 2012, online: <http://www.guardian.co.uk/politics/2012/sep/07/google-blacklists-websites-grant-shapps-family> (site consulted on October 25, 2012)

NIMBUZZ! BLOG, "We have hit 100 Million users mark! Thank you guys :)", August 2, 2012, online: <http://blog.nimbuzz.com/2012/08/02/we-have-hit-100-million-users-mark-thank-you-guys/> (site consulted on October 23, 2012)

O2 MEDIA, "Location Based Messaging: Connect with your customers when they are exactly where you want them!", online: <http://o2media.ie/location-based-messaging.html> (site consulted on October 23, 2012)

OFFICE OF CONSUMER AFFAIRS, "Canadian Consumer Handbook: Misleading Advertising", online: <http://www.consumerhandbook.ca/en/topics/consumer-protection/misleading-advertising> (site consulted on August 22, 2012)

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "A Guide for Individuals: Your Guide to PIPEDA", April 2009, online: <http://www.priv.gc.ca/information/02_05_d_08_e.cfm< (site consulted on February 13, 2012)

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "Cookies – Following the crumbs", 2011, online: <http://www.priv.gc.ca/fs-fi/02_05_d_49_01_e.cfm> (site consulted on November 24, 2011)

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "PIPEDA Report of Findings #2011-001: Google Inc. WiFi Data Collection", June 6, 2011, online: <http://www.priv.gc.ca/cf-dc/2011/2011_001_0520_e.cfm> (site consulted on March 17, 2012)

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "PIPEDA Self-Assessment Tool: Personal Information Protection and Electronic Documents Act", August 12, 2008, online: <http://www.priv.gc.ca/information/pub/ar-vr/pipeda_sa_tool_200807_e.cfm> (site consulted on March 17, 2012)

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting and Cloud Computing", 2010, online: <http://www.priv.gc.ca/resource/consultations/report_2010_e.pdf> (site consulted on January 20, 2012)

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "Review of the Internet traffic management practices of Internet service providers: Submission of the Office of the Privacy Commissioner of Canada to the Canadian Radio-television and Telecommunication Commission (CRTC)", March 3, 2009, online: <http://www.priv.gc.ca/information/pub/sub_crtc_090218_e.cfm> (site consulted on February 18, 2012)

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "Review of the Internet traffic management practices of Internet service providers: Final reply of the Office of the Privacy Commissioner of Canada to the Canadian Radio-television and Telecommunication Commission (CRTC)", September 15, 2009, online: <http://www.priv.gc.ca/information/pub/sub_crtc_090728_e.cfm> (site consulted on February 18, 2012)

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "Review of the Internet traffic management practices of Internet service providers", March 3, 2009, online: <http://dpi.priv.gc.ca/index.php/essays/review-of-the-internet-traffic-management-practices-of-internet-service-providers/> (site consulted on February 20, 2012)

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "The Greatest Threat to Privacy", online: <http://dpi.priv.gc.ca/index.php/essays/the-greatest-threat-to-privacy/> (site consulted on February 20, 2012)

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "The Privacy Implications of Deep Packet Inspection", online: <http://dpi.priv.gc.ca/index.php/essays/the-privacy-implications-of-deep-packet-inspection/> (site consulted on February 20, 2012)

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "What is Deep Packet Inspection?", online: <http://dpi.priv.gc.ca/index.php/what-is-deep-packet-inspection/> (site consulted on February 20, 2012)

OWYANG, J., "Web Strategy Matrix: Google Buzz vs Facebook vs MySpace vs Twitter", February 2010, online: <http://www.web-strategist.com/blog/2010/02/11/matrix-buzz-vs-facebook-vs-myspace-vs-twitter-feb-2009/> (site consulted on September 7, 2012)

PAHLAVAN, K., F. AKGUL, Y. YE, T. MORGAN, F. ALIZADEH-SHABDIZ, M. HEIDARI and C. STEGER, "Taking Positioning Indoors: Wi-Fi Localization and GNSS", 2010, online: <http://www.cwins.wpi.edu/publications/docs/Taking%20Positioning%20IndoorsWi-Fi%20Localization%20and%20GNS.pdf> (site consulted on September 8, 2012)

PAQUETTE, E., "Touche pas à mes cookies!, November 19, 2001, online: <http://archives.lesechos.fr/archives/2001/LesEchos/18533-512-ECH.htm> (site consulted on September 10, 2012)

PARSONS, C., "Deep Packet Inspection: Privacy, Mash-ups, and Dignity", March 2010, online: <http://www.christopher-parsons.com/Academic/Deep_Packet_Inspection-Privacy_Mash-ups_and%20Dignities_1.0(for%20web).pdf> (site consulted on January 20, 2012)

PARSONS, C., "Literature Review of Deep Packet Inspection: Prepared for the New Transparency Project's Cyber-Surveillance Workshop", March 6, 2011, online: <http://www.christopher-parsons.com/blog/wp-content/uploads/2011/04/Parsons-Deep_packet_inspection.pdf> (site consulted on November 24, 2011)

PARSONS, C., "Moving Across the Internet: Code-Bodies, Code-Corpses, and Network Architecture", 2010, online: <http://www.ctheory.net/printer.aspx?id=642> (site consulted on September 7, 2012)

PEW INTERNET & AMERICAN LIFE PROJECT, "Privacy and Data Management on Mobile Devices", September 5, 2012, online: <http://www.pewinternet.org/Press-Releases/2012/Mobile-Privacy.aspx> (site consulted on November 1, 2012)

PINGHUI, Z., "Mengniu smear blitz against Yili ends with jail sentences", March 16, 2011, online: <http://www.scmp.com/article/741054/mengniu-smear-blitz-against-yili-ends-jail-sentences> (site consulted on October 18, 2012)

PLUMMER, R., "Will fake business blogs crash and burn?", May 22, 2008, online: <http://news.bbc.co.uk/2/hi/7287413.stm> (site consulted on January 25, 2011)

QINGCHU, W., "Mengniu says sorry, and accuses", October 23, 2010, online: <http://mobile.shanghaidaily.com/article/?id=452467> (site consulted on August 27, 2012)

QUANTCAST, "Reaffirming Our Commitment to Consumer Choice and Control", December 4, 2010, online: <http://www.quantcast.com/inside-quantcast/2010/12/reaffirming-our-commitment-to-consumer-choice-and-control/> (site consulted on September 22, 2012)

RAMZY, A., "China's New Scandal: Tainted Milk or Smear Campaign?", October 22, 2010, online: <http://www.time.com/time/world/article/0,8599,2027076,00.html> (site consulted on January 25, 2012)

RAYSMAN, R. and P. BROWN, "Software Robots and Unauthorized Access to Web Sites", in *New York Law Journal*, November 13, 2006, online: <http://www.thelenreid.com/resources/documents/1106_Computer%20Law.pdf> (site consulted on March 8, 2011)

REICHHELD, F. F. and P. SCHEFTER, "E-Loyalty: Your Secret Weapon on the Web", (2000), online: <http://www.pearsoned.ca/highered/divisions/text/cyr/readings/Reichheld_Schefter T2P1R1.pdf> (site consulted on October 29, 2012)

RICHARDSON, A., "Location based mobile advertising – Google's following you", May 4, 2011, online: <http://www.youthradio.org/news/location-based-mobile-advertising-googles-following-you> (site consulted on January 20, 2012)

RODGERS, Z., "Questions for Bob Dykes, NebuAd CEO", January 3, 2008, online: <http://www.clickz.com/3628009> (site consulted on October 23, 2012)

ROOSENDAAL, A., "Facebook Tracks and Traces Everyone: Like This!", November 30, 2010, online: <http://ssrn.com/abstract=1717563> (site consulted on January 19, 2012)

ROUSE, M., "Geofencing", January 2011, online <http://whatis.techtarget.com/definition/geofencing> (site consulted on October 23, 2012)

SCHOEN, S., "New Cookie Technologies: Harder to See and Remove, Widely Used to Track You", September 14, 2009, online: <https://www.eff.org/deeplinks/2009/09/new-cookie-technologies-harder-see-and-remove-wide> (site consulted on September 4, 2012)

SEGAL, S., "The Dirty Little Secrets of Search", February 12, 2011, online: <http://www.nytimes.com/2011/02/13/business/13search.html?pagewanted=all&_r=0> (site consulted on October 25, 2012)

SEW STAFF, "What are Doorway Pages?", March 1, 2007, online: <http://searchenginewatch.com/article/2048653/What-Are-Doorway-Pages> (site consulted on September 9, 2012)

SHAW, M., "Location-based advertising takes a cool step forward", August 10, 2012, online: <http://www.mobile-ent.biz/news/read/location-based-advertising-takes-a-cool-step-forward/018981> (site consulted on October 24, 2012)

SHEARMAN, S., "Starbucks trials 02 location-based mobile marketing service", October 15, 2010, online: <http://www.brandrepublic.com/news/1035146/> (site consulted on October 18, 2012)

SINGEL, R., "Privacy lawsuit Targets Net Giants Over 'Zombie' Cookies", July 27, 2010, online: <http://www.wired.com/threatlevel/2010/07/zombie-cookies-lawsuit/> (site consulted on October 22, 2012)

SOHN, G. B., "Hearing on Broadband Providers and Consumer Privacy Before the U.S. Senate Committee on Commerce, Science, and Transportation", September 25, 2008, online: <http://www.publicknowledge.org/pdf/gbsohn-testimony-20080925.pdf> (site consulted on September 6, 2012)

SOLTANI, A., S. CANTY, Q. MAYO, L. THOMAS and C. J. HOOFNAGLE, "Flash Cookies and Privacy", 2009, online: <http://ssrn.com/abstract=1446862> (site consulted on September 4, 2012)

STAT SPOTTING, "Foursquare Statistics: 20 Million Users, 2 Billion Check-Ins", April 27, 2012, online: <http://statspotting.com/2012/04/foursquare-statistics-20-million-users-2-billion-check-ins/> (site consulted on October 24, 2012)

TAYLOR, D., "Edelman screws up with duplicitous Wal-Mart blog, but it's okay?", October 16, 2006, online: <http://www.intuitive.com/blog/edelman_screws_up_with_duplicitious_walmart_blog.html> (site consulted on August 27, 2012)

TELECOMPAPER, "JiWire licenses Wi-Fi positioning system from Skyhook", May 31, 2007, online: <http://www.telecompaper.com/news/jiwire-licenses-wifi-positioning-system-from-skyhook> (site consulted on October 24, 2012)

TERRY, P., "Overstock gets a black eye from black hat", February 25, 2011, online: <http://dailyartifacts.com/overstock-gets-a-black-eye-from-black-hat> (site consulted on October 25, 2012)

THE BLUE NEWS & VIEWS FROM O2, "Free O2 Wifi tempts consumers with Wall's Ice Cream", August 9, 2012, online: <http://news.o2.co.uk/?press-release=free-o2-wifi-tempts-consumers-with-walls-ice-cream#> (site consulted on October 24, 2012)

TRAN, K. D., "Cookies: Technology and Security Issues", online: <http://home.earthlink.net/~ktran/research_papers/Cookies%20Technology%20and%20Security%20Issues.pdf> (site consulted on September 6, 2012)

TRUDEL, P. and F. ABRAN, "L'évaluation et la prise en charge des risques et enjeux", online : <http://www.chairelrwilson.ca/cours/drt3808/prisechargerisquesenjeux.pdf> (site consulted on December 13, 2011)

TRUDEL, P. and K. BENYEKHLEF, "Approches et stratégies pour améliorer la protection de la vie privée dans le contexte des inforoutes", online: <https://depot.erudit.org/bitstream/002690dd/1/0072.pdf> (site consulted on March 17, 2012)

TRUDEL, P., "La responsabilité civile sur Internet selon la Loi concernant le cadre juridique des technologies de l'information", online : <http://www.chairelrwilson.ca/cours/drt6929f/Resp.%20civile-int.fpbq11-01.pdf> (site consulted on December 10, 2011)

TRUDEL, P., "La responsabilité sur internet en droit civil québécois", online : <http://www.chairelrwilson.ca/documents/TRUDEL_resp_internet.pdf> (site consulted on December 13, 2011)

TRUDEL, P., F. ABRAN and G. DUPUIS, "Analyse du cadre réglementaire québécois et étranger à l'égard du pourriel, de l'hameçonnage et des logiciels espions", April 2007, online : <http://collections.banq.qc.ca/ark:/52327/bs1565476> (site consulted on September 9, 2012)

TURNER, N., "O2 enters the location-based deals arena", July 15, 2011, online: <http://www.dma.org.uk/news/o2-enters-locationbased-deals-arena> (site consulted on October 23, 2012)

TWITTER, "Twitter Privacy Policy", May 17, 2012, online: <https://twitter.com/privacy> (site consulted on September 7, 2012)

VAN GROVE, J., "Each Month 250 Million People Use Facebook Connect on the Web", December 8, 2010, online: <http://mashable.com/2010/12/08/facebook-connect-stats/> (site consulted on January 29, 2012)

VANDANA, A., "Using Corporate Blogs for Supporting Interactive Marketing and CRM", September 8, 2011, online: <http://shodhganga.inflibnet.ac.in/bitstream/10603/2697/9/09_chapter%202.pdf> (site consulted on January 21, 2012)

WAL-MART WATCH, "The Wal-Mart Fake Blog Controversy: Anatomy of a Public Relations Disaster", online: <http://walmartwatch.com/wp-content/blogs.dir/2/files/pdf/flog_controversy.pdf> (site consulted on August 27, 2012)

WHORISKEY, P., "Internet Provider Halts Plan to Track, Sell users' Surfing Data", June 25, 2008, online: <http://www.washingtonpost.com/wp-dyn/content/article/2008/06/24/AR2008062401033_pf.html> (site consulted on January 20, 2012)

WILEY REIN LLP, "DoubleClick, Inc. Wins Privacy Lawsuit – May Continue Shipping Cookies", April 2001, online: <http://www.wileyrein.com/publications.cfm?sp=articles&newsletter=4&id=2942> (site consulted on October 22, 2012).

WILLIAMS, C., "BT and Phorm secretly tracked 18,000 customers in 2006: spied on, profiled and targeted for credit cards", April 1, 2008, online: <http://www.theregister.co.uk/2008/04/01/bt_phorm_2006_trial/> (site consulted on October 22, 2012)

WILSON, D., "Facebook admits hiring a PR firm to bad mouth Google", May 13, 2011, online: <http://www.theinquirer.net/inquirer/news/2070674/facebook-admits-hiring-firm-bad-mouth-google> (site consulted on January 25, 2012)

WINDOWS, "Cookies: frequently asked questions", 2012, online: <http://windows.microsoft.com/en-SG/windows-vista/Cookies-frequently-asked-questions> (site consulted on September 2, 2012)

ZDNET FRANCE, « Vie privée et protection des données : la Commission européenne ouvre une procédure contre le Royaume Uni », April 15, 2009, online : <http://www.zdnet.fr/actualites/vie-privee-et-protection-des-donnees-la-commission-europeenne-ouvre-une-procedure-contre-le-royaume-uni-39392143.htm> (site consulted on October 22, 2012)

Encyclopaedias and Dictionaries

GRAYSON, K. A., J. D. HIBBARD and P. KOTLER, "Marketing", in *Encyclopædia Britannica Online Academic Edition*, 2011, online: <http://www.britannica.com/EBchecked/topic/365730/marketing> (site consulted on November 19, 2011)

TECHTERMS, "IP Address", 2012, online: <http://www.techterms.com/definition/ipaddress> (site consulted on September 10, 2012)

Websites

FASKEN MARTINEAU, online: <http://www.fasken.com/> (site consulted on November 1, 2012)

GOOGLE ANALYTICS, online: <http://www.google.com/analytics/> (site consulted on March 6, 2012)