IS THE TRADE IN PERSONAL INFORMATION BENEFICIAL TO CONSUMERS?

Research Project - Final Report
Submitted to the Office of the Privacy Commissioner of Canada
and to Industry Canada's, Office of Consumer Affairs

by

June 2007

Research report published by:

6226 Saint-Hubert
Montreal, Que H2S 2M2

Telephone: 514-521-6820
Toll-free: 1 888 521-6820
Fax: 514-521-0736

union@consommateur.qc.ca
www.consommateur.qc.ca/union

Union des consommateurs' membership
ACEF Abitibi-Témiscamingue
ACEF Amiante – Beauce – Etchemins
ACEF de l'Est de Montréal
ACEF de l'Île-Jésus
ACEF de Lanaudière
ACEF Estrie
ACEF Grand-Portage
ACEF Montérégie-Est
ACEF du Nord de Montréal
ACEF Rive-Sud de Québec
Association des consommateurs pour la qualité dans la construction
Individual members

Union des consommateurs is a member of the organization Consumers International (CI), a federation with 234 members from 113 countries.

Researched and written by
- Me Marie-Eve Rancourt

In collaboration with
- the comité Télécommunication, Télédiffusion, Inforoute et Vie privée

Editor in chief
- Me Marcel Boucher

ISBN : 978-2-923405-20-9

Union des consommateurs would like to thank Industry Canada and Office of the Privacy Commissioner of Canada for their financial assistance to this research project. The opinions expressed in this report are not necessarily shared by Office of the Privacy Commissioner of Canada, by Industry Canada or by the Government of Canada.

In the interests of concision, we chose to not feminize the text herein.

TABLE DES MATIERES

I

UNION DES CONSOMMATEURS, *strength through networking*

Union des consommateurs is a non-profit organization whose membership is comprised of several ACEFs (*Associations coopératives d'économie familiale*), *l 'Association des consommateurs pour la qualité dans la construction* (ACQC), as well as individual members.

Union des consommateurs' mission is to represent and defend the rights of consumers, with particular emphasis on the interests of low-income households. Union des consommateurs' activities are based on values cherished by its members: solidarity, equity and social justice, as well as the objective of enhancing consumers' living conditions in economic, social, political and environmental terms.

Union des consommateurs' structure enables it to maintain a broad vision of consumer issues even as it develops in-depth expertise in certain programming sectors, particularly via its research efforts on the emerging issues confronting consumers. It activities, which are nation-wide in scope, are enriched and legitimated by its field work and the deep roots of its member associations in the community.

Union des consommateurs acts mainly at the national level, by representing the interests of consumers before political, regulatory or legal authorities or in public forums. Its priority issues, in terms of research, action and advocacy, include the following: family budgets and indebtedness, energy, telephone services, radio broadcasting, cable television and the Internet, public health, food and biotechnologies, financial products and services, business practices, and social and fiscal policy.

Finally, regarding the issue of economic globalization, Union des consommateurs works in collaboration with several consumers groups in English Canada and abroad. It is a member of Consumers International (CI), a United Nations recognized organization.

INTRODUCTION

The right to privacy is often defined as the right of the individual to not be pestered and to not have his personal information collected, used or disclosed without his consent. Furthermore, this right to privacy has always been considered an attribute intrinsic to natural persons, which may not be claimed by any business or organization. With deregulation and technological advances, the question of protecting privacy and personal information is arousing increasing interest and concern among Canadians.

Due to its usefulness, especially for marketing purposes, personal information has acquired such value that it has led businesses to make it into a tradable commodity. The collection and sale of personal information is now a business activity equivalent to the sale of any other good or service. In effect, while this commercial activity is generally conducted without the knowledge of the consumer, it is now an integral part of the marketing and even the supply of certain goods or services. Moreover, the particular nature of this sector and its rapid evolution have led several countries to enact laws to oversee its methods and purposes.

The last twenty-five years have seen the advent of an increasing plethora of codes and standards aimed at overseeing the trade in personal information. Initially voluntary, these standards have, over the years, become mandatory in several countries owing to the magnitude this phenomenon has taken. While certain countries, such as the United States, have opted for voluntary oversight, others, including European countries and Canada, have chosen instead to legislate guidelines on the collection and use of personal information.

In Canada, as the courts have recognized, the right to privacy is a fundamental right protected under the Canadian Charter of Rights and Freedoms. In Quebec, this right is also entrenched in the Quebec Charter of Human Rights and Freedoms and protected by various provisions of the Quebec Civil Code. One of the corollaries of the right to privacy is the need to guarantee protection for the personal information of individuals. In effect, such information may only be collected, retained, used or disclosed if certain rules are followed and by complying with certain conditions, as stipulated in the federal and provincial laws on the protection of personal information. In practice, while certain practices do comply with the provisions of these laws, others seem to skirt the limits of legality.

For merchants, a consumer's personal information constitutes extremely valuable data. While it is common to see financial institutions, insurance companies or landlords seek out the services of personal information agents to check, for example, an individual's solvability, such information is increasingly used in the marketing of goods and services. In effect, the beginning of the 1990s saw the advent of a new way to use personal information, i.e. personalized—so-called "one-to-one"—marketing that seeks to individualize the marketing of products to each client as a function of his profile. This approach was made possible by the collection and compilation of personal information—a task greatly facilitated by Internet use.

The information highway, a vast domain, eminently difficult to regulate, facilitates the use of a number of instruments that enable the collection and use of personal information without the knowledge of the party concerned, not to mention the theft of confidential information for fraudulent purposes. Such information is extremely useful to merchants, not only because it enables them to promote their products to individual consumers, but also because, thanks to

profiling techniques, it optimizes their chances of making a sale by tailoring their marketing in accordance with a given consumer's tastes and interests.

The economic potential and competitive advantage that may accrue to the holder of such information raises a number of concerns, including: the consumer's consent re the collection and use of his personal information, security issues re the retention of this data, and avenues of consumer redress. Conscious of the abuses that this type of activity might engender, elected officials in Canada have chosen to impose a variety of conditions on the private sector.

As consumers are increasingly confronted with clauses granting merchants the right to use their personal information for commercial purposes, and as methods enabling the collection and use of information without the consumer's knowledge spread, the time has come to examine whether the trade in personal information benefits consumers in any fashion and whether privacy laws adequately perform their intended role.

To this end, we examined the laws overseeing the protection of personal information at the federal and provincial levels (with particular focus on Quebec), along with the context in which they were adopted, in order to determine their objectives. We then conducted a survey of the different information collection methods, including how they function and how information is subsequently used.

In concluding our analysis we look at the putative advantages and disadvantages for the consumer arising from the personal information trade, as well as the potential risks.

Finally, we offer recommendations bearing both on existing business practices and the rules overseeing them.

APPLICABLE LAWS AND STANDARDS

In Canada, the rules governing the protection of personal information in the private sector are found in the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*),[1] which applies first and foremost to all organizations engaged in commercial activities. *PIPEDA* stipulates the basic rules governing the collection, use and communication of personal information by businesses in the conduct of their activities. However, under the provisions of this federal law (section 26(2)b), provincial legislation may apply to certain businesses in its stead, provided that the law adopted by provincial authorities is judged substantially similas. Shall be considered similar to *PIPEDA* "legislation that provides a basic set of fair information practices which are consistent with the CSA Standard, oversight by an independent body and redress for those who are aggrieved."[2] *PIPEDA* shall however continue to apply to all private sector businesses under federal jurisdiction as well as to businesses engaged in interprovincial or international activities.

To date, Quebec, Alberta and Columbia have adopted laws on personal information protection judged to be substantially similar[3] as well as Ontario for personal information regarding health[4]

As it entered into effect in 1994 (i.e. 10 years prior to *PIPEDA*), Quebec's privacy law, entitled *An Act Respecting the Protection of Personal Information in the Private Sector* (*LPRPSP*), has naturally been the subject of considerably more jurisprudence than its federal counterpart. Moreover, although the provisions of these two laws are similar, there are nevertheless certain potentially quite significant differences which we will discuss, in due course.

This chapter begins with a brief overview of the standards and agreements on privacy protection enacted on the international level. Next, we examine the national context with a view to assessing the intentions behind the standards adopted and the goals pursued by legislators at the time said standards were being elaborated. We conclude the chapter with a comparison of provincial and federal laws.

---

[1] *The Personal Information Protection and Electronic Documents Act*, S.C. 2000, c .5.
[2] Standing Senate Committee on Social Affairs, Science and Technology, 2 December 1999, <http://canadagazette.gc.ca/partI/2002/20020803/html/notice-e.html>.
[3] In Quebec: *Act Respecting the Protection of Personal Information in the Private Sector*, R.S.Q., chapter P-39.1; *Organizations in the Province of Quebec Exemption Order* C.P. 2003-1842, November 19 2003, Canada Gazette part II, Vol. 137, no 25 — December 3 2003. http://canadagazette.gc.ca/partII/2003/20031203/html/sor374-e.html ; In Alberta: *Personal Information Protection Act*, S.A. 2003, c. P-6.5; *Organizations in the Province of Alberta Exemption Order*, C.P. 2004-1163, October 12 2004, Canada Gazette, part II Vol. 138, no 22 — November 3 2004, http://canadagazette.gc.ca/partII/2004/20041103/html/sor219-f.htm ; In British Columbia: *Personal Information Protection Act*, S.B.C. 2003, c. 63.; *Organizations in the Province of British Columbia Exemption Order*, C.P. 2004-1164, October 12 2004, Gazette du Canada partie II, Vol. 138, no 22 — November 3 2004, [En ligne] http://canadagazette.gc.ca/partII/2004/20041103/html/sor220-f.html
[4] *Personal Health Information Protection Act*, S.O. 2004, ch. 3, Schedule A *; Health Information Custodians in the Province of Ontario Exemption Order*, C.P. 2005-2224, November 28 2005, Canada Gazette part II Vol. 139, no 25 — December 14 2005. http://canadagazette.gc.ca/partII/2005/20051214/html/sor399-e.html

Privacy protection and legislation on protecting personal information

International background

Interest in ensuring oversight of privacy protection through the right of access to personal information goes back to the early 1970s. The unprecedented development of new technologies greatly broadened access to increasingly powerful computers for both individuals and businesses. This engendered the concomitant rise of opposing interests: on the one hand, the desire for unlimited access to the information made possible (and indeed facilitated) by these new technologies, and on the other hand, the desire to guarantee the protection of privacy. As stated by the Organization for Economic Cooperation and Development (OECD):

> "Among the reasons for such widespread concern are the ubiquitous use of computers for the processing of personal data, vastly expanded possibilities of storing, comparing, linking, selecting and accessing personal data, and the combination of computers and telecommunications technology which may place personal data simultaneously at the disposal of thousands of users at geographically dispersed locations and enables the pooling of data and the creation of complex national and international data networks. Certain problems require particularly urgent attention, e.g. those relating to emerging international data networks, and to the need of balancing competing interests of privacy on the one hand and freedom of information on the other, in order to allow a full exploitation of the potentialities of modern data processing technologies in so far as this is desirable."[5]

In the 1970s and 1980s, over a third of the member countries of the OECD adopted one or more laws to protect natural persons against the abusive utilization of personal information and recognize their right of access to said information in order to confirm its accuracy and demand, where required, corrections.[6] In countries with a federal structure, both the national state and the provinces adopted laws of this type. Most such laws were enacted after 1973.

The various approaches adopted by different countries to protect privacy have a number of common characteristics, including a few fundamental principles: 1) set, in accordance with the objectives and needs of a given data collection activity, limits to the collection of data of a personal character; 2) restrict the use of the data collected to the declared purposes; 3) create procedures aimed at enabling natural persons to know of the existence of files containing information about them; and 4) provide them with the opportunity to consult said files and, where required, have corrections made to the information appearing therein.

In 1978, the OECD set up an *ad hoc* group of experts on the obstacles to the cross-border flow of data. This group examined the following issues: 1) harmonizing the laws in different countries so as to not create market distortions, 2) oversight re the issues of data security, confidentiality and cross-border flow of data. This group was instructed to elaborate guidelines on *"basic rules governing the transborder flow and the protection of personal data and privacy, in order to facilitate a harmonization of national legislations (…)."*[7] The Group's work was conducted in

[5] OECD, "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," <http://www.oecd.org/document/0,2340,en_3343_34255_1815186_1_1_1_1,00.html> [cited January 26, 2007].
[6] *Ibid.*
[7] *Ibid*, p.7.

close collaboration with the Council of Europe and the European Community. The objectives of the guidelines elaborated by the Group were as follows:

> a) achieving acceptance by Member countries of certain minimum standards of protection of privacy and individual liberties with regard to personal data;
> b) reducing differences between relevant domestic rules and practices of Member countries to a minimum;
> c) ensuring that in protecting personal data they take into consideration the interests of other Member countries and the need to avoid undue interference with flows of personal data between Member countries; and
> d) eliminating, as far as possible, reasons which might induce Member countries to restrict transborder flows of personal data because of the possible risks associated with such flows. [8]

These guidelines were, therefore, to operate in a context of trade liberalization, which included liberalization of the trade in personal information. In effect, although the putative object of these guidelines was the protection of personal information, their acknowledged goal was to ensure a minimum level of protection for such information in a context of free trade expansion, an objective favoured by the OECD. The protection of personal data was not meant to block the free flow of information beyond the strict minimum required. As mentioned in an OECD document: *"The Guidelines (…) while accepting certain restrictions to free transborder flows of personal data, they seek to reduce the need for such restrictions and thereby strengthen the notion of free information flows between countries."*[9]

On 23 September 1980, the OECD Council adopted the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (hereafter, referred to as the Guidelines). The Guidelines are in fact recommendations. Countries are meant to take their stated principles and objectives into consideration when crafting their own laws.

These Guidelines subsequently led to the adoption of the European Parliament and Council Directive of 24 October 1995 on the *Protection of individuals with regard to the processing of personal data and on the free movement of such data*. Member countries must modify their own national legislation to ensure their harmonization with this new directive. Moreover, it's important to underline that this European directive contains a provision prohibiting European organizations from exchanging personal information with organizations from other countries, unless said countries have themselves implemented adequate guarantees ensuring the right of individuals to protection of their personal information. As for determining whether the level of protection offered by an organization located in a third country is adequate, this will depend on the entire context pertaining to the data and its transfer, notably: the nature of the data, the purpose and duration of the information processing envisaged, the data's country of origin and its final destination, the general and sectoral legal rules in force in the third country, and the professional rules and safeguards applied in said country.[10] This rule authorizes a few exceptions, notably when an individual has consented to the data transfer or if said transfer is necessary to execute a contract to which the individual is a party. In cases where a third country is bereft of legislation on the protection of personal information, the transfer may nevertheless

[8] *Ibid*, p.34.
[9] *Ibid.*
[10] European Union, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, Official Journal L 281, 23/11/1995, p. 31. Para.25(2).

be effected, provided that the recipient offers sufficient guarantees, which may take the form of contractual clauses.[11] In that context European Union and the United States established a dialog in order to agree on a system which would insure the protection of personal information tranfered between a member of European Union and the United States[12] The *Safe Harbour Principles*, considered as offering an adequate protection as defined by the guideline, were adopted in July 2000 by the European Commission, after two years of negociations between EC members and the U.S.[13]

In contrast with European countries, the United States has opted instead for a non-regulatory approach, based on voluntary codes. This strategy was set forth by the U.S. government in 1997 in a document entitled *A Framework for Global Electronic Commerce* (*FGEC*). It favours private sector initiatives and seeks to avoid excessive regulation of electronic commerce. In June 1998, the Federal Trade Commission (FTC) conducted a survey of the practices observed in over 1,400 Internet sites to assess respect for fundamental principles in terms of ethical information processing. The survey revealed that many sites did not respect the principles aimed at ensuring the protection of privacy in an acceptable fashion. In effect, whereas, nearly 85% of sites gathered information from consumers, just 14% advised consumers of their information processing practices. Only 2% of the businesses sites surveyed had adopted a comprehensive policy in this regard.[14] As for websites targeting children, the FTC found that while 89% collected personal information, only 23% asked children to get their parents' permission before providing this information. The percentage of sites allowing parents to exercise control over the collection and use of this information was even lower.[15]

In the wake of this report, the *Children's Online Privacy Protection Act of 1998*[16] (*COPPA*), which seeks to regulate issues pertaining to the protection of personal information on Internet sites targeting children under 13 years of age, was enacted and came into force on April 21, 2000. Aside from this law, the only form of oversight pertaining to the collection and use of personal information in the United States remains self-regulation, i.e. "voluntary standards developped and accepted by those who take part in an activity"[17] despite the fact that FTC's 1998 and 1999 reports mentionned the ineffectiveness of that approach[18].

FTC and United States Department of Commerce organised in 1999 *a Public Workshop on Online Profiling,* which gathered all the important internet publicity agencies. Members of the

---

[11] *Ibid*, paragraph 26.
[12] POULLET, Yves, *Les Safe Harbour Principles, une protection adéquate ?* Paris, 17 juin 2000, http://www.juriscom.net/uni/doc/20000617.htm#_ftn10 [cited June 25 2007].
[13] CHASSIGNEUX, Cynthia, *Aterritorialité des atteintes face aux logiques territoriales de protection juridique et problème de l'absence d'homogénéité des législations protectrices (quid des Safe Harbour Principles)*, *Lex Electronica*, vol. 9, n°2, Special issue, winter 2004, p.3 http://www.lex-electronica.org/articles/v9-2/chassigneux.htm
[14] For a policy to be considered comprehensive, it must appear on the organization's website. Otherwise, a policy was not considered comprehensive.
[15] United States Federal Trade Commission (FTC), "*Privacy Online: A Report to Congress*", 1998, p. 2, <http://www.ftc.gov/reports/privacy3/priv-23a.pdf> [cited April 10 2007].
[16] *Children's Online Privacy Protection Act of 1998,* 15 U.S.C. §§ 6501-6506.
[17] TRUDEL, Pierre, « Quel droit et quelle régulation dans le cyberespace ? » Sociologie et sociétés, vol. 32, no 2, automn 2000, p. 205 https://papyrus.bib.umontreal.ca/dspace/bitstream/1866/57/1/0042.pdf [cited June 25 2007].)
[18] United States Federal Trade Commission (FTC), Op. Cit., note 16, p.40 et "*Self-Regulation and Online Privacy: A Report to Congress*", 1999, p.12 [En ligne] http://www.ftc.gov/os/1999/07/privacy99.pdf [cited April 10 2007].

industry anounced the creation of a Working group, the *Network Advertising Initiative* (NAI) to develop a framework for self-regulation of the online profiling industry[19]. Despite that initiative, FTC's 2000 report comes to the same conclusions concerning the ineffectiveness of autoregulation and suggests that regulation might be necessary for the protection of personal information[20]. Still, to this day, no law, except for COPPA, has been adopted to better that protection.

At an OECD Ministerial Conference held in Ottawa in October 1998, entitled "A Borderless World: Realizing the Potential for Electronic Commerce," OECD member countries adopted the *Declaration on the Protection of Privacy on Global Networks,*[21] in which they reaffirmed their commitment to the Guidelines. Moreover, they invited non-member countries, international organizations, industry and businesses to respect the principles and objectives stated therein.

The national context

Following the adoption of the *Guidelines* by OECD member countries and Canada's adherence to them in 1984, the federal government undertook to encourage private sector adoption of voluntary codes on the protection of personal information.[22] However, as the 1980s drew to a close, the Privacy Commissioner, who was mandated to monitor respect for the *Privacy Act*[23] and promote the right to privacy, became concerned about the lack of progress in this regard and demanded federal legislation that would require organizations under federal jurisdiction to develop such codes.[24]

Aware of electronic commerce's economic potential and concerned that excessive regulations might undermine this potential, in the second half of the 90s, the government of Canada began to develop strategies and policies bearing on the commercial, legal, technological and social issues pertaining to this sector. In particular, said strategies and policies sought to answer the privacy concerns raised by this sector.[25] In 1994, on the occasion of the Throne Speech, the Speaker of the House of Commons, the Honourable Gilbert Parent, announced the government's intention to implement a Canadian information highway strategy.[26] In April of that same year, the federal government formed the Information Highway Advisory Council (IHAC). The Council's mandate consisted of deciding *"how best to develop and use the information*

[19] United States Federal Trade Commission (FTC), "*Online Profiling: A Report to Congress" 2000*, p. 7 http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf [cited June 25 2007].
[20] *Ibid*., p. 21
[21] OECD, *Declaration on the Protection of Privacy on Global Networks* C(98)177, <http://webdomino1.oecd.org/horizontal/oecdacts.nsf/Display/48790CCA6B7BD80FC125729B00515E6E?OpenDocument [cited January 25, 2007].
[22] Privacy Commissioner of Canada, *Annual Report 1984-1985.*
[23] *Privacy Act,* R.S.C., 1985, c. P-21. This law concerns the protection of personal information in federal government institutions. The position of the Privacy Commissioner was created under section 53 of this law.
[24] Privacy Commissioner of Canada, *1988-1989 Annual Report* (Ottawa: Department of Supply and Services), 1989; *1989-1990 Annual Report* (Ottawa: Department of Supply and Services), 1990.
[25] SMITH, Margaret, *The Privacy of Personal Information and Electronic Commerce – Recent Developments,* May 31, 2000, <http://dsp-psd.tpsgc.gc.ca/Collection-R/LoPBdP/BP/prb0005-e.htm> [cited January 29, 2007].
[26] Debates of the House of Commons (Hansard), Volume 133, Issue 002, 2nd Session, 35th Parliament.

highway for the economic, cultural and social advantage of all Canadians (…) and how to achieve an appropriate balance between competition and regulation." [27]

Even as the government undertook to provide a regulatory framework to ensure adequate privacy protection for Internet users, voluntary standards—the fruit of a consultation process involving the private sector, government and consumer advocacy groups—saw the light of day. Elaborated under the guidance of the Canadian Standards Association (CSA), these voluntary standards are based on ten principles that attempt to strike a balance between, on the one hand, the right to privacy of individuals and, on the other hand, the information needs of the private sector. Considered a voluntary standard, the CSA's model code was designed to serve as a model that businesses may adopt and amend, in accordance with their particular context.

In 1996, the Uniform Law Conference of Canada (ULCC), an independent organization that works to promote the harmonization of laws across the country, recommended that a law be drafted to govern the protection of personal information in the private sector. Said law would have the following objectives:

- apply equally to all businesses and non-government organizations, regardless of size or type of activity;
- treat all personal data in the same way, regardless of their differing sensitivity;
- be based on established data protection principles such as those found in the Canadian Standards Association Model Code for the Protection of Personal Information;
- establish an administrative mechanism to oversee the implementation of the law (such as existing data protection commissions);
- provide the data protection commission with the power to educate the public about data protection in the private sector;
- investigate and mediate complaints, but only after the company complaint process had been tried first (assuming there was a company complaint process and that the process had clear and short timelines) while allowing for exceptional cases where a complaint could go directly to the commission);
- allow the commission to publish the names of companies that did not comply with the data protection law; and
- include an offence provision for violation of the law.[28]

In 1996, in a report entitled "Building the Information Society: Moving Canada into the 21st Century," Industry Canada affirmed that legislative recognition of the right to privacy was imperative, particularly as regards the retention of personal information in electronic databases.[29] That same year, the federal ministers for Industry and Justice announced the federal government's intention to legislate to protect privacy.

In January 1998, Industry Canada and the Department of Justice released a working document on the protection of personal information which highlighted the fact that consumer confidence was essential to the development of the information economy. As this document put it: *"legislation that establishes a set of common rules for the protection of personal information will*

[27] Health Canada, Information Highway Advisory Council, "Canada's Health Infostructure," http://www.hc-sc.gc.ca/hcs-sss/ehealth-esante/infostructure/ihac_ccai_e.html [cited April 20, 2007].
[28] SMITH Margaret, opinion cited, note 25.
[29] Canada, Industry Canada, "Building the Information Society: Moving Canada into the 21st Century," Ottawa, 1996, p. 25.

help to build consumer confidence and create a level playing field [so that] the misuse of personal information cannot result in a competitive advantage."[30] According to Industry Canada, the admitted objective of a legislative framework on the protection of personal information had to do, first and foremost, with commercial considerations: *"To create an environment conducive to the growth of electronic commerce in Canada, the Government has committed to developing legislation that will protect personal information in the private sector, while allowing for the flow of information that is essential to our ability to compete in a global economy."*[31] Far less elaborate than the ULCC document, Industry Canada's working document stated that federal legislation was necessary to attain this objective, and that such legislation should take the following four key elements into account:

- obligations based on fair information practices;
- administrative arrangements for an overseeing body to ensure accountability;
- powers for overseeing authorities and judicial bodies; and
- powers and responsibilities that will promote public awareness and ensure effective implementation of obligations.[32]

In effect, with the objective of strengthening consumer confidence, Canada adopted standards and laws on the protection of personal information that would implement mechanisms apt to avert the fraud and abuses that can result from the uncontrolled collection and use of this type of information. In light, however, of the importance of the collection and use of personal information to the conduct of business activities, this legislation, which prioritized facilitating such business activities, had to find the right balance between standards that would be sufficient to ensure public confidence regarding protection of privacy and a regulatory regime that would not constitute a barrier to trade and the free flow of information. This balance was to be found via oversight that respected the key elements above.

Organizations and commercial activities

On January 1, 2004, the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*) came into full effect.[33] This law applies *"to every organization in respect of personal information that (…) the organization collects, uses or discloses in the course of commercial activities (…)."*[34] Thus, with the exception of activities conducted by businesses not under federal jurisdiction and active in a province that has adopted a substantially similar law, all commercial activities conducted in Canada by private sector organizations come under the purview of this law.

---

[30] Canada, Departments of Industry and Justice, Electronic Commerce Working Group, "The Protection of Personal Information: Building Canada's Information Economy and Society," January 1998, p. 6.
[31] *Ibid.*
[32] *Ibid*, p. 11.
[33] Office of the Privacy Commission of Canada, *Factsheet: Complying with the Personal Information Protection and Electronic Documents Act*. "PIPEDA has been coming into effect in stages. As of January 2001, the Act has applied to personal information about customers or employees in the federally-regulated sector in the course of commercial activities. It also applies to information sold across provincial and territorial boundaries. As of January 2002, the Act has also applied to personal health information collected, used or disclosed by these organizations.
Since January 1, 2004, PIPEDA applies right across the board — to all personal information collected, used or disclosed in the course of commercial activities by all private sector organizations, except provinces which have, by then, enacted legislation that is deemed to be substantially similar to the federal law."
[34] *PIPEDA*, Art.4.

The term "organization" contained in the Act refers not only to associations, societies, and trade unions, but also to individuals engaged in a commercial activity.[35] By "commercial activity," *PIPEDA "means any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists."* In an information factsheet issued in 2004, the Privacy Commission explained as follows how *PIPEDA* applies to charitable works and not-for-profit organizations:

> *"The presence of commercial activity is the most important consideration in determining whether or not an organization is subject to the Act. (…)*
>
> *Whether or not an organization operates on a non-profit basis is not conclusive in determining the application of the Act. The term non-profit or not-for-profit is a technical term that is not found in the PIPEDA. The bottom line is that non-profit status does not automatically exempt an organization from the application of the Act.*
>
> *Most non-profits are not subject to the Act because they do not engage in commercial activities. This is typically the case with most charities, minor hockey associations, clubs, community groups and advocacy organizations. Collecting membership fees, organizing club activities, compiling a list of members' names and addresses, and mailing out newsletters are not considered commercial activities. (…)*
>
> *As the definition of commercial activity makes clear, selling, bartering or leasing a membership list or a list of donors would be considered a commercial activity. As a result, consent is required for the disclosure of this information."*[36]

With the Privacy Commission having specified that monetary considerations are not necessary for an activity to be commercial in nature, one must acknowledge that uncertainty persists re the exact characteristics required to determine whether an activity is considered a commercial activity within the meaning of the *PIPEDA*. Moreover, the provision of a service in exchange for a sum of money doesn't necessarily constitute a commercial activity, as attests a ruling made in 2006 by the Assistant Commissioner, which ruled that a private school wasn't conducting any commercial activity within the meaning of the Act[37] and that since the school was not subject to *PIPEDA*, the Commissioner was not competent to investigate. The Assistant Commissioner based her ruling on two grounds: 1) the establishment's principal activity is to educate and 2) the generation of profits for the establishment's proprietors is not among the organization's objectives.

These conclusions concerning whether *PIPEDA* applies to a given organization or not—which are based on an organization's principal activity and objectives, rather that the character of the activity as such—seem hard to reconcile with the letter of the law and with the interpretation of same offered by the Commission in 2004 (see above). Thus, if the definition of what constitutes

---

[35] *PIPEDA*, Art.2(1).

[36] Office of The Privacy Commissioner of Canada, *Factsheet: The Application of the Personal Information Protection and Electronic Documents Act to Charitable and Non-Profit Organizations*, <http://www.privcom.gc.ca/fs-fi/02_05_d_19_e.asp> [cited May 2, 2007].

[37] Office of The Privacy Commissioner of Canada*, "*Commissioner's Findings - *PIPEDA* Case Summary #345: Private school not covered by *PIPEDA*," July 5, 2006, <http://www.privcom.gc.ca/cf-dc/2006/345_20060705_e.asp> [cited June 2, 2007]. We would like to point out that in publishing summaries rather than the full text of its rulings, with the complete arguments upon which they are founded, the Privacy Commission does not facilitate the interpretation of its rulings.

a "commercial activity" leaves room for interpretation and if the existing laws and jurisprudence don't allow us to establish the legal definition of this term with certainty, determining whether certain organizations are subject to federal law or not may also be clouded with uncertainty.

Personal information

As for the definition of what constitutes "personal information" *PIPEDA* stipulates that it is: *"information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization."*[38] Personal information *"includes any factual or subjective information, recorded or not, about an identifiable individual. This includes information in any form, such as: age, name, ID numbers, income, ethnic origin, or blood type; opinions, evaluations, comments, social status, or disciplinary actions, employee files, credit records, loan records, medical records, existence of a dispute between a consumer and a merchant, intentions (for example, to acquire goods or services, or change jobs)."*[39]

Principles

It is evident that the code elaborated by CSA was incorporated into *PIPEDA* and represents the heart of this federal legislation. The CSA code defined the obligations and responsibilities of organizations in relation to the collection, use and disclosure of personal information. Its ten principles, restated and detailed below, constitute the principal obligations of businesses and other organizations under *PIPEDA* in relation to the processing and management of personal information:

1. Accountability: An organization is responsible for the personal information it processes and must appoint one or more individuals to ensure compliance with *PIPEDA* principles. The public must have access to these persons' contact information and the Privacy Protection Officer must be granted sufficient authority to execute his functions and responsibilities.

2. Identifying purposes: An organization must identify the reasons for collecting personal information before or at the time of collection. Moreover, the consumer must be informed of how the information will be used and/or communicated.

3. Consent: Any time personal information about an individual is collected, used or disclosed, the individual must be informed and he must give his consent (except in certain specific cases[40]). This consent must be obtained prior to or at the time of the data collection. It must be obtained anew if any new use of this personal information is envisaged, regardless of whether this information was obtained directly from the person concerned or from a third party, unless it is not appropriate to obtain such consent.

4. Limiting collection: An organization may only collect the personal information necessary for specific purposes and must do so in an honest and lawful fashion. It is prohibited to

[38] *PIPEDA*, Art.2.
[39] Office of The Privacy Commissioner of Canada, *Factsheet: Complying with the Personal Information Protection and Electronic Documents Act,* <http://www.privcom.gc.ca/fs-fi/02_05_d_16_e.asp> [cited May 3, 2007].
[40] *PIPEDA,* Art.7; *LPRPSP*, Art. 18-25; *PIPA* Alberta, Art. 14, 17, 20; *PIPA* British Columbia, Art. 12, 15, 18; and see *infra* on personal information of a public nature.

collect more personal information than necessary. An individual has every right to refuse to disclose personal information that is not necessary for carrying out the transaction.[41]

5. Limiting use, disclosure, and retention: Personal information must not be used or disclosed for any other purpose than that for which it was collected, unless the individual so consents, or the Act so requires. Personal information shall only be retained for as long as it is needed to satisfy the purposes for which it was collected.

6. Accuracy: Personal information must be as accurate, complete and up-to-date as required for its intended purposes. Organizations are required to make all necessary efforts to eliminate the possibility of using inaccurate or out-of-date personal information.

7. Safeguards: Personal information must be protected via safeguards that correspond to their degree of sensitivity. Such measures must not only include network security measures to safeguard data from unauthorized access (i.e. hackers) or similar threats, they should also ensure physical security (e.g. locked doors and the limiting of access to authorized personnel).

8. Openness: an organization must ensure that precise information on its personal information management policies and practices are understandable and easily available.

9. Individual access: Upon request, an organization must inform any individual of the existence of any personal information about him in its possession; explain how it is used; state how and to whom it may be disclosed; and allow said individual to access this information. Provisions must also exist for challenging the accuracy and completeness of such information, as well as for making appropriate changes and corrections. On the other hand, access may be refused if certain information includes confidential information or information about other persons.

10. Provide recourse: Any individual must have the right to lodge a complaint concerning non-compliance with the above mentioned principles by communicating with the responsible person or persons at the organization in question. Organizations must therefore develop simple and easily accessible complaint procedures, investigate the complaints lodged and, when a complaint is founded, make the necessary changes to their information management practices and policies.

The provincial scene

In the 1970s, Quebec became a pioneer in terms of privacy protection through the adoption of a number of laws to ensure oversight over the use of and access to certain types of personal information. The first such initiative was the adoption of the *Consumer Protection Act,*[42] which guaranteed that all persons have the right to access their credit file. Subsequently, other laws, such as the *Professional Code,*[43] established principles now considered fundamental, such as

[41] The Privacy Commissioner judged the complaint of the applicant who opposed the verification of his credit record as a condition for opening a bank account to be founded. Office of The Privacy Commissioner of Canada, *C*ommissioner's Findings – "*PIPEDA* Case Summary #40*:* Applicant objects to credit check as condition for opening bank account," March 12, 2002, <http://www.privcom.gc.ca/cf-dc/2002/cf-dc_020312_f.asp> [cited May 3, 2007].
[42] R.S.Q., chapter P-40.1.
[43] R.S.Q., chapter C-26.

professional privilege and the confidentiality of personal information. It was in this context that Quebec adopted *An Act Respecting the Protection of Personal Information in the Private Sector* (hereafter referred to as *LPRPSP*, its acronym in French) in 1994. To date, two other provinces, Alberta and British Columbia have enacted similar laws. These laws, entitled the *Personal Information Protection Act*, (*PIPA*) in both provinces, came into force on January 1, 2004. These provincial laws have all been judged to be substantially similar to *PIPEDA*. Consequently, they, rather than the *PIPEDA*, apply in their respective provinces to the intra-provincial activities of private sector organizations not under exclusive federal jurisdiction.[44]

In enacting the *LPRPSP*, Quebec became the first jurisdiction in North America to legislate on the collection, use, disclosure and retention of personal information in the private sector. This law applies to personal information *"that a person collects, holds, uses or communicates to third persons in the course of carrying on an enterprise"*[45] in the province of Quebec.

Personal information

In Article 2 of the *LPRPSP*, the term "personal information" is defined as *"any information which relates to a natural person and allows that person to be identified."* The jurisprudence of the *Commission d'accès à l'information* has further refined this definition by specifying that the information covered by the Act is that which *"cerne les caractéristiques de l'individu: il se définit par rapport à cette personne et à celle-là seulement. C'est une donnée objective qui fonde son existence sur un être en chair et en os"* ("...circumscribes the characteristics of an individual: it is defined in reference to this person and this person only. It is an objective datum the existence of which is founded on a flesh and blood being").[46] Thus, personal information, within the meaning of the *LPRSP* enables the characterizing and distinguishing of one person from another. Such characteristics may be partial, but significant (e.g. age, retirement income, recommendations, etc.)[47].

Organizations

By "enterprise" is meant the rather broad meaning given in Article 1525 of the Quebec Civil Code: *"The 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, constitutes the carrying on of an enterprise."*[48]

The other two provincial privacy acts also apply, except where expressly specified, to any organization, in relation to the personal information it collects, uses or communicates to third parties.

---

[44] Office of the Privacy Commissioner of Canada, "About Us: Mandate and Mission of the OPC," <http://www.privcom.gc.ca/aboutUs/index_e.asp> [cited June 1, 2007].
[45] *LPRPSP*, Art.1.
[46] Commission d'accès à l'information, *Claude Stebenne c. Assurance-vie Desjardins*, ruling of 16 December 1994, P-0020, p. 5, <http://www.cai.gouv.qc.ca/07_decisions_de_la_cai/01_pdf/jurisprudence/940366de.pdf> [cited May 20, 2007].
[47] *Ibid*.
[48] *Civil Code of Quebec*, C.c.Q., 1991, c. 64, Article 1525. The entire text of the Code may be consulted online at: <http://www.canlii.org/qc/laws/sta/ccq/20050513/whole.html> [cited May 10, 2007].

The definition of the term organization in Alberta's *PIPA* includes corporations, unincorporated associations, unions, partnerships and individuals who conduct commercial activities.[49] As for the notion of personal information, this is defined as "information about an identifiable individual."[50] The Act specifies, however, that information that enables the contacting of an individual at a place of business is excluded, provided that it is only used for that purpose.[51]

British Columbia's *PIPA* also applies to all organizations, except where expressly specified (the Act's definition specifically mentions foundations and non-profit organizations). Here again, personal information is information about an identifiable individual. The Act specifies that information that enables the contacting of an individual at a place of business is excluded. Such information includes a person's name, title, business address, and business telephone and fax numbers, as well as his e-mail address.[52]

Differences between federal legislation and provincial legislation

Organizations subject to privacy legislation

The scope of provincial legislation differs from that of the *PIPEDA*. As mentioned above, the federal act applies to organizations engaged in commercial activities, which excludes for all practical purposes, the activities of not-for-profit organizations and charities. Provincial laws, which are broader in scope, also apply to this category of organizations. Thus, whereas legislation in British Columbia mentions non-profit organizations in its definition of the term "organisation," Alberta's *PIPA* stipulates that non-profit organizations are subject to the law insofar as personal information is collected, used or disclosed in the context of commercial activities.[53] There also exists a difference regarding the treatment of so-called "information of a public nature."

Personal information of a public nature

Whereas, in British Columbia and Quebec, the rules in relation to the collection, retention, use and disclosure of personal information do not apply to such information if it is of a public nature (e.g. personal information available in the phone book or broadcast on television or printed in newspapers, etc.),[54] the federal law and Alberta's legislation limit this exemption to cases where such information is used for the purposes for which it was made public.[55]

---

[49] *PIPA* Alberta, Art. 1(i).
[50] *PIPA* Alberta, Art. 1(k).
[51] *PIPA* Alberta, art. 4(3)d.
[52] *PIPA* British Columbia, Art. 1 and OGILVY RENAULT Resources Center, "The Office of the Privacy Commissioner of Canada responds to the Geist complain" (2005), <http://www.ogilvyrenault.com/fr/ResourceCenter/ResourceCenterDetails.aspx?id=897&pId=43> [cited May 10, 2007].
[53] *PIPA* Alberta, Art. 56(2). In contrast with the finding of the Assistant Privacy Commissioner cited above (*PIPEDA* #345, opinion cited, note 30), Alberta's *PIPA* expressly mentions private schools as subject to the Act in Article 56 (1).
[54] *Personal Information Protection Act*, B.C. Reg. 473/2003, Art. 6 (this regulation stipulated that such information is only excluded if the individual refused its inclusion in the public register); *PIPEDA,* Art.1.
[55] *Personal Information Protection Act Regulation*, Alta. Reg. 366/2003; Art. 7; *PIPEDA,* Art. 7 and 26.

These differences between provincial laws have the effect of imposing different rules on companies from one province to another. They also create uncertainty regarding the applicable criteria and definitions when it comes to inter-provincial commercial activities.

The organizations entrusted with enforcing privacy laws

Whereas at the federal level, the Privacy Commission is charged with ensuring respect for *PIPEDA*, the provinces have entrusted the enforcement of their respective laws to quasi-judicial bodies: i.e. the Office of the Information and Privacy Commissioner in Alberta and British Columbia and *la Commission d'accès à l'information* in Quebec. The differences between the powers granted to these bodies has a direct impact on how these laws are administered and how complaints are processed.

The role conferred to the Privacy Commission by the federal government is that of an ombudsman, i.e. he is to function as a conciliator and mediator. The Commissioner's rulings are simply recommendations and are in no way binding. If, following a ruling by the Commissioner, a complainant still believes that he has been prejudiced, he may still, under section 14 of *PIPEDA*, bring a case before the Federal Court. He may, for example, ask the Court to render binding a ruling of the Commissioner or, where a Commissioner has found a complaint to be unfounded, to make a new ruling, following an examination of the practices of the organization against which the initial complaint was lodged. The Court's role shall not be to examine the Commissioner's report but instead to take a fresh look at the evidence presented by both parties.[56] If the Court allows the application, it may order the organization to review its practices and/or order payment of damages to the claimant. It should be pointed out that this two-stage procedure (first, turning to the Commission, and then, to the Court) not only makes the process more complicated, but it also renders public a debate that the applicants might prefer to keep confidential, precisely since it concerns a violation of their privacy or an issue of confidentiality.[57] To date, very few complainants have exercised this right of appeal.[58] We would like to point out that, to date, the Federal Court has never granted damages to a plaintiff in a cause bearing on privacy issues.[59]

As for the provincial organizations, the *Commission d'accès à l'information*, may, for example, *"make any order it considers appropriate to protect the rights of the parties and rule on any issue of fact or law."*[60] The Commission may also order an enterprise *"to communicate or rectify personal information or refrain from doing so."*[61] Its rulings are executory within thirty days. The PIPAs in Alberta and British Columbia grant similar powers to their respective Privacy Commissioners.[62] As in Quebec, British Columbia's *PIPA* gives an enterprise thirty days to

[56] Office of the Privacy Commissioner, "Factsheet: Applications for Court Hearings Under *PIPEDA*," <http://www.privcom.gc.ca/fs-fi/02_05_d_31_e.asp> [cited 10 May 2007].
[57] J. Lawford, *Consumer Privacy under* PIPEDA*: How Are We Doing?* (2004), Public Interest Advocacy Centre (PIAC), < http://www.piac.ca/files/pipedareviewfinal.pdf> [cited June 2, 2007].
[58] Out of the over 1,400 complaints received by the Privacy Commissioner, only 9 have been commented on by the Federal Court. Ian Kerr, "Submission to the House of Commons Standing Committee on Access to Information, Privacy and Ethics on the Personal Information Protection and Electronic Documents Acts (PIPEDA)," p. 15, <http://www.cippic.ca/en/projects-cases/privacy/submissions/IK_PIPEDA_Review_Submission_(final)_FORMATTED.pdf> [cited 20 April 2007))
[59] *Ibid.*
[60] *LPRPSP*, Art.55.
[61] *Ibid*.
[62] *PIPA* Alberta and British Columbia, Art. 52.

comply with a ruling rendered by the Commission. In Alberta, an organization must comply within fifty days.[63]

These differences in the roles conferred on provincial commissions as opposed to their federal counterpart are also reflected in the monitoring and investigative powers granted them. Whereas, under the provisions of provincial laws the Privacy Commissioner may investigate any organization regarding its personal information management policies,[64] the federal Act stipulates for its part that the Commissioner must, before proceeding with the investigation of an enterprise's practices, have *"reasonable grounds to believe that the organization is contravening a provision of Division 1 or is not following a recommendation set out in Schedule 1 (…)."*[65] Consequently, under the provisions of *PIPEDA*, the federal Privacy Commissioner is not authorized to conduct random investigations on his own initiative to inspect the policies and practices of organizations as regards any personal information they are likely to collect. This requirement invoking "reasonable grounds" may constitute an obstacle to enforcement of and compliance with the Act, as it allows challenges from any enterprise that the Commissioner might wish to investigate.[66]

Penal provisions

Under provincial legislation, the bodies charged with enforcement may impose fines on offenders when certain of their provisions have been violated or when investigations conducted pursuant to these laws are obstructed. In such cases, both the legal entity and its officers, administrators or representatives may be subject to fines.[67] On the other hand, these provincial laws do not provide for the granting of damages to the complainant by their respective Commissioners. To obtain the payment of damages, the complainant must act in accordance with the general rules applicable to civil law in his province.[68]

No penal provisions were incorporated in *PIPEDA*. Consequently, neither the Privacy Commission nor the Federal Court has the power to impose any fine or penalties whatsoever on offenders. As we saw above, the Federal Court, when rendering a ruling under the provisions of *PIPEDA*, has the power to order the payment of damages to the claimant.

---

[63] *PIPA* Alberta, Art. 54; *PIPA* British Columbia, Art. 53.
[64] *LPRPSP*, Art. 80.2 to 81; *PIPA* Alberta and British Columbia, Art. 36 to 44.
[65] *PIPEDA*, Art. 18(1).
[66] This is the action that Equifax took. After the Privacy Commissioner had initiated an investigation, Equifax instituted proceedings for a judicial review with the aim of having this investigation ended, citing the Privacy Commissioner's lack of "reasonable grounds" for launching such an investigation, despite the fact that four individual complaints on Equifax's practices had been filed with the Consumer Protection Bureau. Canadian Internet Policy and Public Interest Clinic (CIPPIC), "Submission to the House of Commons Standing Committee on Access to Information, Privacy and Ethics on the Personal Information Protection and Electronic Documents Act (*PIPEDA*)," November 28, 2006, pp. 8-9. However, on March 14, 2007, Equifax concluded an agreement with the Privacy Commission and dropped the legal challenge it had filed in the Federal Court. Office of the Privacy Commissioner, News release, "Privacy commissioner works with Equifax to conclude audit," March 16, 2007, http://www.privcom.gc.ca/media/nr-c/2007/nr-c_070316_e.asp [cited 18 mars 2007].
[67] *PIPEDA,* Art.91-93; *PIPA* Alberta, Art. 59; *PIPA* British Columbia, Art. 56.
[68] *PIPA* Alberta, Art.60; *PIPA* British Columbia, Art. 57.

Inclusion of e-mail addresses as personal information

Apart from instances where an individual's electronic address is composed of his name, it would not appear that an e-mail is liable to enable identification of a person or is apt to be associated with an identifiable person. Does an individual's electronic address constitute information covered by the laws on the protection of personal information?

In a decision rendered in 2005, the Assistant Privacy Commissioner answered this question in the affirmative, at least with respect to work-related electronic addresses. In this particular case, unsolicited e-mails were sent for marketing purposes to electronic addresses that had been collected in directories open to public access and in a directory that was only accessible to the members of a particular association. In this case bearing on a professional and non-personal electronic address, the Assistant Commissioner concluded that:

> *"The interpretation section of the Act prescribes the types of information that are not subject to the protections of the Act, specifically, the name, title or business address or telephone number of an employee of an organization. As a business e-mail address is not specified in section 2, the Assistant Commissioner concluded that it was an individual's personal information for the purposes of the Act."*[69]

If a professional electronic address constitutes personal information, then an *a fortiori* case must be made for considering personal electronic addresses as personal information under the provisions of *PIPEDA*. Moreover, the Assistant Privacy Commissioner had previously recognized as founded another complaint concerning the communication of e-mails.[70]

Furthermore, the Privacy Commission's website specifically mentions e-mail addresses as constituting personal information: *"Email is a highly convenient and cost-effective way to communicate. Your private email address, along with the content of personal email messages, is your personal information."*[71]

As we saw above, legislation in Alberta and British Columbia both include professional e-mail addresses in the list of types of information not enjoying privacy protection. The Act in Alberta further specifies that this exemption only applies to uses consistent with the intended purposes of the circulation or posting of said information.[72]

Given the fact that these two provincial Acts adopted an approach similar to that of the federal Act, which specifically excluded professional information from its purview, and the fact that e-mail addresses were expressly mentioned in the list of personal information, it is a strong bet that personal e-mail addresses shall also be considered as constituting personal information under the provisions of these laws.

---

[69] Office of the Privacy Commissioner, "Commissioners Finding's - *PIPEDA* Case Summary #297, Unsolicited e-mail for marketing purposes," April 8, 2005, <http://www.privcom.gc.ca/cf-dc/2005/297_050331_01_e.asp> [cited May 3, 2007].

[70] Office of the Privacy Commissioner, "Commissioners Finding's - *PIPEDA* Case Summary #277: Mass mailout results in disclosure of contest entrants e-mail addresses," September 2, 2004, <http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040902_02_e.asp> [cited May 10, 2007].

[71] Office of the Privacy Commissionner "Factsheet: Protecting your Privacy on the Internet," <http://www.privcom.gc.ca/fs-fi/02_05_d_13_e.asp - 003> [cited May 15, 2007].

[72] It's worth remembering that whereas the exclusion regarding information of a public nature is subject to a similar restriction in Alberta, as well as under federal legislation, this restriction does not apply in British Columbia and Quebec where information of a public nature is not protected.

Aside from generally excluding information of a public nature, Quebec's *LPRPSP* contains no particular provisions on work-related contact information. In the absence of jurisprudence, one might wonder whether, in accordance with the *LPRPSP's* wording, an e-mail address constitutes personal information, i.e. *information "which relates to a natural person and allows that person to be identified."* It seems obvious that a simple e-mail address would suffice to identify its owner if the first and last names of said owner appear in this address. An anonymous address might be a different story. According to certain analysts, the interpretation favoured by the Privacy Commission could *"have an impact on the interpretation of Quebec privacy legislation, especially since the federal Privacy Commissioner has the power to consult the provincial authorities and to enter into agreements to standardize privacy practices."*[73]

[73] Ogilvy Renault, opinion cited, note 52.

THE COLLECTING OF PERSONAL INFORMATION

Impact of the expanding telecommunications sector

Technological developments in recent years and the introduction of fibre optics into the economy have engendered a revolution in telecommunications. This development has had and will continue to have a direct impact on the capacity to collect and use personal information and, by the same token, on the protection of privacy. For example, the Internet, as we now know it, was simply unimaginable 25 years ago. The first server, which appeared in 1990, thus signalling the birth of the "World Wide Web" (WWW), only permitted the visiting of a handful of websites, most of them American.[74] In those days, the average speed of a private Internet connection was between 2,400 and 9,600 bits/sec.[75] Prior to the 1990s, the telecommunications sector concentrated on two main functions: telephone and fax services. It was only with the takeoff of the Internet, a few years later, that telecommunications would assume a multiplicity of functions: on-line newspapers, shopping, document consultation, classified advertising, on-line payments, etc. A number of factors contributed to an exponential expansion in the potential of information technologies: the acceleration of internet connection speeds, which has now reached 10G bits/sec,[76] the digitalization of information and its transmission, the phenomenal increase in the power of micro-processors[77] and the public's broadened access to computers. It is estimated that computers double in power every 18 months, even as prices drop by half at the same time.[78] As a consequence, it is now easy and affordable to acquire powerful computer equipment. And that makes it easy to gather and store an impressive quantity of information.

These developments in information technologies have brought about revolutionary changes in modern society, which has made the transition from the industrial age to the information age. Digitalization has been applied to every type of information, including those that most directly concern human beings. People's lives have now taken the form of a complex digital existence, in which information sets provide access to numerous spheres of activities and services: work, health, education, finance, leisure activities, etc. Included in this mass of data, which allows an individual to identify himself and which is now stored in computer databases, one finds a wide gamut of information: social assurance number, health insurance number, driver's licence, folios, user names and passwords permitting access to various files or services, permanent codes, address, date of birth, telephone number, etc. Such information is of great value to those in its possession because through it one may identify and *know* the individuals in question, even to the point of enabling identity theft.

---

[74] POULLET, Yves, Consultative Committee of the Convention for the Protection of Individuals with regard to automatic processing of personal data, "Report on the Application of Data Protection Principles to the Worldwide Telecommunication Networks," (Strasbourg: Council of Europe, 2004) p. 6.
[75] *Ibid*, p. 7.
[76] *Ibid*. This is in reference to average computer hardware—state of the art equipment can of course attain far greater speeds.
[77] *Ibid,* in 1987, the average computer had an 8 MHz processor with 640 kilobytes of memory (RAM) and a 20 MB hard drive. In 2004, the average computer had a 2.4 GHz processor (i.e. 300 times more powerful than the one in 1987), 256 MB of RAM (i.e. 400 times more than in 1987) and a hard drive with a capacity of 60 GB (i.e. 3,000 times more storage capacity).
[78] *Ibid.*

Easy access to such information sets makes it easy and fast to enter into communication with an individual and/or ascertain his interests and activities. The combining of increased information storage capacity with ease of data processing has led to an increase in the commercial value of such information, which businesses now turn to as an everyday resource to better know the clients with whom they do business... or those with whom they would like to do business. In effect, although personal information agents were among the first to market such information, principally in order to analyse credit files, the information collected today, through digital techniques, is far more diversified and potentially far more "eloquent."

In order to analyse how the trade in personal information functions, it's worthwhile to first study the methods that businesses use to collect information on consumers. There are two main categories of methods: collection of information explicitly disclosed by the consumer and collection done without his knowledge. As we shall see, these different methods make it possible for businesses to obtain a large quantity of information about individuals. However, before examining these different methods, let's take a quick look at the types of organizations that engage in information collection.

Types of organizations that collect personal information

Among the types of organizations that most frequently collect personal information are various government departments, non-profit organizations, businesses and personal information agents, each of which collects information for its own motives and goals. Moreover, said information is used in different ways as well: administrative purposes, communications, information disclosure or advertising, marketing, the sale of personal information, etc.

Concerning the communication of personal information, government agencies often transfer personal information on taxpayers to other government agencies, but generally do not disclose it to private businesses. On the other hand, certain governmental agencies do publish certain types of general information compiled from personal information collected from individuals (e.g. income and health statistics). This information is then used by businesses to guide their business strategies. It should be noted here that governmental agencies are subject to different protection of personal information laws, which are only applicable to the public sector (a federal act applies to federal government agencies[79] and each province has its own laws that apply to its own agencies[80]).

Non-profit organizations, for their part, tend to swap their lists of donors or they may, on occasion, rent these lists to information brokers.[81] The Canadian Red Cross, for example, acknowledges in its privacy policy that it engages in such practices.[82]

---

[79] *Privacy Act*, R.S.C., 1985, c. P-21.
[80] In Quebec, *An Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information,* R.S.Q., c. A-2.1.
[81] LAWSON Philippa et al, "On the Data Trail: How detailed information about you gets into the hands of organizations with whom you have no relationship," Canadian Internet Policy and Public Interest Clinic, p. 8, <www.cippic.ca> [cited 15 mars 2007].
[82] Canadian Red Cross, *Policy on the Collection, Use and Disclosure Of Personal Information,* "(…) we may exchange donor names and personal contact information with other reputable humanitarian, charitable and not-for-profit organizations for the purpose of fundraising." <http://www.croixrouge.ca/article.asp?id=010958&tid=001> [cited 4 April 2007].

Businesses in possession of personal information on consumers generally collected this data in the course of their normal business activities as retailers or service providers.[83] Whereas, many businesses retain this information strictly for internal use, others opt to sell, rent or trade it for commercial purposes, in accordance with their company's practices.

The activities of personal information agents are subject to specific oversight in the *LPRPSP*, which defines a personal information agent as *"Any person who, on a commercial basis, (...) establishes files on other persons and prepares and communicates to third parties credit reports bearing on the character, reputation or solvency of the persons to whom the information contained in such files relates (...)."*[84] In Quebec, personal information agents have a particular status and must register with *la Commission d'accès à l'information* to practice their profession (we will take a look at this question a little later). Alberta and British Columbia have also established specific provisions governing the practices of personal information agencies. Whereas, British Columbia has stipulated a variety of provisions in its *PIPA* that apply specifically to personal information agencies,[85] Alberta has opted instead to enact a distinct law.[86]

Information collection methods

Direct collection

Direct collection consists essentially of the consumer voluntarily disclosing personal information in the act of completing a form or request that requires this type of information. A number of examples of this kind of voluntary disclosure come to mind: when subscribing to a newspaper or periodical, when purchasing plane tickets, when ordering goods or services by telephone or on-line, etc. One will nevertheless note that although such disclosure is voluntary, when a consumer orders a good or service he discloses information that he would not have to reveal were he to make the same purchase in person at the merchant's place of business.

In addition to this information, which is directly disclosed by the consumer and which is essential for the purchasing of the good or service (i.e. name, address, contact information and credit card number), businesses turn to other methods to obtain additional information. Although these other methods do entail a certain degree of voluntary disclosure, they are markedly less open and far more intrusive.

Loyalty cards

Loyalty cards enable those issuing them to compile data on the consumption behaviour of their holders. A study done in 2004 by the CBC revealed that 76% of Canadian consumers possess at least one loyalty card (*Air Miles, Sears*, etc). The information that businesses acquire on consumer habits via these cards can be used to establish a portrait or psychological profile of individual consumers. This data, once compiled, can then be communicated to business partners, telemarketers, etc.

[83] LAWSON, *opinion cited,* note 81.
[84] *LPRPS*P, Art. 70.
[85] *PIPA* Art. 1(4), 9(6), 12(1)g, 15(1)g, 15(1)k, 2392)a, 23(3.1), 51 c), 52(1)iv.
[86] *Fair Trading Act*, R.S.A. 2000, c. F-2.

The holders of these cards, who present them every time they make a purchase in order to gain bonus points, discounts, etc., therefore agree to disclose to businesses who they are, what they buy and where they buy. For example, Sears issues a loyalty card which, their advertising claims, offers the right to numerous privileges as part of: *"One of the richest rewards programs in the country, allowing you to earn up to 3% of your Sears Card purchases when you redeem for a Sears Club Rewards Card."* Harmless in appearance, these loyalty cards, which are used in businesses, supermarkets, pharmacies, etc., enable the issuing business to harvest masses of information on the consumer. However, not only is the consumer not necessarily conscious of disclosing this information, he is quite likely to be unaware of its scope, which ranges from information on the status of his health, to his consumption habits, travels, alcohol consumption, the importance he accords to his image and even his sexual practices!

The information harvested in this fashion is then compiled and processed in databases, with a view to confecting a profile of each individual consumer. This information may then be used or resold to merchants, manufacturers and distributors for targeted marketing—a technique for reaching certain types of consumers apt to be interested in their products. If this type of information is invaluable to businesses purely as statistical data, one may easily imagine the value it acquires as a personalized profile associated with the consumer's contact information.

The Air Miles loyalty card, which is administered by the Loyalty Group, mentions in its privacy policy that it:

> *"collects personal information for the following purposes (...):*
> - *To communicate information and offers to Collectors, Sponsors and Suppliers;*
> - *To understand and analyse Collectors' responses, needs and preferences;*
> - *To develop, enhance, market and/or provide products and services to meet those needs."*[87] (Our underlines)

This implies, of course, that the collection of personal information and the sharing of same is not limited to the client's personal contact information, as their privacy policy clearly stipulates, but also extends to the purchases made—the purpose being to compile this data as a whole for subsequent use. Thus:

> *"With your permission, we collect Personal Information about you to:*
> - *identify you,*
> - *establish and maintain a relationship with you, and to provide you with ongoing service,*
> - *develop an understanding of your needs and eligibility for products and services and to bring you offers from Sears or its selected third party business partners."*[88]

Let's underline the use of the expression *"with your consent."* Given that Sears' privacy policy is part of its overall relationship with the customer, when a consumer applies for a Sears card he is automatically accepting its terms, i.e. he is implicitly consenting to the conditions set by the

[87] Air Miles, "The Air Miles Privacy Pledge," https://www.airmiles.ca/servlet/ContentServer?pagename=Airmiles/Visitors/Privacy [cited April 2, 2007].
[88] Sears Canada, "Your Privacy," http://www.sears.ca/gp/browse.html/ref=sc_bb_l_0_43336011_9/002-6473987-6706404?ie=UTF8&node=43339011&no=43336011&searsBrand=core&me=A10FHFRJZ0GJG3 [cited April 10, 2007].

company, including the right to collect information that can identify him and to share this information with third parties, something which would not be legally permissible without the consumer's consent. Given that this consent covers the company's activities in relation to the uses of his personal information in their entirety and that the consumer is not free to refuse any of the company's specific planned uses—uses of which, moreover, he is at no time clearly informed—it goes without saying that these methods raise far more red flags in terms of openness.

Contests, surveys, polls or forms completed when purchasing goods or services

The personal information of persons who take part in contests or surveys are often harvested and analysed by the businesses that collect them. While they may be compiled anonymously simply to assess a product's popularity, they may also be associated with individual contest/poll participants and serve as a profiling tool.

The company *CanadaSurveyPanel.com* offers the opportunity to participate in paid surveys on the Internet. An alert observer will discover the company's privacy policy by clicking on the right side of the bottom of the screen. It informs him, in small print, just what the company plans to do with the information provided by participants:

> *"Information is collected from the consumer through online forms. Applicants submit their name, address, title, e-mail address, and age along with other demographic information and optional questions chosen by the advertiser. (...) Information collected by CanadaSurveyPanel.com on behalf of advertisers is the sole property of the advertiser and is shared only with the advertiser. Each advertiser individually controls what is done with the information collected."* [89]

Therefore, if a consumer wishes to know how the information he provides by taking part in the survey may be used and retained, and with whom it may be shared, he must check the privacy policies of the advertisers—in addition to that of the polling firm.

The Publisac Company, which is owned by the Transcontinental group, is presently conducting a contest on the Internet as a means to collect personal information. Its privacy policy states that:

> *"In addition, from time to time, we may use your personal information for the following purposes:*
> - *to detect and protect Transcontinental and other third parties against error, fraud, theft and other illegal activity, and to audit compliance with Transcontinental policies and contractual obligations;*
> - *to understand your needs and preferences, including to contact and communicate with you and to conduct surveys, research and evaluations;*
> - *to obtain audited statements regarding numbers of subscribers per publication;*
> - *to engage in business transactions, including the purchase, sale, lease, merger, amalgamation or any other type of acquisition, disposal, securitization or financing involving Transcontinental;*[90]

[89] Canada Survey Panel.com, "Privacy Policy," <http://canadasurveypanel.com/?p=privacy> [cited March 20, 2007].
[90] Transcontinental Group, "Privacy Policy," <http://www.transcontinental.com/privacy.html> [cited April 5, 2007].

- *for any other purpose we may indicate to you from time to time."*

(Our underlines)

In effect, the consumer discloses his personal information, tastes, preferences, and purchasing behaviour on multiple occasions, not only during transactions, but also when participating in promotional activities. The quantity and sensitivity of the information disclosed may vary considerably from one occasion to the next. Such information is generally recorded and may be combined with information harvested via other channels so that companies may obtain even more detailed portraits of individual consumers.

Using information technologies to collect personal information

A U.S. study done in the year 2000, the Georgetown Internet Privacy Policy Survey, examined 1) to what extent commercial Internet sites collected information on their customers and 2) what type of information was collected. This survey revealed that 92.8% of the 361 sites studied collected at least one type of personal information (name, electronic address, postal address, etc.), 56.8% collected at least one type of demographic information (gender, preferences, postal code, etc.) and 56.2% collected both types of information. Finally, only 6.6% of the sites surveyed did not collect any information of either type.[91]

The development of new technologies has not only enabled increases in the uses and sizes of computer databases, as well as facilitated the access to and processing of data, it has also led to the development of a multiplicity of programs or file types that collect internet users' personal information, often without their knowledge, with a view to filling these very databases. Here, then, is an overview of the different IT techniques presently used, including a word on how they work and the types of information they collect.

Cookies

Cookies are files left on the hard disc of an Internet user when the latter visits a website. They collect certain information that is sent back to their originating site. Their life spans vary from very short (non-persistent cookies only last for the duration of the visit to their website) to several years in the case of persistent cookies. It all depends on the originating server. They may even be permanent, i.e. operational until the Internet user himself deletes them. Once a cookie has expired, the Internet user's browser will cease to send the information it contains.

Persistent cookies generally collect much more detailed information, such as the Internet user's surfing habits (i.e. sites visited, pages of interest to him). They may even go so far as to communicate the surfer's political allegiances, religion, ethnic origin, etc. While the information collected is not personal information *per se*, such information becomes personal information in a legal sense if it may be connected to an identifiable individual, for example if the Internet user has registered on the site that generated the cookie.[92] Many sites ask visitors to register before they can access the site's content or in order to make a purchase. Since in such circumstances, the Internet user will be asked to provide information on his identity, in addition to whatever other information is requested by the site, the latter information is in effect "personalized."

[91] Study cited by SMITH, opinion cited, note 25.
[92] "Les cookies démystifiés," <http://www.tactika.com/cookie/cookie5.htm>

Non-persistent cookies do not really pose any issues in terms of the protection of personal information as they only exist for the duration of the surfer's visit to the site in question. Their main purpose is to facilitate access to and surfing on the site. They are therefore deleted upon completion of the visit to the site. An example of this type of cookie is the "shopping cart," used by most sites where on-line purchases may be made. This particular cookie records the various items that the Internet user wishes to buy before he makes his payment.[93]

As for persistent cookies, they provide information to the webmaster of the Internet site that installed them, which may be consulted as soon as the Internet user makes a return visit. In effect, it is then that the cookie forwards the information that it has accumulated since the preceding visit.[94] The site's webmaster may then use this information to tailor the offers, advertising and information that will be displayed the next time the Internet user returns to the site—the object being to personalize his visit and, especially, impact his consumption behaviour.

Commission Nationale de l'Informatique et des Libertés (CNIL), on its web site, offers examples of some of the ways cookies can be used to collecti personal information :

> *« dans la rubrique de ce site intitulée « Comment déclarer vos traitements ? », vous avez la possibilité de commander des formulaires de déclaration à la CNIL en nous laissant vos coordonnées. Nous aurions pu à cette occasion déposer dans votre ordinateur un cookie contenant ces coordonnées. Libre à nous, ensuite, de faire le lien entre votre adresse IP et votre adresse postale afin de prendre connaissance de manière nominative du parcours que vous avez suivi. Tiens, vous avez consulté tel dossier thématique ! Tiens, vous avez consulté tel communiqué de presse… Nous aurions pu ainsi, à votre insu, constituer un premier profil de votre comportement, associé à vos coordonnées ! »*[95]

Persistent cookies mainly serve commercial purposes. By recording an Internet user's tastes, interests and characteristics, a business is well-placed to subsequently offer information or products that are more likely to interest him, and to target its advertising with greater precision.

The celebrated retailer *Amazon*, for example, uses both types of cookies. In its "Privacy Notice," *Amazon.ca* states the following regarding the list of information that it automatically collects and analyses:

> *"Examples of the information we collect and analyze include the Internet protocol (IP) address used to connect your computer to the Internet; login; e-mail address; password; computer and connection information, such as browser type, version and timezone setting, browser plug-in types and versions, operating system, and platform; purchase history, which we sometimes aggregate with similar information from other customers to create features such as Bestseller Lists; the full Uniform Resource Locators (URL) clickstream to, through, and from our Web site, including date and time; cookie number;*

[93] FORTIER, Caroline, "Les cookies, le profilage et les intrusions dans la vie privée," <http://www.lexum.umontreal.ca/cours/internet2000/forc/forc.html> [cited 18 mars 2007].
[94] ROUILLÉ-MIRZA, Ségolène, *Les collectes de données personnelles à l'insu des internautes* (2001), dissertation in Multimedia and Information Technologies Law, Université Panthéon-Assas - Paris II, p. 8.
[95] Commission Nationale de l'Informatique et des Libertés « vos traces » Les cookies, [http://www.cnil.fr/index.php?id=170 [cited March 30, 2007].

> *products you viewed or searched for; and the telephone number used to call our customer service number."*[96]

In addition to the above types of information, other information is voluntarily disclosed by the consumer. *Amazon.ca*'s "Privacy Notice" states in this regard that:

> *"You provide most such information when you search, buy, post, participate in a contest or questionnaire, or communicate with customer service. (…) As a result of those actions, you might supply us with such information as your name, address, and telephone number; credit card information; names of people to whom purchases have been shipped, including address and telephone number; names of people (with addresses and telephone numbers) listed in 1-Click settings; content of reviews and e-mails to us; and financial information."*[97]

When one sums up voluntarily disclosed information with the information collected using digital techniques, it's clear that the total amount of information collected can be quite considerable. Moreover, although the Internet user may set his browser to not accept cookies, certain sites simply do not permit access for users that refuse cookies. Most sites recommend that users accept cookies to "enhance" their visit to the site. *Amazon.ca*, for example, makes a pretty good case:

> *"(…) cookies allow you to take full advantage of some of Amazon.ca's coolest features, and we recommend you leave them turned on."*[98]

Likewise, Ticketpro makes a similar suggestion:

> *"Cookies are used to make personalized content available while safeguarding your password to protect your personal and financial information. Cookies can be de-activated with the 'Help' command. However you may not always be able to access the de-activation feature in certain parts of the Site."*[99]

Malware

The Internet world is overflowing with different types of malware. For the purposes of our research, we will concentrate on the ones that collect information. Generally categorized as spyware, these programs collect information on the Internet user once they've installed themselves on his computer, without his knowledge.[100] Spyware is mainly developed either by businesses that advertise on the Internet (what spyware does is collect information on the Internet user for the purposes of on-line advertising[101]) or directly by software developers who include them in certain software programs. The latter are generally distributed free of charge on the web. They generate income through the sale of the information collected by the embedded spyware.[102] In both cases, the goal is to make a profit.

---

[96] Amazon.ca, "Privacy Notice," http://www.amazon.ca/gp/help/customer/display.html/701-8773470-7208349?ie=UTF8&nodeId=918814 [cited March 30, 2007].
[97] *Ibid.*
[98] *Ibid.*
[99] Ticketpro, "Confidentiality Policy," <http://ww1.ticketpro.ca/privacy.php> [cited April 10, 2007.)
[100] Wikipedia, "Logiciel espion," <http://fr.wikipedia.org/wiki/Logiciel_espion> [cited May 8, 2007].
[101] *Ibid.*
[102] *Ibid.*

The functioning of spyware entails a three-stage process. First, there is the installation phase: spyware will often be attached to a program downloaded and installed by the user (e.g. the music downloading software "Kazaa" contains the "cydoor" spyware program). Also, some spyware programs take advantage of security flaws in browsers to self-install. Second, comes the data collection stage (in the case of "cydoor," all searches and downloads using Kazaa are recorded). Finally, the information is sent to a third party, usually the software developer or a business.[103] Certain types of spyware (know as adware) can also automatically display advertising, which is based on the information collected and is sometimes tailored to the profile of the Internet user, as revealed by his surfing history and habits.

Different spyware programs collect different types of information, including logs of the websites visited, credit card numbers, key-words typed when using search engines, the Internet user's personal information, on-line purchases, etc.[104]

Log files

Log files, collect, as their name suggests, data on connections made by the Internet user. Each site has its own log files which record the activities that take place when a surfer connects to the site. These files, analogous to a log in text format, collect, for each page visited on the site in question, certain types of information,[105] including the IP address of the computer logged into the site or page, its configuration, the type of browser used, the time and dates of connection, the number of pages viewed, the preceding site and the following site, etc.

Log files do not collect personal information as such because the data they record is only associated with an IP address, i.e. the anonymous number or address that is assigned to each computer that connects with the Internet. Be that as it may, the data recorded in the log of an anonymous Internet user can still be used to learn a lot about him. A striking illustration of this recently garnered much attention: a document that AOL put on-line in August 2006, listing the search requests of millions of American Internet users, alerted the public to the risks of being identified via the information in log files. While this data demonstrated that 45% of users click on the first search result displayed, it also established that one can develop a profile of any Internet user by cross-comparing log file data. In effect, the anonymous number assigned to each user made it possible to inventory every search request made over the preceding three months, to discover the key words submitted, the time and dates of these searches, and the addresses of the sites visited.

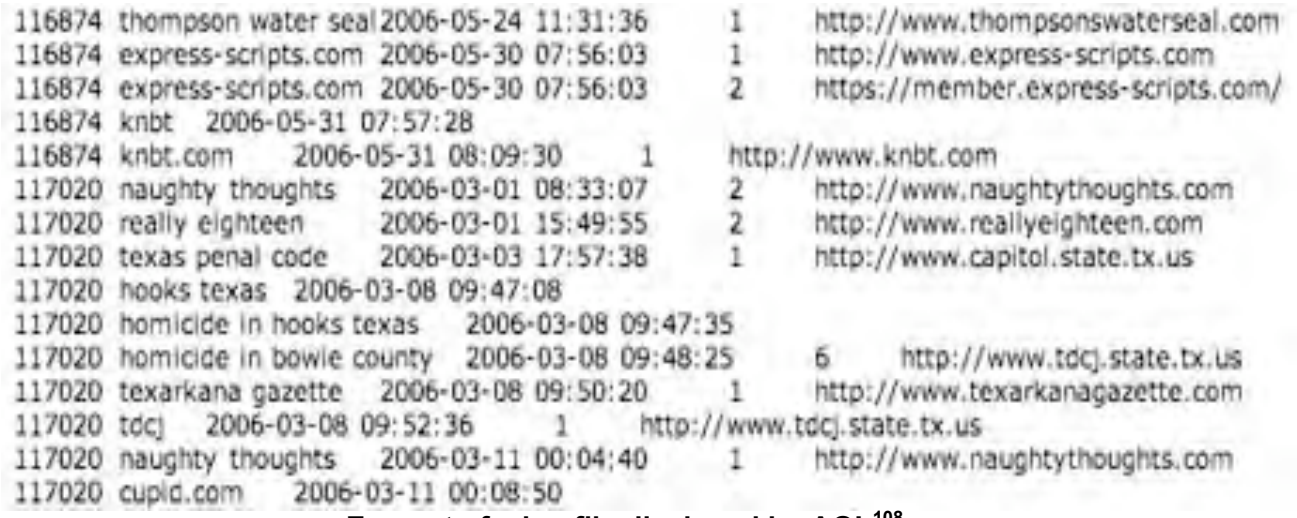
This practice has raised serious concerns due to the fact that while such data is anonymous, *"the list of searches associated with each identifier has enabled many tracers to track down Internet users, identify their social security numbers, their addresses on occasion and even their names in certain cases. Simply by observing the daily list of search requests, over several months, it's not often difficult to determine an Internet user's interests, to imagine his private life and, indeed, to discover his identity."*[106]

---

[103] Wikipedia, opinion cited, note 100
[104] *Ibid.*
[105] Adcom Internet, "les fichiers log," <http://www.adcom.fr/expertise/fichier_log.htm> [cited April 13, 2007].
[106] *Ibid.*

In effect, the log file links data to an IP address, i.e. a specific computer. As such, this data can, in particular, serve to profile individuals, as attests the exercise conducted by journalists from the Guardian who concluded the following regarding user "number 17556639":

> *"In March this year, a man with a passion for Portuguese football, living in a city in Florida, was drinking heavily because his wife was having an affair. He typed his troubles into the search window of his computer. 'My wife doesnt love animore,' he told the machine. He searched for 'Stop your divorce' and 'I want revenge to my wife' before turning to self-examination with 'alchool withdrawl,' 'alchool withdrawl sintoms' (at 10 in the morning) and 'disfunctional erection.' On April 1 he was looking for a local medium who could 'predict my futur.'"*[107]



116874	thompson water seal	2006-05-24 11:31:36	1	http://www.thompsonswaterseal.com
116874	express-scripts.com	2006-05-30 07:56:03	1	http://www.express-scripts.com
116874	express-scripts.com	2006-05-30 07:56:03	2	https://member.express-scripts.com/
116874	knbt	2006-05-31 07:57:28		
116874	knbt.com	2006-05-31 08:09:30	1	http://www.knbt.com
117020	naughty thoughts	2006-03-01 08:33:07	2	http://www.naughtythoughts.com
117020	really eighteen	2006-03-01 15:49:55	2	http://www.reallyeighteen.com
117020	texas penal code	2006-03-03 17:57:38	1	http://www.capitol.state.tx.us
117020	hooks texas	2006-03-08 09:47:08		
117020	homicide in hooks texas	2006-03-08 09:47:35		
117020	homicide in bowie county	2006-03-08 09:48:25	6	http://www.tdcj.state.tx.us
117020	texarkana gazette	2006-03-08 09:50:20	1	http://www.texarkanagazette.com
117020	tdcj	2006-03-08 09:52:36	1	http://www.tdcj.state.tx.us
117020	naughty thoughts	2006-03-11 00:04:40	1	http://www.naughtythoughts.com
117020	cupid.com	2006-03-11 00:08:50		

Excerpt of a log file disclosed by AOL[108]

As Michael Arrington put it on the TechCrunch site:

> *"The most serious problem is the fact that many people often search on their own name, or those of their friends and family, to see what information is available about them on the net. Combine these ego searches with porn queries and you have a serious embarrassment. Combine them with 'buy ecstasy' and you have evidence of a crime. Combine it with an address, social security number, etc., and you have an identity theft waiting to happen. The possibilities are endless."*[109]

It's quite clear then that data collected through digital techniques may not be, or may not remain, as anonymous or harmless as one might initially think. Clearly, determining what type of information really falls under the definition of personal information has become problematic when anonymous data may also serve to identify the person who provides it... or, one might add, from whom it is extracted.

---

[107] "Big Brother et les fichiers logs," <http://www.futura-sciences.com/news-big-brother-fichiers-log_9682.php> [cited April 13, 2007].
[108] Ibid.
[109] Tech Crunch, <http://www.techcrunch.com/2006/08/06/aol-proudly-releases-massive-amounts-of-user-search-data/> [cited April 10, 2007].

Harvesting

Address collection, better known as "harvesting," is a procedure by which e-mail addresses are automatically collected on any Internet sites where they may appear and added to a mailing list. Software has been developed to comb the Internet and record any e-mail addresses found on websites, blogs, etc. As soon as an electronic address appears on line, there's a strong chance that it will be rapidly harvested for spamming purposes and added to a list that will be put up for sale.[110]

The sale of lists of electronic addresses is now a common practice. As such lists may be used for mass mailings as well as for more precisely targeted mailings, their commercial value varies in accordance with how detailed their contact information is.[111]

"Phishing"

This rather evocative term is a neologism that combines "fishing" (perpetrators try to hook "fish" in an ocean of Internet users) and "phreaking" (a telephone fraud technique used in the 1980s).[112] Phishing consists of sending massive numbers of e-mails that appear to come from a legitimate business, in the hopes of fooling the consumer into believing that he has been contacted by a trusted third party. The e-mail will indicate, for example, that the business needs to verify certain information and ask the Internet user to provide confidential information (bank account number, password, etc.) in a return e-mail or at an internet site that faithfully reproduces the corporate design of the organization (bank, large company, etc.), which the "fish" user will be asked to visit via hyperlinks in order to record his confidential information.

One will note that it's the user and not the information system that is manipulated via phishing. That said, although this type of fraud does not depend on information technologies (such false representations may be made on the telephone as well), it's clear that the ability to effect mass electronic mailings is a great boon to the efforts of such swindlers, who can "cast" a phenomenal quantity of "lines" and sit back and wait to see if someone "bites." Moreover, the risks of being caught are also greatly reduced.

Phishing techniques are constantly being perfected and it can now be extremely difficult for consumers to spot them. In Canada, almost every financial institution has served as bait for phishing expeditions.[113] Phishers have refined their techniques and now target their mailings with greater precision. Recently, an e-mail purporting to be from the Desjardins Financial Group (written in French, by the way, a rarity in the past) asked the addressee to click on a hyperlink in the e-mail to visit a site that was a carbon-copy of the Desjardins site where he was asked to update certain personal information, if he wished to maintain his access to Desjardin's AccèsD services. Those Internet users who provided the information requested subsequently experienced the distressing surprise of finding their bank accounts empty.

---

[110] POELLHUBER David, "La sécurité du courriel ? Perspective annuelle et solutions en entreprise," <http://www.zerospam.ca/docu/le-contexte-de-la-securite-du-courriel.html> [cited March 18, 2007].
[111] For example, 2 million undifferentiated electronic addresses can be sold for 99 U.S. dollars and 100,000 addresses of AOL subscribers for 100 U.S. dollars.[111] Eric Labbé, "Le Spamming et son contrôle," December 1997, <http://www.droit.umontreal.ca/~labbee/> [cited March 26, 2007].
[112] Wikipedia, "Hameçonnage," <http://fr.wikipedia.org/wiki/Hame%C3%A7onnage> [cited April 10, 2007].
[113] *Ibid.*

Radio-frequency identification

Radio-frequency identification (RFID) makes it possible to effect remote collection and retention of information. Radio-labels, which are destined to replace bar codes on merchandise, are small objects that can be glued to or embedded in products, fabrics, or other materials, including even living beings. *"These radio-labels are comprised of an antenna attached to an electronic chip that enables them to receive and answer to radio messages sent by a transceiver."*[114] Whereas bar codes only allow the assigning of a number per type of product, with RFIDs each specific item may be given its own number. This would enable the tracing of objects at every stage: from the assembly line to the end consumer. And it would be very cost-effective to boot. [115]

Many manufacturers see this new technology as the ultimate technological solution to all traceability issues. The use of tiny electronic chips embedded in the label would, according to their advocates (naturally), make life a lot easier for consumers. In the words of Xavier Lemarteleur:

> *"Who hasn't dreamt of no longer having to line up at the supermarket because the groceries are toted up automatically by a remote sensor, or of no longer having to fumble around for bus tickets or search high and low for the car keys (a feature already offered by certain manufacturers) or the house keys? This is the world promised by the use of RFIDs."*[116]

This technology has enormous potential—and given the ingenuity of engineers the number of possible applications is guaranteed to grow by the day... a fact that raises concerns re the protection of consumers' privacy at an equally rapid clip. Radio-labels can collect and transmit a vast quantity of information about a consumer, without his knowledge. For example, a great deal of information about an individual may be gleaned simply by electronically reading the different radio-labels on his person when he enters a commercial establishment (e.g. the clothes he's wearing, the objects in his pockets or in a bag, etc.). If the receiver is strong enough, one could even envisage a quick inventory of all RFID-labelled objects inside an individual's home. Moreover, as RFIDs can also be used in different types of ID (passport, driver's licence, health insurance card, credit cards, etc.), it would be possible, at the same time, for a receiver to pick up information that serves to identify individuals. Obviously, even greater concerns arise when one realizes that anyone in possession of a receiver would be able to collect this information.

RFID technology is not very widespread and to date little personal information is collected through its use. Consequently, no further mention will be made of this technique in our study. That said, we felt it necessary to mention it since it seems likely to grow in importance in the coming years and could become a very popular technique for collecting information, including personal information.

---

[114] Wikipedia, "Radio-identification," <http://fr.wikipedia.org/wiki/Radio-identification> [cited April 17, 2007].
[115] CNIL, "Moins de 20 cents l'unité," <http://www.cnil.fr/index.php?id=1063> [cited April 17, 2007].
[116] LEMARTELEUR Xavier, "Traçabilité contre vie privée: Les RFIDs," <http://www.juriscom.net/uni/visu.php?ID=587> [cited April 16, 2007].

4. UTILIZATION OF PERSONAL INFORMATION

The collection and use of personal information by merchants is not a new practice. It existed well before the advent of the Internet. One of the first businesses to discover the commercial potential residing in consumers' personal information was the Polk Company, a publisher of business directories specializing in the sale of motor vehicles, founded in 1870 in the United States. The founder, Ralph L. Polk recorded his customers' driver's licence particulars so that he would be able to contact them in the event of a manufacturer's recall. However, he soon realized that by combining the type of vehicle bought and the date of purchase with personal information such as the name, address and age of automobile owners, he possessed information that could easily be sold to advertising firms. The latter, in turn, used this data to determine each given individual's lifestyle and income, as well as the likelihood that he would be interested in purchasing this or that product.[117]

In Canada, there exists a flourishing market for personal information. The use of such information for commercial purposes is of increasing interest to businesses intent on reaching Canadian consumers who, in 2004, spent 277 billion dollars at the retail sales level. Statistically, Canadians respond to direct sales solicitations 25% more often than Americans do. Moreover, they receive fewer such solicitations than Americans do and 84% read the ones they receive in their entirety.[118] This data is indicative of attractive and much coveted business opportunities. Consequently, businesses are mobilizing ever increasing resources to know consumers and their tastes, interests, opinions and concerns, as well as their weaknesses and vices… so as to, as they claim, better meet consumers' needs—i.e. to more successfully convince them to buy their products.

From targeted marketing to profiling

As the new technologies continue to evolve consumer behaviour has also changed rapidly. Whereas, traditionally, consumers used to go out to different stores to shop and to rent or buy a good or service, today, increasing numbers do their shopping on the Internet, in the comfort of their homes. Conscious of this reality, most businesses in Canada now have an Internet site. This new approach to consumption makes the information that businesses can gather on the Internet user, his tastes and preferences a valuable resource since it enables them to communicate information that corresponds to the consumer's wants, which also optimizes the chances of making a sale. No need to leave the house, no lining up, no crowds... the new pro-active marketing techniques used by businesses seek out the consumer in his home and lead him to buy now, rather than wait until the consumer comes to the merchant. This is the context that has seen a boom in new marketing techniques and the attendant proliferation of businesses specializing in the collection, processing and analysis of data.

---

[117] SHOLTZ, Pierre, "Economics of Personal Information Exchange," *First Monday* 5(9), <http://www.firstmonday.org/issues/issue5_9/sholtz/index.html> [cited April 4, 2007].

[118] Double Click, "Abacus Canada and Canada Post Borderfree Give Direct Marketers Access to Canada's Growing Consumer Market," *The Smart Marketing Report,* <http://www3.doubleclick.com/market/2005/02/dc/direct.htm?&c=0502_smr&id_lead=newsletter&id_source=newsletter_0502> [cited April 4, 2007].

The website of Canada Post Borderfree, a company that provides marketing services and acts as an intermediary between businesses and consumers waxes eloquent in this regard:

> *"By offering consumer segmentation tools to match the best prospects to a retailer's customer profile, circulation planning, and a series of integrated marketing campaigns and analytics, Canada Post Borderfree helps its partners find success in market expansion."*[119]

This is a new approach to marketing, made possible by the marriage of new technologies with personal information collection that is more specifically targeted and personalized—and, therefore, more effective. Whereas, on average only 6.4% of consumers open e-mail solicitations (which doesn't even guarantee that the content will be read), this climbs to over 30% when such messages are personalized.[120] Hence, the importance that merchants accord to the collecting and processing of consumers' personal information.

Whereas, certain businesses use the personal information on consumers that they collect directly in the course of their normal business activities, others do business with companies that specialize in information collection and processing. These businesses supply merchants or ad agencies with lists of potential clients, profiled in accordance with products and services, or they provide additional information on the existing clients of a business so as to enable it to develop more detailed customer profiles.

Online marketing networks, called advertising management solution, have been developed and allow companies to draw upon agencies, such as DoubleClick, to manage the ads placed on their Websites. Companies calling on DoubleClick's service allow it to collect information on their site's users through cookies. The information thus collected is more detailed and can help establish an accurate profile of the individual visitors, thereby enabling companies to place ads more likely to appeal to the site users' interests.[121]

La Commission nationale de l'informatique et des libertés (CNIL), a French agency, sees profiling as *"the capacity of computer to categorize individuals and make decisions about them, according to pre-defined characteristics or characteristics determined after a statistical study."*[122] The different items of information collected are classified in terms of "segments," in order to establish behavioural segmentation, *"a technique that enables the breakdown of an establishment's clientele into homogenous classes of clients called segments, in accordance with their observed behaviour."*[123] Targeted marketing therefore makes use of profiling to establish a general portrait of the consumer and his lifestyle, based on his consumption habits, interests, tastes, etc., in order to send him personalized advertising.

The Internet offers advertising agencies the tools needed to reach a clientele targeted in this fashion, at little expense. Networld media, a marketing agency that offers a behavioural targeting service on the Internet, provides the following example of how its service functions:

---

[119] Canada Post, Borderfree, <http://www.borderfree.net/en/business/media/releases/2005-05-17.jsp> [cited April 10, 2007].
[120] NANTEL Jacques, "La publicité Web à la croisée des chemins," *La Presse*, January 30, 2004, <http://www.inoxmedia.ca/carnet/archives/000263.html> [cited April 5, 2007].
[121] CHASSIGNEUX, Cynthia, « *La protection des informations à caractère personnel* » dans le Guide juridique du commerçant électronique, sous la direction de LABBE E., POULIN D., JACQUOT F., BOURQUE J-F., Montréal, 2001, http://www.jurisint.org/pub/05/fr/index.htm [cited June 5, 2007].
[122] Commission National de l'informatique et des libertés (CNIL), *Dix ans d'informatique et de liberté* (Economica: 1998), p. 37.
[123] ROUILLÉ-MIRZA Ségolène, opinion cited, note 94, p. 18.

> *"Jean Tremblay is looking for a new car. While shopping for his next car on-line, Jean visits certain sites specializing in automobiles on the NetWorldMedia network such as GuideAuto.com, Essais-auto.com or AutoConseils.ca, and clicks on a General Motors ad that he finds interesting.*
>
> *Once our system records at least two actions demonstrating Jean's interest in cars, he will be considered as meeting the profile "of someone in the market for an automobile". Subsequently, in the next 30 days, regardless of which of the 150 sites in the NetWorldMedia network that Jean visits, he will be exposed to more ad banners on cars made by Ford, GM, Toyota, etc."*[124]

One must not, however, confuse this type of targeting with contextual targeting which consists of displaying advertising as a function of a webpage's content rather than as a function of an Internet user's profile. Whereas, behavioural targeting analyses the past surfing patterns of an Internet user in order to show him advertising related to the various fields of interest observed, contextual targeting will only display advertising related to a particular field of interest during surfing on sites about the same area of interest. Behavioural targeting is therefore much more complex (and expensive) than contextual targeting because it requires the identification of the Internet user and the collecting of information about him via the various IT techniques described above. Adam Sohn, the Director of on-line services at Microsoft states that behavioural profiling increases the chances that an Internet user will click on an ad by 76%.[125]

Access to personal data is also offered to enterprises wishing to reach the consumer via non-virtual means. In most cases this involves lists containing the names and addresses of persons sharing common characteristics: e.g. a subscription to a certain type of magazine, response to a type of direct mail solicitation, type of credit card held, age group, etc.[126] A telephone number and/or electronic address will also often figure in the information included in such lists. The asking price for such lists depends on the data requested and the mode of delivery (diskette, CD-ROM, e-mail, etc.) and, in most cases, the price will be set in terms of a single use.[127] Rather than send the list to the company that purchased it, a personal data collection business wishing to maintain control over its lists may send the list directly to a mailout service, which will prepare and post the mailout to the persons targeted. Certain restrictions may apply to the use of such lists, such as the prohibition on offering certain products or services to minors.[128]

In the interests of compiling information that is as comprehensive as possible, companies are seeking increasingly to pool their databases. The idea is to enable the development of consumer profiles that are even more specific. DoubleClick, the biggest advertising agency on the Internet, evoked the following potential advantages of cross-referencing the data it presently possesses:

> *"As for targeting, our ideal is to know everything about everybody. We're presently trying to merge our data with Amazon.com's data. They're the leader in retail sales on the Internet. Up to now, we've known the IP addresses of computers—i.e. the number that*

---

[124] Networld Media, <http://networldmedia.net/FR/annonceurs-internet/ciblage-comportemental/ciblage-comportemental.html> [cited 13 avril 2007].
[125] J. Mintz, "Microsoft Adds Behavioral Marketing," *Associated Press,* December 27, 2006, <http://www.msnbc.msn.com/id/16370058/> [cited March 27, 2007].
[126] LAWSON et al, opinion cited, note 81, p. 9.
[127] *Ibid.*
[128] *Ibid.*

> *identifies each individual computer and locates it geographically—and users' habits. We could find out that such and such Internet user had connected x number of times at site 'y' during the last three weeks and how he got there—i.e. if he often visited sites about football, etc. With Amazon.com's database we'll also know their first and last names, addresses and telephone numbers."* [129]

Although the agreement with Amazon fell through, another one was later concluded with Abacus, a cooperative database enterprise. On its website, Abacus vaunts the value of its approach as follows:

> *"A cooperative database allows consumer activity to be viewed not from the narrow perspective of purchases made with one company but those made right across the mail order spectrum with many different organisations."*[130]

Behavioural targeting can be done based on 1) information voluntarily disclosed by the consumer in the course of normal business activities, 2) using data collected via digital techniques, or 3) by combining data obtained through both methods. Moreover, beyond advertising on the Internet, individualized digital advertising should grow in the coming years. Still in its infancy in Canada, this means of circulating advertising will make it possible to reach the consumer by relaying digital solicitations on his cellphone or to gaming consoles connected to the Internet. Neighbourhood businesses, for example, will be able to tout their specials to any passers-by, spotted via their GPS coordinates, a soon to be standard feature on cellphones.[131]

Case studies

DOUBLECLICK

Founded in 1996, DoubleClick is an American company whose main activity is Internet-based advertising. DoubleClick uses persistent cookies to build profiles of the millions of Internet users who visit websites belonging to its network. This is done without the knowledge of said web surfers. Based on the profiles identified, individualized advertising on the products of DoubleClick business partners is sent to the profilees.[132] Apparently, DoubleClick, which collects information on over 11,000 websites, amassed profiles on over 100 million Internet users between 1996 and 2000.[133] According to Media Metrix, in the month of December 1998 alone, 45.8% of Internet users in the United States visited at least one site belonging to the DoubleClick network.[134] Once a persistent cookie has been installed on the hard drive of an Internet user, it will record all subsequent surfing activity. This enables DoubleClick to trace the sites visited by a given Internet user, the searches done, and the products bought or viewed[135] in order to develop a user profile. Moreover, DoubleClick also uses cookies to discover which

---

[129] J. Boyer, "La révolution d'internet," *Petites affiches*, November 10, 1999.
[130] Abacus, <http://www.abacusalliance.com/The%5FAbacus%5FAlliance/> [cited April 4, 2007].
[131] L. Benhamou, "La publicité de l'ère numérique traque les consumers," *La Presse*, March 28, 2007, <http://www.cyberpresse.ca/article/20070328/CPACTUEL/70328065/1015/CPACTUEL> [cited March 28, 2007].
[132] FORTIER, opinion cited, note 93.
[133] *Ibid*.
[134] EPIC (Electronic Privacy Information Center) "The Cookie Page," <http://www.epic.org/privacy/internet/cookies> [cited April 3, 2007].
[135] RODGER Will, "Activists Charge DoubleClick Double Cross," *USA Today*, June 7, 2000.

advertising has been sent to an Internet user in order to avoid constantly exposing him to the same ads.[136]

Of course this monitoring of the activities of individuals for the purposes of commercial profiling raises serious privacy protection concerns. As Jason Catlett, President of Junkbuster, an organization dedicated to the fight against "privacy invading marketing," puts it:

> *"The web sites in Doubleclick's surveillance network have to disclose the fact in their privacy policies, but there's no requirement that consumers be asked to consent to Doubleclick's profiling. The vast majority of people online would want to be asked before profiles are built about them, and this should be required by law. The European Union is starting to requiring this, and for years Doubleclick's European operations have been years far less intrusive than its US ones."*[137]

In fact, DoubleClick provoked a wave of objections from privacy protection advocates when it announced its buyout of Abacus, a personal information cooperative database company. Whereas, up to that point the information collected by DoubleClick remained anonymous, it gained the capacity to connect identifiable individuals with this heretofore anonymous data by merging the databases of the two companies. In the wake of the outcry wrought by its announcement, DoubleClick made a point of reassuring the public that it had no intention of merging the personal information possessed by the two companies. Although this declaration was sufficient to reassure the Federal Trade Commission, which approved the transaction despite objections, Jason Catlett explained that, in the absence of binding standards, there were no guarantees that this merging of databanks would not go forward:

> *"DoubleClick seems to have convinced the FTC that it did not actually associate names and addresses with its previously anonymous cookies, despite the fact that this was their stated intention prior to their backdown in March. Even assuming that DoubleClick did not actually get around to matching up any of its massive stockpiles of online and offline data, they are still technically able to do so, and they continue to collect huge amounts of identified and identifiable information in ways that are unfair and unacceptable violations of privacy."*[138]

Given that Abacus' American division has a database that contains the names, addresses, credit card numbers, telephone numbers and data on the personal consumption habits of 90% of American households,[139] the precise profiling that the merging of its database with that of DoubleClick would enable, would constitute a massive intrusion into the privacy of individuals. On April 13, 2007, DoubleClick was bought out by Google (for 3.1 billion dollars[140]). That led DoubleClick CEO David Rosenblatt to comment: *"Google is the absolute perfect partner for us, combining DoubleClick's cutting edge digital solutions for both media buyers and sellers with Google's scale and innovative resources will bring tremendous value to both our employees and clients."* This development offers scant encouragement to critics.

---

[136] FORTIER, Caroline, opinion cited, note 93.
[137] CATLETT, Jason, "FTC drops investigation of DoubleClick," <http://www.junkbusters.com/new.html#DCLK> [cited April 18, 2007].
[138] *Ibid.*
[139] FORTIER Caroline, opinion cited, note 93.
[140] Press Release, "Google to acquire DoubleClick," <http://www.doubleclick.com/us/about_doubleclick/press_releases/default.asp?p=572> [cited April 18, 2007].

PERSONAL INFORMATION AGENTS

> *"Any person who, on a commercial basis, personally or through a representative, establishes files on other persons and prepares and communicates to third parties credit reports bearing on the character, reputation or solvency of the persons to whom the information contained in such files relates is a personal information agent."*[141]

Quebec's *LPRPSP* stipulates that any personal information agent that operates a business in Quebec must register in order to conduct his commercial activities. There are approximately one hundred registered personal information agents in Quebec. Among these is Equifax, one of the best known credit agencies. These businesses collect credit information and may, in particular, provide personal information to insurance companies, employers or a potential landlord, provided that the person concerned has given his consent to the person wishing to obtain such information via the services of a third party.

It would appear, based on an investigation conducted by *La facture*,[142] a public affairs program that certain agencies disclose information even when they aren't provided with proof that the applicant has obtained the necessary consent. As Odette Oger, Vice-President of Equifax Canada, explains:

> *"We receive hundreds of thousands of information requests (…). It's a fact that we don't ask for proof of consent for every transaction!"*

This investigation also revealed that personal information agencies may obtain and disclose banking information, which does not, however, appear in credit files. In effect, it seems that some employees at financial institutions provide certain agencies with information on their institution's clients in exchange for remuneration. These agencies then resell this information to their own clients. Personal information agencies and banks were not the only businesses investigated by *La facture*. Bell Canada as well was found to be at fault: provided with just a telephone number by the show's investigator, Bell disclosed the name of the subscriber, his wife's name, their address, a second telephone number, and the name of the company registered in the subscriber's name. Although Bell acknowledged that it did in fact disclose this information, it claimed that this was an isolated case.

Although the law requires prior consent from the concerned party re any collecting of his personal information, the fact that it's possible to buy personal information on others without too much trouble attests to this sector's importance to businesses today and to the profits at stake. The reports ordered by *La facture* as part of its investigation cost between $200 and $500 each. The type of information disclosed by personal information agents can be decisive regarding whether a business chooses to do business with a given individual. In short, it could decide to reject his products or services, in light of the information it obtains.

This investigation clearly raised grave concerns regarding the protection—and disclosure—of personal information, especially since the businesses in question are subject to tighter oversight than most businesses. Moreover, the fact that it's possible, as *La facture* demonstrated, to illegally buy personal information about an individual raises a number of questions regarding the real uses of this information by businesses and concerning respect for the laws on protecting personal information.

---

[141] *LPRPSP*, Art. 70 and subsequent articles.
[142] *La facture*, broadcast of February 13, 2007, <http://www.radio-canada.ca/actualite/v2/lafacture/niveau2_13625.shtml> [cited 17 April 2007].

Violations of the law by personal information agencies seem to be a widespread phenomenon. Although agencies conducting their activities in other provinces are not legally required to register, as is the case in Quebec, they are nevertheless subject to certain provisions of the law.[143] However, as the laws in Alberta and British Columbia only came into force in January 2004, to date no rulings have been made against these agencies by the Privacy Commissioners of these provinces.[144] On the other hand, Canada's Privacy Commissioner has heard numerous complaints about such businesses and has rendered twelve decisions favourable to plaintiffs[145]. Among the offences under the PIPEDA found substantiated by the Commissioner, eight dealt with principle 4.9 of Appendix 1 and Sections 8(3) and (5), which state that upon request, an individual shall given access to the information with due diligence[146], two dealt with violation of both principle 4.3, that states that the knowledge and consent of the individual are required for the collection, use, or disclosure of personal information and principle 4.7, which stipulates that personal information shall be protected by security safeguards appropriate to the sensitivity of the information[147], one dealt with violation of principle 4.5, which states that personal information must be retained only as long as necessary for the fulfillment of the purposes for which it was collected[148] and one dealt with violation of principle 4.10.4 which requires that organizations examine complaints and take appropriate measures if an investigation shows a complaint to be justified.[149]

[143] *PIPA* British Columbia, Art. 1, 9(6), 12(1)g, 15(1)g,k, 23(2)(3.1), 51c), 52(2), as well as the *Business Practices and Consumer Protection Act*, SBC 2004, c.2, Art.106-112; *PIPA* Alberta, Art. 1c), 14g), 17g), 20o), as well as the *Fair trading Act,* R.S.A. 2000, c.F.2, Art.3 and 43 to 51.
[144] Since the Act came into force, British Columbia's Privacy Commissioner has only made 9 rulings, (Office of the Information Privacy Commissioner for British Columbia, *Private sector - orders,* <http://www.oipcbc.org/sector_private/orders_decisions/orders_2006.htm> [cited June 1, 2007]. His counterpart in Alberta has made 12 rulings. Office of the Information Privacy Commissioner for Alberta, *Orders and Investigation Report - orders*, <http://www.oipc.ab.ca/orders/orders.cfm> [cited June 1, 2007].
[145] Complaints judged as founded by the Privacy Commissioner: Commissioner's Findings – "Summary of findings regarding *PIPEDA* cases #64, 67, 102, 124, 134, 150, 182, 187.
[146] Commissioner's Findings – "Summary of findings regarding *PIPEDA* cases *#59, 64, 67, 102, 124, 134, 187, 291*
[147] Commissioner's Findings – "Summary of findings regarding *PIPEDA* cases *#150 et 317*
[148] Commissioner's Findings – "Summary of findings regarding *PIPEDA* cases *#326*
[149] Commissioner's Findings – "Summary of findings regarding *PIPEDA* cases *#182*

ANALYSIS OF THE LEGALITY OF CERTAIN BUSINESS PRACTICES

The consumer's consent to the collection and disclosing of his personal information is at the heart of the laws enacted to ensure the protection of this type of information, as it is only through such consent that the consumer may retain a certain control over its circulation. It is therefore important to evaluate to what extent the businesses to which the consumer discloses his personal information—voluntarily or not—comply with their legal obligations to obtain consent when they collect, use or disclose such information.

In our examination of this question, our first step was to effect an objective analysis of the on-line privacy policies of ten companies, using an analysis grid.[150] Secondly, as the issue of consent constitutes the bedrock concern of protection of personal information legislation, we took a close look at this particular aspect of privacy policies and evaluated a few of the clauses contained in them in terms of their compliance with existing legal obligations under said legislation.

One person conducted this survey between April 10 and April 20, 2007. Companies were chosen with a view to ensuring a sample group with a wide range of commercial activities. We opted for established and relatively well-known enterprises with an Internet site.

As the businesses analysed are subject to either *PIPEDA* or the *LPRPSP*, the principles that we chose to evaluate constitute the main provisions entrenched in both pieces of legislation.

Our analysis grid sought to evaluate whether the online privacy policies of the ten organizations respect the following essential principles of legislation to protect personal information:

- The consumer shall be made aware of the collection, use and disclosure of his personal information; (*PIPEDA* Principle 4.2, *LPRPSP* Art. 8; Identifying Purposes).
- The consumer may refuse his consent to the collection, use and/or communication of his personal information; (*PIPEDA* Principle 4.3, *LPRPSP* Art. 9, 12-15; Consent).
- The collection of information shall be restricted to that which is necessary for the specified purposes; (*PIPEDA* Principle 4.4, *LPRPSP* Art. 5, 9(2); Limiting Collection).
- Personal information shall only be retained for a limited period of time; (*PIPEDA* Principle 4.5, *LPRPSP* Art. 12; Limiting Use, Disclosure, and Retention).
- Safeguards exist to protect the information collected; (*PIPEDA* Principle 4.7 and LPRPSP Art. 10; Safeguards).
- The consumer may address a personal information officer to gain access to his file, lodge a complaint or to obtain any other information; (*PIPEDA* Principle 4.9 and LPRPSP Art. 27, 29: Individual Access. And *PIPEDA* Principle 4.10 and LPRPSP Art. 32-36: Challenging Compliance).
- The policy made available shall be clear and easily understood;[151] (*PIPEDA* Principle 4.8 and *LPRPSP* Art. 14: Openness).

The results grid below enabled us to evaluate the content of privacy policies and their conformity with existing legislation. As we saw above, the consumer's consent to the collection, use and disclosure of his personal information constitutes the cornerstone of federal and

[150] *Amazon.ca, Mountain Equipment Coop, 24/7 Real Media, Canadian Red Cross, Cyberpresse.ca, Ikea, Aeroplan, Admission, Air Canada, Ticketpro.*
[151] See the Results Grid below.

provincial legislation. In order to assess whether various criteria in relation to consent are respected, our first step was to verify the following points re the ten privacy policies in question: the consumer is expressly informed of the policy (point 1); explicit consent is sought ("opting-in") (point 2); the policy indicates what information will be collected, as well as its intended use and disclosure (point 3); the policy provides for the opportunity to control and/or refuse the use and disclosure of information not required for the effecting of the transaction (points 4 and 5); the policy requires a new request for consent should there be any amendment to privacy policies (the presence of a unilateral modification clause shall be considered a violation of this principle) (point 6); privacy protection of information is not subject to the undisclosed privacy policies of any third parties with which the enterprise exchanges information, business partners, etc. (point 7); the information collected is restricted to that which is required for the purposes of the transaction (point 8); indication of a time limit re the retention of information (point 9); reference to the consumer's right to access personal information about him (point 11); no payment required for the access to information procedure (point 12); mentioning of a complaint procedure in case of non-compliance with the principles governing the protection of personal information (point 13); assigning of a personal information officer who may be contacted by telephone and inclusion of his telephone number (point 10); and reference to the existence of safeguards to ensure the protection of the information collected (point 14). Finally, we assessed whether the policy as a whole seemed clear and easily understood, such that it would enable a consumer to grant free and informed consent, on the basis of its content (point 15).

Whereas, the Grid enabled an objective assessment of official privacy policies, the subsequent discussion shall highlight several examples of irregularities that we were able to identify, notably clauses that contravene existing laws, mislead the consumer or which proved erroneous or deceptive upon inspection.

Results grid

Results grid	Yes	No	Unspe-cified
1) Privacy policy is expressly brought to the consumer's attention	1	9	
2) Explicit request for consent ("opting-in"	1	9	
3) Identification of the information collected, its uses and/or intended disclosure	8		2
4) Mentioning of the right to control how one's personal information shall be used	1	8	1
5) Option to control/refuse the disclosure of personal information	1	8	1
6) Mentioning of a requirement to request the consumer's explicit consent should a new use of his personal information be envisaged		8	2
7) Personal information is not subject to any undisclosed external privacy policies	5	5	
8) Limiting of the information collected to that which is required for the purposes of the transaction	6	3	1
9) Indication of a cut-off date regarding the retention of the information collected	2	1	7
10) Mentioning of the personal information officer and his contact information (including a telephone number)*	3	7	
11) Mentioning of the possibility of consulting one's personal information**	3		7
12) Free access to one's file (or access available for a reasonable fee).	3		7
13) Mentioning of a complaint procedure	4	6	
14) Mentioning of safeguards	5		5
15) A clear and easily understood policy	1	9	

* We consider the presence of a telephone number an essential element in a privacy policy since it not only enables a consumer to lodge a complaint, but also to obtain information rapidly.

** As for the possibility of consulting of one's personal information, we believe the presence of a telephone number or access to one's personal account via the Internet is sufficient to satisfy this requirement.

Highlights

Our survey found that, as a general rule, privacy policies are not expressly brought to the consumer's attention. These policies are generally accessible via a hyperlink on the company's website. However, this link is often written in small print and is often not easy to find. Furthermore, these policies are often hard to understand and confusing. For example, they frequently suggest that such information is not collected or communicated without the consumer's consent when in fact, it may well be.

Some businesses make mandatory disclosure of personal information a condition for the conclusion of a transaction, and even for simply using their Internet site.

Half of the enterprises surveyed disclose the consumer information they collect to third parties whose privacy policies don't necessarily match their own.

All of the enterprises surveyed included a clause that provides for the possibility of a modification of their privacy policy. This opens the door to a change in the use and communication of the consumer's personal information without his being consulted. That would contravene the provisions of privacy legislation which stipulate that consent is only valid for the

purposes for which it was requested and that any change requires that the consumer be asked to renew his consent.

With a single exception, all of the enterprises surveyed presume consent rather than attempt to obtain the consumer's explicit consent.

Analysis

The nature and form of consent

As we have seen the legislation governing the protection of personal information stipulates that businesses must, except in certain specific cases,[152] obtain prior consent from the individual concerned for any collection, use or communication of personal information, as defined by such legislation. An individual may refuse to disclose any personal information not necessary for the effecting of a given transaction. Businesses may not legally make access to a good or service subject to the collection of any other type of personal information.[153]

As it happens, it appears that many businesses make the conclusion of a transaction subject to the disclosure of personal information going well beyond the required information. This practice is particularly common when a purchase is made on the Internet. *Amazon.ca*, for example, mentions that it collects the following information: the name, address, telephone number and credit card information of the person making the purchase; the name, address and telephone number of the recipient; the names, addresses and telephone numbers of the persons figuring in the Internet user's *1-clik* address book, the content of comments and e-mails sent on *Amazon*, certain financial information, IP address, user name, electronic address, *amazon.ca* password, computer and connection information (e.g. browser type and version, operating system and platform), purchase history on Amazon, the full URL clickstream to, through, and from its website (including date and time of connection). Furthermore, under *Amazon.ca* terms and conditions for using its site, it is impossible to refuse to consent to the collection, use and disclosure of personal information:

> *"By using the Amazon.ca site and the services offered through it, you agree to be bound by these conditions of use and all related policies, conditions and guidelines. If you do not agree with any of these conditions of use, you may not use the Amazon.ca site."*[154]

Protection of personal information laws also require, depending on the degree of sensitivity of the information collected, explicit consent, i.e. "opting-in." In the conclusions of an investigation,[155]—after citing *PIPEDA*'s Principle 4.3.4, which states that *"organizations must take into account the sensitivity of the information; although some information (for example, medical records and income records) is almost always considered to be sensitive, any*

---

[152] *PIPEDA,* Art.7; *LPRPSP,* Art.18 to 25; *PIPA* Alberta, Art. 14, 17, 20; *PIPA* British Columbia, Art. 12, 15, 18. See also *supra* personal information of a public nature.
[153] *PIPEDA,* Schedule 1, Principle 4.3.3; *LPRPSP,* Art. 9.
[154] Amazon.ca, "Conditions of Use," <http://www.amazon.ca/gp/help/customer/display.html/701-8773470-7208349?ie=UTF8&nodeId=918816> [cited April 13, 2007].
[155] Office of the Privacy Commissioner, "Commissioner's Findings – *PIPEDA* Case Summary #207 (2003): Cellphone company meets conditions for 'opt-out' consent," <http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030806_02_f.asp> [cited April 13, 2007].

information can be sensitive depending on the context,"—the Privacy Commissioner identified positive consent *"*as *the most appropriate and respectful form for organizations to use in any circumstances."* He then stated that, in certain cases, the use of implicit consent, which consists of presuming consent, unless the consumer advises otherwise (i.e. he "opts out"), may be justified if the following conditions are respected:

> *"1. The personal information must be clearly non-sensitive in nature and context.*
> *2. The information-sharing situation must be limited and well-defined as to the nature of the personal information to be used or disclosed and the extent of the intended use or disclosure.*
> *3. The organization's purposes must be limited and well defined, stated in a reasonably clear and understandable manner, and brought to the individual's attention at the time the personal information is collected.*
> *4. The organization must establish a convenient procedure for easily, inexpensively, and immediately opting out of, or withdrawing consent to, secondary purposes and must notify the individual of this procedure at the time the personal information is collected."* [156]

Although it does so in different terms, *la Commission d'accès à l'information* also requires that explicit consent be given (see Article 14 of the *LPRSP*).[157] *La Commission* specifies that consent is *"a deliberate act that must meet all of the following characteristics:*

- **Consent must be manifest**, meaning that it is clear, certain and indisputable.
- **Consent must be free**, meaning that it must be given without compulsion.
- **Consent must be enlightened**, meaning that it must be precise, rigorous and specific. Thus, the enterprise must indicate what information will be communicated, to whom, why and how, and what the consequences will be. The person who gives consent must be well enough enlightened regarding the communications that will be made so that he or she can render an informed judgement on the scope of the consent.
- Consent is also given for a **specific purpose** and for the **length of time needed** to achieve the purposes for which it was requested. The length of time will not necessarily be related to a number of days, months or years, but may refer to a specific event or situation."[158]

Despite the foregoing, our analysis indicates that very few organizations seek the consumer's explicit consent. Thus, out of all the privacy policies analysed, just one company (*Ikea*) adopted an active consent policy (i.e. one requiring "opting-in"). For every other enterprise, not only was consent presumed rather than patently expressed, it was quite simply impossible, during the effecting of a transaction, to withdraw one's consent, notwithstanding the fact that privacy legislation stipulates that consent must be obtained prior to or at the time personal information is collected.[159]

When it is possible, withdrawing consent requires going through complex written procedures. For example, Aeroplan mentions in its policy that:

> *"Aeroplan will not collect, use or disclose any Personal Information about a member without the consent of the member."* [160]

---

[156] *Ibid*.
[157] *LPRPSP,* Art. 14.
[158] Commission d'accès à l'information, <http://www.cai.gouv.qc.ca/index-en.html> [cited April 16, 2007].
[159] *PIPEDA,* Schedule 1, Principle 4.3.1; *LPRPSP,* Art. 1; *PIPA* British Columbia, Art. 6; *PIPA* Alberta, Art. 7(1)
[160] Aeroplan, "Privacy Policy,"
<http://www.aeroplan.com/privacy/privacy_policy/privacy.do> [cited April 16, 2007].

A little further, the policy specifies that:

> *"we will provide our members with detailed explanations of the procedures at their disposal to delete their name from the lists we exchange with our partners*[161] *(this entails completing a form on paper*[162]*)"*[163]

The Canadian Red Cross's privacy policy also imposes a written procedure for the withdrawal of consent.[164]

This procedure may contravene Quebec's *LPRPSP*, which stipulates in Article 25 that *"Any person wishing to have personal information concerning him deleted from a nominative list may, at any time, by means of a request made orally or in writing to any person holding or using the list, obtain that the information be deleted."*[165] In our opinion, as the intention of legislator was to enable the consumer to withdraw his consent whenever he should so decide, the consumer should be able to inform the merchant in a manner of his choosing, rather than have it imposed on him by the latter. Moreover, such an interpretation would ensure that the right of individuals to withdraw their consent might be more widely exercised. This is so since the requirement of a written procedure, or of any other particular procedure imposed by the merchant, could prevent many people from exercising their right to opt out.

Consent regarding the use of personal information

The requirement for consent, as defined above, applies not only to the collection, but also to any use of the information collected. In order to verify compliance with this requirement, we analysed the ways that the information collected might be used and endeavoured to determine whether valid consumer consent is obtained prior to such uses.

As mentioned above, only one company sought the consumer's explicit consent—eight of the businesses engaged in secondary uses of the information collected without obtaining positive consent.

---

[161] Aeroplan's list of partners includes airlines, hotels, car rental agencies, credit cards, telecommunications companies, insurance companies, oil companies and retailers. In total, the list contains over one hundred businesses. <http://www.aeroplan.com/earn_miles/our_partners/partner_contact_information.do> [cited April 16, 2007].

[162] We were unable to find online either the detailed explanations or the paper form mentioned by Aeroplan. The hyperlink leading to it was not functional.

[163] Aeroplan, "Privacy Policy," <http://www.aeroplan.com/privacy/privacy_policy/privacy.do> [cited April 16, 2007].

[164] *"Where a Client or Donor does not wish to have his or her name and personal contact information disclosed to other organizations as provided in this Policy, or where a Client does not wish to receive information on other services, he or she may so inform the CRCS. Notice must be in writing to the CRCS, either to the program under which such Personal Information is being collected or to the General Manager of the CRCS Zone in which the person is ordinarily resident, or to the CRCS Privacy Officer at the National Office in Ottawa."* Canadian Red Cross, Web Privacy Policy, <http://www.redcross.ca/article.asp?id=010958&tid=001> [cited April 13, 2007].

[165] *LPRPSP*, Art. 25. Both federal and provincial legislation specify that a person may withdraw consent at any time, without mentioning what form such a notification shall take. *PIPEDA*, Schedule 1, Principle 4.3.8; *PIPA* British Columbia and Alberta, Art. 9.

Aeroplan, for example, detailed its personal information collection, use and communication practices as follows:

> *"Aeroplan® and its Partners share personal information about Aeroplan® members (…) about members' preferences in order to offer and provide quality rewards, benefits, products, goods and services to members efficiently.*
> *(…) In order to offer and provide the services and privileges to which members are entitled, Aeroplan® must collect, use and disclose information in relation to its members. This information may be personal (…).*
> *(…) From time to time we may transfer personal information to our agents for processing in order to determine which members may be most interested in rewards, benefits, products, goods and services offered by Aeroplan® or its Partners.*
> *(…) Aeroplan® collects personal information for the following purposes: to have a better understanding of members' preferences, needs and interests; to allow our partners to offer our members rewards, benefits, products, goods and services under the Aeroplan® Program."*[166]

Analysis of this clause indicates that the information collected will be used and communicated for marketing purposes to Aeroplan partners, i.e. to over a hundred businesses. One will note that the phrase mentioning the transfer of information to *"our agents for processing in order to determine which members may be most interested in rewards, (…)"* seems to signify that these agents draw up members profiles for Aeroplan and its partners.

Transparent policies for informed consent

Consent shall only be informed if the person granting it understands its scope. Such consent is only possible if policies are clear and transparent, such that they enable the consumer to know and understand which information shall be collected and the uses to which it shall be put. As it happens, out of the ten privacy policies analysed, only *Mountain Equipment Coop*'s policy satisfied these criteria. Here, then, are a few examples of practices which, in our view, mislead the consumer, thus invalidating his consent.

An *Aeroplan* clause mentions the following:

> *"Personal information about members' preferences, needs and interests is used to determine which members may be most interested in products or services offered by Aeroplan® and its Partners. The information is used solely to allow Aeroplan® and its Partners to communicate offers of rewards, benefits, products, goods and services under the Aeroplan® Program that are most likely to be of interest to the members. Aeroplan® does not provide individualized profiles of individual members to Partners or third parties."*

This clause expressly indicates that the company does not communicate individualized profiles. However, two paragraphs further, Aeroplan mentions that:

> *"From time to time Aeroplan® may also provide a Partner with a list of members who meet certain general criteria (…)."*

Isn't "a list of members who meet certain general criteria" the same as a list of persons corresponding to a certain profile? The nuance between behavioural segmentation and

[166] Aeroplan, "Complete Privacy Policy,"
<http://www.aeroplan.com/privacy/privacy_policy/privacy.do> [cited April 16, 2007].

individualized profiling is, in our opinion, very slight and the formulation of these clauses is far too likely to mislead the consumer.

At *Air Canada*:
"When you book your travel or join aircanada.com, the fact of your doing so provides Air Canada with your implied consent to use your information to fulfil your request. (…) Air Canada will not use or disclose your personal information for purposes other than those for which it was collected without your explicit consent or as required by law." [167]

Thus, nowhere in its policy does Air Canada mention that it transfers the personal information it collects to other companies. Air Canada does, however, disclose this information to Aeroplan.[168] The latter, as already mentioned, communicates the information in its possession to over a hundred partners. For a consumer to be apprised of this fact he must consult Aeroplan's personal information privacy policy. It seems to us that this lack of transparency misleads the consumer as regards the use and disclosure of information about him and makes informed consent impossible.

Half of the privacy policies we studied included such third-party clauses. As a consequence, a consumer wishing to know every possible use of his information would have to read each partner's privacy policy.

Whereas, the Aeroplan site includes a list of over a hundred partners to whom it communicates personal information, other businesses have a non-exhaustive list, thus making it impossible for the consumer to know who might possibly be in possession of his information. For example, TicketPro mentions the following in its privacy policy:

> *" When you have given us personal information to make a purchase on the site, you have consented to our sharing of the information, when necessary, with agents, representatives, contractors, suppliers of services and partners to the event, such as promoters, artists, retailers, professional associations and other third parties (hereinafter referred to as 'Events Partners') connected with the ticket or the show, activity or event.*
> *It is impossible for us to offer you an individual choice of whether or not to share your personal information with Events Partners. Events Partners may use our information according to their individual policies of confidentiality. They may therefore use the information to communicate with you, or to share it with others. You must communicate directly with Events Partners to communicate your preference regarding their use of your personal information.*
>
> *Except where otherwise indicated above, Ticketpro.ca has no control over the practices regarding personal information of Events Partners or other third parties. As described above, when purchasing tickets at the Site, or when choosing to receive communications or enter contests, draws or other programs associated with third parties or their sponsors; or when filling out entry forms posted on the Site, or otherwise choosing to allow us to share your personal information with third parties according to the terms of*

[167] Air Canada, "Privacy Policy," http://www.aircanada.com/en/about/legal/privacy/policy.html [cited 15 April 2007].
[168] *Ibid. "By joining aircanada.com you automatically join Aeroplan (…). To support this, the Air Canada Family* and Aeroplan partners are required to exchange information in order to ensure that your Aeroplan account is maintained and that miles are credited and debited correctly."*

> *this confidentiality policy, you authorize Ticketpro.ca to share your personal information with Events Partners and other concerned third parties, and release Ticketpro from all responsibility concerning their actions or omissions."*[169] *(Our underlines)*

Once TicketPro has obtained the consumer's mandatory consent, the terms of this personal information disclosure policy give it and its partners *carte blanche* to use and disclose the information collected in a completely arbitrary fashion.

Limiting information collected and the period of time information may be retained

Both provincial and federal law require organizations and enterprises to 1) limit the quantity of information collected to that which is necessary for the purposes for which it is collected,[170] 2) limit the period of time that data may be retained[171] and 3) enable an individual to demand that his information be withdrawn from any list that the party that collected the information may have drawn up.[172]

Once again, the practices of certain businesses proved problematic. Aeroplan, for example, mentions that a member whose account has been inactive for three years may demand that his information be destroyed. In the absence of such a demand on the member's part, Aeroplan will retain this information for seven years. Moreover, if a member *"wishes to terminate enrollment in the Program, all the information held regarding the member by Aeroplan® is archived within sixty (60) days and retained strictly for compliance verification purposes until the three or seven year period described above has elapsed."*[173]

At Admission, one is informed that to delete one's information, one must communicate with customer service. However, the following qualification is added:

> *"Please note that deleting your account on My Account will not delete all of your contact information or other information contained on our systems, as much or all of this information will be retained to preserve records of our commercial relationship with you."*[174]

> *Federal law requires businesses to elaborate guidelines on the retention of personal information.*[175] *The Privacy Commission mentions on its website that one shall "keep personal information only as long as necessary to satisfy the purposes [and shall] destroy, erase or render anonymous information that is no longer required for an identified purpose or a legal requirement."*[176]

---

[169] Ticketpro, "Confidentiality Policy," <http://ww1.ticketpro.ca/privacy.php> [cited April 3, 2007].
[170] *PIPEDA*, Schedule 1 Principle 4.4 and ss; *LPRPSP* Art. 5; *PIPA* Alberta and British Columbia Art. 11.
[171] *PIPEDA*, Schedule 1 Principle 4.5 and ss; *LPRPSP* Art. 12; *PIPA* Alberta, Art. 35; *PIPA* British Columbia, Art. 35(2).
[172] *PIPEDA*, Schedule 1 Principle 4.3.8; *LPRPSP.* Art. 24-26; *PIPA* Alberta and British Columbia, Art. 9.
[173] Aeroplan, "Privacy Policy," opinion cited, note 166.
[174] Réseau Admission, Privacy Policy, <http://www.admission.com/html/admission/policiesPrivacy.html?&l=EN> [cited April 13, 2007].
[175] *PIPEDA*, Schedule 1, Principle 4.5.2.
[176] Office of the Privacy Commissioner, "Factsheet: Complying with the Personal Information Protection and Electronic Documents Act," <http://www.privcom.gc.ca/fs-fi/02_05_d_16_e.asp>

It's clear that a retention policy must establish the period of time that personal information will be retained.[177] In light of the existing legislative provisions and jurisprudence, it is, however, impossible to say whether the Privacy Commissioner disposes of the powers required to determine whether the planned length of retention of a given enterprise's retention policy is or is not abusive.

Provincial laws also stipulate limits on the period of time information may be retained.[178] *La Commission d'accès à l'information* specifies the following on its website: *"The file is retained as long as the object for which the information has been collected has not been accomplished."*[179] Here as well, the absence of jurisprudence on this matter makes it difficult to establish benchmarks in relation to this requirement.

The policy of the Admission Network, which refuses to delete information about an individual, is clearly in contravention of statutes. That said, one could also question the pertinence of the three or seven-year delay—following the realization of the original purpose for which information was collected—before the retention of personal data is terminated, a practice which certain businesses have adopted.

Safeguarding information

The laws on the protection of personal information legally require businesses to take measures to safeguard the personal information they collect.[180] As a consequence, a business may not absolve itself from whatever damages a person might incur should his personal information be stolen from it in the absence of reasonable safeguards. Be that as it may, many companies waive any responsibility on their part in the event of lost or stolen data.

What makes the quantity of information amassed by businesses and the length of time such is retained even more worrisome is the fact that the security in relation to its use and storage is also problematic. Thus, a recent study in Europe indicated that over half of the continent's large corporations do not encrypt their output data. And yet, 13% of the enterprises surveyed acknowledged that some of their confidential output data had been hacked in the preceding year. This study raised certain concerns regarding the true willingness of businesses to protect the confidential data they hold and communicate in a manner that contravenes legal obligations. In effect, of the businesses surveyed, *"over half (59%) eschewed data encryption, affirming that they didn't see it as commercially necessary. This shows that major sensitization efforts are still needed concerning the dangers of hacked data and the solutions available for preventing this problem."*[181]

> *"Today, it's less expensive for a business to refund clients than to put safeguards in place," claims Alain Mercier, principal consultant at Montreal's Centre for Research on Information Technologies. "It can be very expensive to implement sufficiently effective*

[177] Office of the Privacy Commissioner, Commissioner's Findings, "*PIPEDA* Case Summary #255 - Airport authority's collection and retention practices questioned," <http://www.privcom.gc.ca/cf-dc/2003/cf-dc_031224_f.asp> [cited June 1, 2007].
[178] PIPA British Columbia, Art. 35(2); PIPA Alberta, Art. 35.
[179] Commission d'accès à l'information, "FAQ – Private Enterprises: Personal files held by private enterprises," <http://www.cai.gouv.qc.ca/>
[180] *PIPEDA,* Art. 4.7 and ss; *LPRPSP*, Art 10, 11.
[181] "Les entreprises nonchalantes face aux courriels," *La Presse Affaire*, April 12, 2007, <http://technaute.lapresseaffaires.com/nouvelles/texte_complet.php?id=81,12399,0,042007,1345603.html&ref=cyberpresse> [cited April 13, 2007].

> *safeguards and even then, there would probably be some way of getting around them. What may happen is that people will lose confidence somewhat in on-line transactions," continues Mr. Mercier. "We're stretching an elastic band, but just how far we'll be able to go before restoring balance remains to be seen."*[182]

It's not easy today for consumers to find out what safeguards exist to protect their personal information since generally speaking the privacy policies of businesses make no mention of this question. In addition, let's underline the fact that businesses are under no obligation to publicly denounce any theft of personal information in their possession—as a consequence, the consumer may never even find out if personal information about him is stolen from a business.

Other considerations

In the course of our analysis, we noted a number of other problematic situations, beyond the ones directly related to the issue of consent, such as:

- At Aeroplan, any complaint or demand for an investigation will be investigated or answered within 60 days—even though the law stipulates a maximum delay of 30 days.[183]

- At two companies (La Presse and Air Canada), it was impossible to contact the privacy protection officer at the number given in the privacy policy because said number was no longer valid.

- Because they are written in small type and located at the bottom of the screen, the privacy policies on the websites of the businesses surveyed are hard to find. Moreover, these policies are often incomprehensible to the consumer, due to their length, the wording used, their lack of openness and their complexity. That practice proves quite ineffective as regard to communication quality since it requires the consumer to scroll the page to access the required document.[184]

- The lenght of the policies, the language they use, their lack of transparence and their complexity often make them incomprehensible to the consumer.

In 2003, the International Conference of Data Protection and Privacy Commissioners adopted a resolution underlining the importance for organizations to provide much more specific information on how they process and use personal information.[185] Noting that information notices are an excellent tool for informing individuals about how the personal information collected about them is used, the OECD conducted a study to analyse information notices on privacy protection. The study underlined that although 60% of people declare that they are not indifferent when it comes to these policies, most do not read them. Moreover, even when people

[182] CRAIG, Pierre, "Hameçonnage, ne soyez pas le poisson," *La facture* broadcast, November 29, 2005, <http://www.radio-canada.ca/actualite/v2/lafacture/niveau2_5811.shtml> [cited March 20, 2007].
[183] *PIPEDA* Art. 8(3); *LPRPSP,* Art. 32; *PIPA* British Columbia, Art. 53. In Alberta the maximum time allowed is 50 days: *PIPA* Alberta, Art. 54(1).
[184] GAUTRAIS, Vincent, « The color of electronic consent» 2003, University of Ottawa Law & Technology Journal, p. 189-212. https://papyrus.bib.umontreal.ca/dspace/handle/1866/1358
[185] International Conference of Data Protection and Privacy Commissioners, <http://www.privacyconference2003.org/resolution.asp> [cited April 10, 2007].

do take the time to read them, these policies are so complex, so long and written in such an arduous technical and legal language, that they retain very little of what they read. The study concluded that the policies presently circulated by companies have proven ineffective for communicating information. They are too long and repetitive, are replete with legal and financial jargon, fail to highlight the important points, and do not encourage people to read them.[186] Furthermore, the consumer who wishes to conclude a transaction via internet often proceeds thhrough that medium because he wants to save time and is looking for a speedy way. The trouble is, since reading on screen requires 25 % more time than reading from paper[187], the lenght of the privacy policies is even more problematic[188]. The study demonstrated that it would be easy to improve a privacy policy by, for example, using check boxes, signature fields, evocative titles, etc. Three quarters of the persons surveyed believed they would pay more attention to these policies if they were more effectively presented.[189]

In 2001, a group of official organizations in the United States[190] commissioned a study with two objectives: determining why consumers do not read privacy policies and formulating principles on the drafting of more effective policies.[191] This study sought to develop simplified privacy policy declarations and to measure the extent to which they are understood by consumers throughout the United States. The researchers evaluated consumer comprehension of these policies via several test cycles, conducted over a 12-month period. Content and presentation were modified with each cycle in order to obtain, by the end of the study, a prototype for an accessible and easily understood policy. One of the conclusions of this study concerned the need to put the information provided in context, so as to facilitate consumer comprehension. For example, although consumers are informed that information about them may be disclosed to third parties, most consumers have no concrete knowledge of how such practices work and how they might be affected. This study also found that complex information must be simplified to facilitate comprehension and enable informed consent.

The effect of the electronic support is not to be neglected when comprehension of the privacy policies is concerned. Many authors stressed the reduced lisibility of a screen when compared to paper[192], stating that : « *Le document écran est source de beaucoup plus d'imprécisions, d'éventuels quiproquos, encore que l'usager ne manquera pas de faire preuve, face à un document électronique, de sa désinvolture habituelle. S'il se donne la peine de « scroller » (scrolling), c'est-à-dire de faire défiler le texte, il n'absorbe pas vraiment le contenu du texte et*

[186] OECD, "Making Privacy Notices Simple : An OECD Report and recommendations", July 24, 2006, DSTI/ICCP/REG(2006)5/FINAL, p. 4, <http://appli1.oecd.org/olis/2006doc.nsf/43bb6130e5e86e5fc12569fa005d004c/a56f6b2f04871d3fc12571b5003dac3f/$FILE/JT03212215.PDF>

[187] NIELSON, Jakob, « Writing for the Web » Sun microsystem, États-Unis, http://www.sun.com/980713/webwriting/

[188] GAUTRAIS, Vincent, Opinion cited, note 184, p. 8

[189] *Ibid*.

[190] The organizations in question were: the Federal Trade Commission, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, the National Credit Union Administration, and the Securities and Exchange Commission.

[191] KLEIMANN Communication Group Inc., "Evolution of a Prototype: Financial Privacy Notice," February 28, 2006, <http://www.ftc.gov/privacy/privacyinitiatives/ftcfinalreport060228.pdf> [cited 20 mars 2007].

[192] GAUTRAIS, Vincent, Opinion cited, note 184, p. 8 ; see also NIELSON, Jakob, Opinion cited, note 187, DILLON, Andrew « Reading from paper versus screens : a critical review of the empirical littérature » (1992) 35 Ergonomics, 1297-1326

ne vas pas voir d'éventuels liens hypertextes insérés dans le texte initial, pour finir par « cliquer » sans forcément avoir pleinement conscience de ce à quoi il s'engage.»[193]

[193] GAUTRAIS, V. et MACKAAY E., « Les contrats informatiques » in Denys-Claude LAMONTAGNE, *Contrats spéciaux*, Cowansville, Yvon Blais Ed., 2001, p. 296

ADVANTAGES, DISADVANTAGES AND POSSIBLE ABUSES OF EXISTING PRACTICES

Although the virtual world of the Internet is different from the real world in that it enables instantaneous access to a sea of information and products, one mustn't forget that behind the computer screen there's also a sea of people without whom such access would be impossible. In effect, aside from connection fees (and provided one avoids pay-for-use sites), the Internet user may surf the net as he pleases without parting with one red cent. However, the Internet is not free and webmasters must use considerable ingenuity to cover the costs of operating their websites. They manage this feat largely through advertising. Advertising is the instrument that makes it possible to generate revenues for the different stakeholders, advertising agencies and merchants. The better a webmaster knows the profiles of the Internet users that visit his site, the more effective and profitable the advertising on his site will be. Website designers, hosts, Internet service providers and ad agencies all benefit from Internet advertising. The consumer is the common denominator of their attentions and, at the end of the day, the source of their revenues, by virtue not only of his purchases, but also through the information he provides, which is itself a tradable commodity.

What are the advantages to the consumer of this trade in personal information?

Profiling

Advertising men proclaim vociferously that in the end it is the consumer who benefits from the collection, exchange and sale of personal information, since these activities enable him to enjoy greater access to more information on new products and services and to receive information better tailored to his tastes and preferences, which, ultimately, may allow him to make better informed choices. Moreover, information provided by the consumer is not always traded or sold to third parties, but is often retained by the business that collected it in order to enhance a given consumer's future relations with said enterprise.

The Ritz-Carlton hotel chain, for example, retains information on its guests. The needs and choices expressed by over 500,000 guests have been recorded in the chain's information system: Customer Loyalty Anticipation Satisfaction System (CLASS). CLASS includes information on a guest's stay such as: bed size, type of pillow (feathers of foam), food ordered, etc.—in a word, every choice made by a consumer indicating his preferences. This information will serve to ensure that future stays are made more pleasant through more personalized services.[194]

Certain consumers appreciate this kind of personalizing of services and advertising, as this enhances their consumption experiences and ensures that they more closely match their tastes and expectations.[195] For example, the Internet user who frequently visits travel-related websites may be exposed to more ads on vacation packages or discounts on plane tickets, without he himself having to do additional searches. This makes it easier for the consumer to discover—

[194] O'HARROW Robert Jr. "Consumers trade privacy for lower prices," *Washington Post*, December 31, 1998, p. A-1.
[195] Ponemon Institute, Revenue Science, Chapell & Associates, September 2004.

and benefit from—offers tailored to his interests. According to a recent poll, 65% of consumers consider advertising to be less annoying or intrusive when it better matches their interests or needs.[196]

Targeted advertising is based on individual profiling. Yes, the so-called "one-to-one" personalized marketing technique does allow the consumer to receive, based on his established profile, offers that should prove of greater interest to him. However, it would be naïve to believe that the only aim of these practices is the consumer's satisfaction. The *Abacus* website notes: *"As the majority of customers are often recruited at an initial loss, it is vital that they are encouraged to purchase from you again."*[197] Thus, while the Internet is perceived as open, neutral and anonymous, the effect of profiling is to transform it into a guided and watchful instrument that makes it possible to manipulate users by choosing the content that they will be exposed to, and by providing them with limited information, as a function of their past surfing history and the needs of the advertising agency's clients.

Moreover, the explosive increase in the number of databases containing personal information raises a number of questions that go beyond the issue of the legality (or not) of the different methods in use. According to Solove:

> *"The problem with databases and the practices associated with them is that they disempowered people. They make people vulnerable by stripping them of control over their personal information. There is no diabolical motive or secret plan for domination; rather, there is a web of thoughtless decisions made by low-level bureaucrats, standardized policies, rigid routines and a way of relating to individuals and their information that often becomes indifferent to their welfare."*[198]

One of the problems decried by privacy advocates is the danger represented by the systematic recourse to personal information databases, particularly by certain businesses and even by governments, when, in fact, nothing guarantees the accuracy of the information contained in them. And yet, the use of such information can be of considerable consequence, as it can influence the granting of credit, hiring decisions, the inclusion of an individual's name on lists of terrorists or suspected criminals, etc.

In addition, consumer profiling creates different categories of consumers, i.e. those who are likely to buy and those who are not—"good" consumers and "bad" ones, a categorization that opens the door to discriminatory practices on the part of businesses. In June 1995, *la Cour de cassation* (France's Supreme Court) ruled that behavioural segmentation—defined as the attribution of characteristics to an identifiable individual based on purchasing or consumption behaviour—is in fact illegal. The cause heard by *la Cour* concerned a bank which had created categories such as "will not improve with time," "slacker," "modernist," "hard to convince," "mistrustful." In effect, each client was coded and the bank's staff given instructions on how to deal with the clients in each particular segment.[199]

Moreover, the prevalence of targeted marketing raises fears that increasingly aggressive and invasive methods will appear, particularly on the Internet. Possible examples include: making it

---

[196] *Ibid*.
[197] Abacus, <http://www.abacusalliance.com/Data%5FDriven%5FSolutions/> [cited April 15, 2007].
[198] SOLOVE D., *The Digital Person: Technology and Privacy in the Information Age* (New York: 2004), p. 1.
[199] DINANT Jean-Marc, "Les traitements invisibles sur Internet," <http://dess-droit-internet.univ-paris1.fr/bibliotheque/rubrique.php3?id_rubrique=242> [cited April 15, 2007].

impossible to access a site without first viewing an advertisement in its entirety, ads that conceal the close window function, ads activated via hidden hyperlinks, etc. The further development of IT techniques that enable targeted marketing is likely to lead businesses to increase their use... to the great displeasure of Internet users who deem pop-ups[200] three times as annoying as direct-mail solicitations and nine times more annoying than TV ads.[201] Designed to enable the marketing of the products and services that a given consumer is most likely to purchase, profiling techniques are liable to change the web, not only through the use of increasingly aggressive advertising, but also by their exploiting of the Internet user's weak points as they encourage him to over-consume.

In general, information collection techniques on the Internet constitute a violation of privacy and privacy protection laws because they collect and use information without the knowledge of the Internet user. The use of these different profiling enabling techniques has, among other things, led several organizations to denounce their non-compliance with respect for individual liberties and privacy.[202] Consequently, it's worth examining these different methods to determine whether they are beneficial to consumers.

Cookies

Initially, cookies were designed for the benefit of the Internet user: a kind of computer *aide-mémoire*, they enabled faster and more efficient surfing, especially upon an Internet user's return visits to a website. For example, thanks to a cookie, a given site would automatically appear in the surfer's preferred language, or automatically enter his user code, saving the Internet user from the bother of having to indicate his preferences every time. They also allow the webmaster to analyse the clickstream followed by visitors to his site, with a view to improving its design. Furthermore, cookies facilitate on-line shopping by recording the items (and their optional characteristics) that a consumer puts in his virtual shopping cart. Cookies that essentially record a surfer's clickstream and behaviour on a given site (e.g. number of visitors, number of visits, pages viewed, etc.), and compile information anonymously, can also serve to help the webmaster improve the site (content, form, ergonomics).

On the other hand, the use of cookies raises two main concerns from the point of view of compliance with protection of personal information legislation. Firstly, they are installed automatically on the computers of Internet users, often without their knowledge. Secondly, the Internet user has no control over the information cookies collect nor over how this information is used. In effect, sites that use cookies generally do not advise users of their presence and do not inform them of the information they collect. This means that information is collected without the Internet user's explicit consent. Moreover, although much of this information is anonymous, it may potentially be connected to an identifiable individual, if the latter has registered on the site. For example, a subscriber to an on-line magazine or newspaper must declare his identity, as must someone who shops in-line or joins a mailing list. Thus, if these sites installed persistent cookies on the user's computer, any information subsequently collected will become personal information in that it is connected to an identifiable individual. One need only consider the case

[200] "A *pop-up* is a secondary window that appears in front of the main window without being requested by the user when the latter is surfing on the Internet. " <http://fr.wikipedia.org/wiki/Fen%C3%AAtre_intruse> [cited April 15, 2007].
[201] NANTEL, Jacques, opinion cited, note 120.
[202] RISACHER, Nancy, "Le procès de l'Internet," Lamy, Droit de l'informatique et des réseaux, No.102, April 1998.

of *Amazon.ca* whose cookies collect reams of information, as we saw above. If an Internet user has already registered or has already made purchases on its site, or if he does so at some future date, Amazon.ca will be able to connect the information it collects to the user as an identifiable person, i.e. to his complete identity, including contact information (address, phone number, etc.).

Thus, while it is reasonable to believe that the information collected by non-persistent cookies is useful to the consumer in that it facilitates surfing on a site and on-line purchases, and, moreover, is not personal, it's an entirely different story when it comes to persistent cookies. In effect, the lack of user consent concerning the installation of persistent cookies on his hard drive, as well as the collection and subsequent use of information about him, result in the consumer's total loss of control over his personal information—with the attendant risks of profiling and identity theft that that may entail.

According to Jean-Marc Dinant, the major problem raised by cookies is that they:

> *"...symbolically crystallise in the social imagination the legendary inversion of the client-server paradigm. Cookies are a hard phenomenon for people to accept because they enable a faraway and even unknown site to secretly (…) use the surfer's hard drive (this happens millions of times a day on the 'net thanks to cybermarketing firms) to record coded personal data about the Internet user, which the site can retrieve and modify at will.*
>
> *With cookies it's possible to brand a given user with certain data about him—data whose significance is entirely secret. It is technically possible to include in cookies sensitive data deduced through certain answers to forms sent in the past. For example, if, via proper programming, a Holocaust denial site comes to the conclusion that a given Internet user is Jewish, it can stick a coded star on his back such that every site belonging to the same DNS family will be apprised of this fact before loading any of its pages."* [203]

Spyware

As with cookies, the primary problem with spyware is that they automatically install themselves on the Internet user's computer and collect information without the knowledge of the Internet user.[204] Software writers of spyware plead their legality by arguing that their presence is often specified, where applicable, in the user's licence of the associated downloaded program. However, very few users read these licences which are long and complex. Moreover, even when the user is notified of the spyware's presence, he is not informed about the type of information collected, nor is he informed about its future use and disclosure.

In addition to the harm that may directly result from the collecting of personal information, spyware also affects the Internet user's computer in a number of ways: it uses up RAM, it uses up space on the hard drive, it mobilizes processor resources and it negatively impacts other applications, etc.[205]

---

[203] DINANT Jean-Marc, opinion cited, note 199.
[204] Moreover, certain spyware programs are very difficult to remove. Sometimes manual deletion is impossible and a special program is required. See: "Le logiciel espion" <http://www.dataprotex.be/fr/logiciel-espion.html> [cited May 7, 2007].
[205] *Ibid.*

Considered a nuisance by one and all, spyware programs are denounced for their malicious, secretive and often illegal actions. While spyware may offer certain advantages, consumers are definitely not the beneficiaries—rather it is industry that prefers to use this technique to collect information on Internet users, which, it is feared, the latter would refuse to disclose, were an explicit request made for their personal information.

Spam

As we have already mentioned a person's electronic address is considered personal information under *PIPEDA.* Furthermore, in light of present trends in jurisprudence, the provinces that have adopted similar legislation may also eventually see a person's electronic address as such. For consumers spam is probably the most irritating use to which their personal information is put.

Defended in some quarters as equivalent to direct mail advertising or ad banners on the net, spam constitutes, according to its advocates, an environmentally friendly and economical form of advertising that is easy to delete or ignore.[206] Moreover, it lets small businesses compete with international companies by enabling them to reach a very large number of persons inexpensively.[207] And, in so doing, they introduce consumers to certain products that they would not otherwise have known about. Be that as it may, spamming can be very annoying to its target, if for no other reason than the time spent weeding out spam from one's legitimate e-mail. Moreover, spam very rarely offers products that the consumer might find interesting, as it often consists of phishing attempts or misleading advertising aimed at collecting information from the person in question and/or separating him from his money. In fact, a number of sites have been specifically created to denounce spammers[208] and several states are trying to, somehow, end this practice.[209]

Loyalty cards

With loyalty cards, the consumer is confronted with the following dilemma: if he wishes to enjoy certain advantages or benefit from certain savings, he must in exchange accept intrusions into his privacy and consent to the sharing of his personal information. These cards also raise issues in terms of information and consent: to make an informed choice, the consumer must be clearly informed as regards the nature of his consent. Consumers are divided on the gravity of the erosion of privacy engendered by this practice. While some see an intrusion into their privacy, others don't seem to believe that the collecting of information can be prejudicial. The divergent opinions expressed by two consumers in an article in the Washington Post illustrate this debate:

> *"Schafer and many other shoppers use their club cards and eagerly accept this choice. 'I'm just buying Tide and English muffins and dog food,' said Schafer, 35, who added*

[206] LABBE Eric, opinion cited, note 111.
[207] SCOTT, Richard, "The case for advertising on Usenet," <http://hamilton.htcomp.net/apt/Internet_Advertising.htm> [cited April 15, 2007].
[208] See in particular: <http://www.caspam.org/; http://eservice.free.fr/anti-spam.html>
[209] A number of spam working groups have been set up, particularly in Canada, <http://com-e.ic.gc.ca/epic/site/ecic-ceac.nsf/fr/h_gv00246f.html>, the OECD, <http://www.oecd-antispam.org/sommaire.fr.php3>, and the European Union, <http://europa.eu/scadplus/leg/fr/lvb/l24189a.htm> [cited all, April 15, 2007].

> *that she would feel foolish passing up savings that others around her get. That afternoon she saved $2.50 on her purchases and earned bonus points for more discounts later. 'Why spend a lot more money for something as boring as food?' she asked.*
>
> *Erskine, on the other hand, said she loathes the idea of a corporation sifting through the fine-grained details of something as personal as her food. As a result, on her receipt it was noted she paid an extra $10.47, or about 22 percent more for her groceries than she would have as a Safeway Club member. 'I resent having to pay extra to protect my privacy,' said Erskine, 30. 'Why should I have to give up my information to be able to get a sale item?'"*[210]

According to Robert Gellman, a privacy issues expert, it's the lack of openness around this practice that is problematic:

> *"All the marketers say, 'This benefits consumers.' And it does. But what they won't do is be honest about it. They won't explain exactly what they're doing."*[211]

In effect, the principal criticisms levelled at loyalty cards concern the impressive quantity of information that a business gathers using them, the lack of openness on how this information is used and fact that it is impossible for a consumer to enjoy the advantages that holding the card brings should he refuse, in whole or in part, to consent to the collection, use and disclosure of this information.

Period of retention and safeguarding of data

Legislation on the protection of personal information deals with the safeguarding of data and sets limits on data collection in order to minimize intrusions into privacy and the risks associated with personal information theft.

In effect, identity theft and computer fraud are increasingly common. Moreover, hackers now succeed in hacking the most sophisticated information protection systems, such as those used by financial institutions. The risks that such intrusions represent are an argument in favour of restricting not only the nature and quantity of the information stored in databases, but their period of retention as well. In effect, the greater a fraud artist's access to a large quantity of personal information on a given individual, the greater the potential scope of the fraud, especially when such information covers a long period of time. *Amazon.ca*, for example, mentions in its privacy policy that *"when you update information, we usually keep a copy of the prior version for our records."* The swindler who succeeds in obtaining this information will thus gain access to a massive quantity of personal information, including the different addresses that an individual may have had over the years.

Consequently, in light of our study's findings on the quantity of information collected on consumers and the dearth of safeguards put in place, it seems clear to us that present practices concerning the period of retention and data safeguards not only are not beneficial to the consumer, but they may very well be prejudicial to him. In effect, the ease with which information was illegally bought by the investigators of *La facture,*[212] the numerous intrusions that have taken place in the information systems of different businesses and financial

[210] O'HARROW Robert Jr., opinion cited, note 194.
[211] *Ibid*.
[212] *La facture*, Opinion cited, note 142

institutions, not to mention the keeping of out-dated or erroneous information, all create risks for the privacy of individuals, risks which are only heightened by prolonged data retention and poor safeguarding of this mass of personal information.

Cross-border data flows

Due to the absence of geographical barriers when it comes to the transmission of information, the cross-border flow of data of a personal nature is destined to become increasingly widespread. In effect, not only may a business warehouse the information it collects in databases located in another country, but a foreign company—which is not subject to Canadian law—may also collect personal information on Canadians. Precisely where personal information on consumers is stored can have a major impact on how it is managed, as protections and restrictions vary from country to country. In accordance with the principle prohibiting the extraterritoriality of laws, foreign companies are not subject to Canadian law when operating in another country. They are instead subject to the national legislation of said other country. Moreover, as businesses are under no legal obligation to retain personal information in the province or country where it was collected, many companies send this data to other countries. For example, the Admission network mentions in its privacy policy that:

> *"Your information may be transferred to and maintained in whole or in part on computer networks which may be located outside of the state, province, country or other governmental jurisdiction in which you reside, and may be stored on equipment or in facilities leased or licensed from third parties."*

Likewise, Air Canada specifies the following in its policy:

> *"You should understand that all airlines, including Air Canada, are required by new security laws in the U.S. and several other countries to give border control agencies access to passenger data. Accordingly, any information we hold about you and your travel arrangements may be disclosed to customs and immigration authorities of any country in your itinerary.*
>
> *In addition, laws in the U.S. and other countries require Air Canada and other airlines to collect "ADVANCE PASSENGER INFORMATION" consisting of passport and related information on all passengers prior to travel to or from these countries.*
>
> *Air Canada is required to provide this information to the authorized customs and immigration authorities of these countries."*[213]

Thus, when Canadians' personal information is kept in the United States or another country, it becomes much more difficult to control its use and disclosure. This very situation arose in the context of a complaint lodged against *Abica.com,* a business which offers a variety of research services on individuals and which is presently the subject of an investigation by the Privacy Commissioner of Canada. The facts of this case revealed that the company had provided a range of personal information on an individual who had been the subject of a background check, including a psychological profile that proved unfounded. Beyond the absence of consent to the collection, use and communication of information—which, moreover, sometimes proves false—the concerns raised by this case are, notably, the fact that although the Privacy Commissioner

[213] Air Canada, "Privacy Policy."
<http://www.aircanada.com/fr/about/legal/privacy/policy.html> [cited April 5, 2007].

is authorized to investigate, as the Federal Court has recognized,[214] in practice its authority is limited because, as a U.S. located company, *Abica.com* is not subject to Canadian laws and therefore cannot be compelled to testify or disclose its sources. Therefore, not only does the consumer lack any control over the disclosure of his personal information, but he also lacks control over its content. As a result, false information about him may be communicated with, potentially, deplorable consequences. It all depends on who made the information request: an employer, insurance company, government agency, ill-intentioned individual, etc.

The ease with which new technologies allow data to be transmitted call for the establishment of certain rules for the transmission of personal information beyond the borders within which this information was collected. Without such rules, it would be easy for a company to circumvent a given legislation to transmit and store its data in a country where the legislation pertaining to the protection of personal information is non-existant or permissive[215]. Beyond those considerations, companies need more and more to transfer personal information internationally to complete transactions or due to their internal working. The Quebec legislation is the only Canadian legislation to address explicitly this matter. Section 17 states :

> *17. Every person carrying on an enterprise in Québec who communicates personal information outside Québec or entrusts a person outside Québec with the task of holding, using or communicating such information on his behalf must first take all reasonable steps to ensure*
>
> *1) that the information will not be used for purposes not relevant to the object of the file or communicated to third persons without the consent of the persons concerned, except in cases similar to those described in sections 18 and 23;*
>
> *(…)*
>
> *If the person carrying on an enterprise considers that the information referred to in the first paragraph will not receive the protection afforded under subparagraphs 1 and 2, the person must refuse to communicate the information or refuse to entrust a person or a body outside Québec with the task of holding, using or communicating it on behalf of the person carrying on the enterprise.* [216]

The same obligation applies to public entities as well, through section 70,1 of the Act respecting access to documents held by public bodies:

> *70.1. Before releasing personal information outside Québec or entrusting a person or a body outside Québec with the task of holding, using or releasing such information on its behalf, a public body must ensure that the information receives protection equivalent to that afforded under this Act.*
>
> *If the public body considers that the information referred to in the first paragraph will not receive protection equivalent to that afforded under this Act, it must refuse to release the*

[214] Lawson v. Accusearch inc. (abika.com), 2007 CF 125 (CanLII).
[215] BENYEKHLEF, Karim, « Les transactions dématérialisées » Montréal, 1994, [En ligne] http://www.lexum.com/conf/ae/fr/benyekhlef.html
[216] LPRPSP art.17

> *information or refuse to entrust a person or a body outside Québec with the task of holding, using or releasing it on its behalf.* [217]

However, both PIPEDA and the PIPA in British-Columbia and Alberta remain silent on the subject. Besides, the protection provided by the Quebec legislation fail to prohibit transborder transmission of personal information or to subject it to conditions of equivalent protection[218], as do most European legislations[219]. Therefore, transborder transmission of personal data from Canada, namely to the United States where most of the Canadian personal information is exported, allows companies to circumvent Canadian standards and benefit from legislations that are clearly less binding as far as protection requirements are concerned[220].

[217] *An Act respecting access to documents held by public bodies and the Protection of personal information, , R.S.Q. c. A-2.1*, art. 70.1
[218] BENYEKHLEF, Karim, Opinion cited., note 215
[219] *Ibid.*
[220] *Ibid.*

CONCLUSIONS

This overview of the trade in personal information has highlighted the preponderance of marketing and the effects of the explosive growth in Internet use. The development of new technologies has allowed businesses to gain access to more personal information, often without the knowledge of consumers, and to expand and optimize the collection and use of information.

Our analysis of the legal framework pertaining to this type of commercial activity brought to light certain gaps in the application of legislation as well as problems in defining what constitutes personal information or the determining of which businesses or activities are subject to its provisions.

The lack of harmonization between provincial and federal laws—notably regarding certain definitions and the powers accorded to the agencies charged with enforcing the law—raises concerns re differences in the protection that may be accorded to consumer information. In effect, protection may vary in accordance with the applicable law, the province where the consumer resides or the type of business concerned. The fact that the rulings made by commissioners are only disclosed in the form of summaries can only contribute to maintaining certain ambiguities, as this precludes the comprehensive presentation of the arguments that found said rulings.

Although the industry argues that the collection, use and communication of personal information is in the consumer's interest because such activities make it possible for him to obtain discounts or to receive personalized advertising and offers, such activities may also have other purposes and may result in risks that the consumer has the right to know about and, which, moreover, he must have the opportunity to either accept or reject. However, increasingly, industry practices are giving short shrift to the issue of consent, which nevertheless constitutes the cornerstone of laws that aim to protect consumers' personal information. The absence of frank disclosure and of any request for prior consent to the collection, use and disclosure of personal information seems, unfortunately, to have become the norm. The same holds for the lack of transparency regarding such practices.

The primary goal of the standards imposed on the private sector was to ensure consumer confidence, and thus foster commerce. However, analysis seems to indicate that in practice basic principles are widely flouted. The medium term consequences of the cavalier practices of businesses are likely to be negative—and not just for the consumer, but for industry as well. In effect, consumers are liable to become mistrustful of new technologies, even to the point of shunning them, if they come to realize how the personal information gathered by businesses is used or may be used.

The collection, retention and utilization of certain types of information may in effect benefit the consumer. Possible benefits include not having to waste time repeating certain information and enabling business to offer the consumer personalized service and save money. However, the multiplication of information collection practices, the large quantity of information collected and the marketing purposes to which they are put raise many concerns. Although some of the information gathered does not correspond to the definition of personal information *per se*, the fact that the accumulation of such information could enable the establishing of a reasonably accurate profile of a given individual or that such information could possibly be connected to an identifiable individual suggests that it might be necessary to consider ensuring oversight of

every type of information that may be collected by businesses and make all information collection subject to prior consent.

Although targeted advertising makes it possible to inform a given consumer of different products and services available on the market as a function of his interests, one mustn't lose sight of the fact that the essential goal of advertising is not to inform. Advertising is produced to create needs. Its primary goal is to seduce the consumer, to lead him to seek out a good or service by manipulating him as required and by exploiting his weaknesses, all of which has been greatly facilitated by consumer profiling.

In the end, the question of who benefits from the collection of personal information is of little import, provided that this information collection is done in a transparent fashion and that it respects the fundamental principle pertaining to the collection, use and disclosure of personal information: informed consumer consent. This, then, is the challenge that must be confronted with respect to these new technologies and new practices.

RECOMMENDATIONS

Whereas, the federal government and the provinces have opted to entrust specialized agencies with the enforcement of their laws on the protection of personal information;

Whereas, the powers granted to the Privacy Commissioner under the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*) are less extensive than those granted by analogous provincial laws to the agencies charged with enforcing said laws;

Whereas, due to these differences, Canadian consumers benefit from differing degrees of protection, depending on their province of residence or the type of business concerned;

Whereas, federal legislation does not permit the Privacy Commissioner to undertake investigations on his own initiative;

Whereas, in contrast with the agencies charged with the enforcement of similar provincial laws, the rulings of the Privacy Commissioner are not legally binding;

Whereas, provincial laws stipulate fines and penalties for enterprises that contravene rules on the protection of personal information or obstruct an investigation;

Whereas, businesses, depending on their nature or the province in which a complaint is filed, are not bound to assume the same consequences should they be found in contravention of protection of personal information rules;

Union des consommateurs recommends that the federal government:

- amend *PIPEDA* with a view to granting the Privacy Commissioner monitoring powers, including the conducting of investigations on his own initiative;

- amend *PIPEDA* with a view to granting the Privacy Commissioner whatever powers are required for the exercise of his mandate, notably the power to issue any order he judges necessary to safeguard the rights of certain parties;

- amend *PIPEDA* with a view to making any ruling of the Privacy Commissioner that has the effect of ordering a party to carry out an action or to cease or abstain from carrying out an action a binding decision; and

- amend *PIPEDA* view to imposing penalties on businesses that contravene the law or obstruct an investigation.

Whereas, certain differences between provincial legislation and *PIPEDA* are apt to create uncertainty, notably with respect to which information is protected and which organizations are subject to these laws;

Whereas, due to these differences, Canadian consumers may benefit from different types of protection, depending on their province of residence or the nature of the business in question;

Union des consommateurs recommends:

- That the federal government and the governments of Quebec, Alberta and British Columbia see to the harmonization of their laws on the protection of personal information so as to ensure that these laws apply in a uniform manner to the organizations concerned, regardless of their nature or the province where they conduct business; and

- That the federal government and the governments of Quebec, Alberta and British Columbia see to the harmonization of their laws on the protection of personal information so as to dissipate any uncertainties that may exist regarding the types of information protected by their laws, such that that which is considered personal information shall enjoy equal protection, regardless of the type of organization in question or the province in which the latter has its place of business.

Whereas, protection of personal information laws were elaborated in order to strengthen consumer confidence and implement mechanisms apt to avoid the fraud and abuse that may result from the uncontrolled collection and use of this type of information;

Whereas, the rapid development of telecommunications has given rise to or improved a number of techniques for the collection, storage and processing of information;

Whereas, information on consumers has acquired commercial value thanks, notably, to profiling techniques;

Whereas, one of the essential principles governing oversight of the protection of personal information concerns an individual's consent to 1) the collecting of his information, 2) to the uses it will serve, and 3) to the communication of said information to third parties;

Whereas, consent can only be informed insofar as the individual granting it is in possession of all relevant information;

Whereas, certain information, which is not personal information *per se*, within the meaning of legislation, may be compiled and associated with protected information, without the knowledge of the individuals concerned;

Whereas, our study has identified several cases where businesses have failed in their duty to obtain prior consent for the collection, use and communication of personal information;

Whereas, the information given or made available to the individual whose consent a business must obtain often proves incomplete or difficult to understand;

Whereas, businesses rarely make an explicit effort to make their confidentiality policies known to consumers;

Union des consommateurs recommends:

- That the federal government elaborate and implement a vast public awareness campaign to inform consumers of the following:
  - Their rights under *PIPEDA*;
  - The obligations of businesses re the requirement to obtain prior consent for the collection, use and communication of personal information;
  - Business practices re the processing of personal information, particularly with respect to profiling;

- That this information campaign be elaborated and disseminated with the collaboration of consumers' rights organizations and that sufficient resources be granted these organizations to guarantee adequate participation on their part;

- That provincial governments ensure, in concert with consumers' rights organizations, the dissemination of the information elaborated for this campaign; and

- That provincial governments ensure that sufficient resources be granted these consumers' rights organizations to guarantee adequate participation on their part.

Union des consommateurs further recommends:

- That the federal government institute a working group mandated to study the oversight that should exist under protection of personal information laws regarding the various types of information that businesses are able to collect and which, without constituting personal information in the strict sense, may be assembled in such a fashion as to generate profiles of individuals;

- • That sufficient resources be granted consumer advocacy organizations to guarantee their adequate participation in this working group;

- • That the federal and provincial governments implement a vast information campaign to inform businesses of their obligations under the provisions of protection of personal information laws; and

- • That the federal and provincial governments, in collaboration with consumer advocacy organizations, elaborate a model for a comprehensive privacy policy that shall be easy to understand and easy to use, which may be made available to businesses with a view to facilitating proper consent by consumers regarding the collection, use and communication of information, which concerns them.

Finally, Union des consommateurs recommends:

- That the agencies charged with the enforcement of laws to protect personal information use the powers at their disposal to ensure that the privacy policies of businesses meet the criteria necessary to enable consumers to give their informed consent to the collection, use and communication of information pertaining to them.

MEDIAGRAPHY

LEGISLATION

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

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

Personal Information Protection Act, S.A. 2003, c. P-6.5.

Personal Information Protection Act, S.B.C. 2003, c. 63.

GOVERNMENTAL AGENCIES

Canada. Industry Canada. "Building the Information Society: Moving Canada into the 21st Century." Ottawa: 1996.

Canada. Departments of Industry and Justice. Electronic Commerce Working Group. "The Protection of Personal Information: Building Canada's Information Economy and Society. Ottawa:1998.

Canada. House of Commons Standing Committee on Access to Information, Privacy and Ethics. "Privacy Protection in Canada and the PIPEDA Review." Ottawa: 2006.

Commission d'accès à l'information.
http://www.cai.gouv.gc.ca

Debates of the House of Commons (Hansard). Volume 133, Issue 002, 2nd Session, 35th Parliament.

European Union. "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data." *Official Journal.* L 281, 23/11/1995 P. 0031 – 0050.
http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

OECD. "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data." C(80)58/Final, September 23, 1980.
http://www.oecd.org/document/53/0,3343,en_2649_201185_15589524_1_1_1_1,00.html

OECD. "Déclaration relative à la protection de la vie privée sur les réseaux mondiaux." C(98)177. October 8, 1998.
http://webdomino1.oecd.org/horizontal/oecdacts.nsf/Display/DE3F18783E4829AAC125729B00515E52?OpenDocument

OECD. *Simplifier les notices d'information sur la protection de la vie privée: rapport et recommandation de OECD*. DSTI/ICCP/REG(2006)5/FINAL, July 24, 2006.
http://appli1.oecd.org/olis/2006doc.nsf/43bb6130e5e86e5fc12569fa005d004c/a56f6b2f04871d3fc12571b5003dac3f/$FILE/JT03212215.PDF

Privacy Commissioner of Canada. *Annual Report 1984-1985*. Ottawa: Department of Supply and Services, 1985.

Privacy Commissioner of Canada. *Annual Report 1988-1989.* Ottawa: Department of Supply and Services, 1989.

Privacy Commissioner of Canada. *Annual Report 1989-1990.* Ottawa: Department of Supply and Services, 1990.

Privacy Commissioner of Canada.
http://www.privcom.gc.ca

Smith, Margaret. "Consumer protection and electronic commerce." Canada. Law and Government Division. October 20, 2000.
http://dsp-psd.tpsgc.gc.ca/Collection-R/LoPBdP/BP/prb0018-e.htm

United States Federal Trade Commission. *Privacy Online: A Report to Congress*. 1998, p. 2.
http://www.ftc.gov/reports/privacy3/priv-23a.pdf

ARTICLES

"Big Brother et les fichiers logs." *Futura-Sciences.*
http://www.futura-sciences.com/news-big-brother-fichiers-log_9682.php

"Les pourriels pullulent." *Radio-Canada* (March 20, 2007).
www.radio-Canada.ca/nouvelles/societe/2007/03/20/005-piratage-mardi.shtml

"Les entreprises nonchalantes face aux courriels." *La Presse Affaire* (April 12, 2007).
http://technaute.lapresseaffaires.com/nouvelles/texte_complet.php?id=81,12399,0,042007,1345603.html&ref=nouvelles

"Les aspirateurs d'adresse mail dans la ligne de mire de la Cour de Cassation." *Atelier juridique.*
http://www.atelier.fr/juridique/aspirateurs,adresse,mail,ligne,mire,cour,cassation-31912-21.html

"L'adresse électronique professionnelle: renseignement personnel ou information à caractère public?" *Ogilvy-Renault* (2005).
http://www.ogilvyrenault.com/fr/ResourceCenter/ResourceCenterDetails.aspx?id=897&pId=43

"Les données personnelles de 59000 personnes exposées."
http://souriez.info/article.php3?id_article=217

ADCOM INTERNET. "Les fichiers logs."
http://www.adcom.fr/expertise/fichier_log.htm

Barrigar J., Burkell J., Kerr I. "Let's Not Get Psyched Out of Privacy." *ID Trail.* http://www.idtrail.org/files/LETS_NOT_GET_PSYCHED_OUT_OF_PRIVACY%20final%5B1%5D.pdf

Benhamou, Laurence. "La publicité de l'ère numérique traque les consumers." *La Presse.* http://www.cyberpresse.ca/article/20070328/CPACTUEL/70328065/5320/CPACTUEL

Benzakour, Nadia. "La publicité sur internet et la nécessaire protection du consumer." (2004). http://www.u-paris2.fr/dess-dmi/rep_travaux/84_N.Benzakour_PSI.pdf

Boyer, Joël. "La révolution d'internet." *Petites Affiches* (November 10,1999).

Canadian Internet Policy and Public Interest Clinic (CIPPIC). "Submission to the House of Commons Standing Committee on Access to Information, Privacy and Ethics on the *Personal information Protection and Electronic Document Act* (PIPEDA)." (November 28, 2006). http://www.cippic.ca/en/projects-cases/privacy/submissions/CIPPIC_Submission_Nov06wFNs.pdf

CIPPIC. "Compliance with Canadian Data Protection Laws: Are Retailers Measuring Up?." (April 2006). http://www.cippic.ca/en/bulletin/compliance_report_06-07-06_(color)_(cover-english).pdf

Commission nationale informatique et liberté (CNIL). "La radio-identification." http://www.cnil.fr/index.php?id=1063

CNIL, A. Vitalis, F. Paoletti, H. Delahaie. *Dix ans d'informatique et de libertés.* Paris: Éd. Économica, 1988.

Delwaide, Karl and Antoine Aylwin. "Leçons tirées de dix ans d'expérience: La Loi sur la protection des personal information dans le private sector du Québec." http://www.privcom.gc.ca/information/pub/dec_050816_f.asp

Dinant, Jean-Marc. "Les traitements invisibles sur internet." http://dess-droit-internet.univ-paris1.fr/bibliotheque/rubrique.php3?id_rubrique=242

Dumerain Emilie, A. Eesterellas, E. Imani. "La répression pénale du spam." (2005). http://www.e-juristes.org/La-repression-penale-du-spam

Electronic Privacy Information Center (EPIC). "The Cookie Page." http://www.epic.org/privacy/internet/cookies

Fortier, Caroline. "Les cookies, le profilage et les intrusions dans la vie privée." http://www.lexum.umontreal.ca/cours/internet2000/forc/forc.html

Kerr, Ian. "Submission to the House of Commons Standing Committee on Access to Information, Privacy and Ethics on the *Personal Information Protection and Electronic Documents Act* (PIPEDA)." http://www.cippic.ca/en/projects-cases/privacy/submissions/IK_PIPEDA_Review_Submission_(final)_FORMATTED.pdf

Kleimann Communication Group Inc. "Evolution of a Prototype: Financial Privacy Notice." (February 28, 2006).
http://www.ftc.gov/privacyinitiatives/ftcfinalreport060228.pdf

Labbé, Éric. "Le spamming et son contrôle."
http://www2.droit.umontreal.ca/~labbee/SPAM.HTM

Lawford, John. "Consumer Privacy Under PIPEDA: How Are We Doing ?." Public Interest Advocacy Center (PIAC).
http://www.piac.ca/privacy/report_consumer_privacy_under_pipeda_how_are_we_doing+print

Lawson, Philippa et al. "On the Data Trail: How Detailed Information About you Gets Into the Hands of Organizations With Whom you Have no Relationship." Canadian Internet Policy and Public Interest Clinic.
http://www.cippic.ca

Lemarteleur, Xavier. "Traçabilité contre vie privée: Les RFIDs."
http://www.juriscom.net/uni/visu.php?ID=587

Mintz, Jessica. "Microsoft Adds Behavioral Marketing." Associated Press.
http://www.msnbc.msn.com/id/16370058/

Nantel, Jacques. "La publicité web à la croisée des chemins."
http://www.google.ca/search?hl=fr&ie=ISO-8859-1&q=nantel+publicit%E9+web&meta=

O'Harrow, Robert Jr. "Consumers Trade Privacy for Lower Prices." *Washington Post* (December 31, 1998), p.A- 1.

Poellhuber, David. "La sécurité du courriel ? perspective annuelle et solutions en entreprise."
http://www.zerospam.ca/docu/le-contexte-de-la-securite-du-courriel.html

Ponemon Institute. "Online Advertising and Privacy Survey Shows Consumers Hold Strong Preference for Targeted Advertising."
http://www.revenuescience.com/site/media/press-releases/2004/20040909.asp

Poullet, Yves. *Report on the Application of Data Protection Principles to the Worldwide Telecommunication Networks.* Consultative Committee of the Convention for the Protection of Individuals with Regars to Automatic Processing of Personnel Data. Strasburg: Council of Europe, 2004.
http://www.coe.int/t/e/legal_affairs/legal_co%2Doperation/data_protection/documents/reports_and_studies_by_experts/T-PD(2004)04_Poullet_report.pdf

Risacher, Nancy. "Le procès de l'internet," *Lamy, Droit de l'informatique et des réseaux.* No.102. April 1998.

Rodger, Will. "Activists Charge DoubleClick Double Cross." *USA Today* (June 7, 2000).
http://www.usatoday.com/life/cyber/tech/cth211.htm

Rouillé-Mirza, Ségolène. "Les collectes de données personnelles à l'insu des internautes."(2001).
http://www.u-paris2.fr/dess-dmi/rep_travaux/19_segolenerouille.pdf

Scott, Richard. “The Case for Advertising on Usenet.”
http://hamilton.htcomp.net/apt/internet_Advertising.htm

Sholtz, Paul. “Economics of Personnal Information Exchange.” *First Monday* 5(9).
http://www.firstmonday.org/issues/issue5_9/sholtz/index.html

Skok, Gavin. “Establishing a Legitimate Expectation of Privacy in Clickstream Data.” 6 Mich. Telecomm. Tech. L. Rev. 61 (2000).
http://www.mttlr.org/volsix/skok.html

Solove, Daniel. “The Digital Person: Technology and Privacy in the Information Age.” (2004)
http://docs.law.gwu.edu/facweb/dsolove/Solove-Digital-Person.htm

RADIO AND TELEVISION BROADCASTS

La Facture.

“Hameçonnage, ne soyez pas le poisson.” With Pierre Craig. November 29, 2005.
http://www.radio-canada.ca/actualite/v2/lafacture/niveau2_14348.shtml

“Victime de vol d’identité.” With Jacques Taschereau. February 13, 2007.
http://www.radio-canada.ca/actualite/v2/lafacture/niveau2_14651.shtml