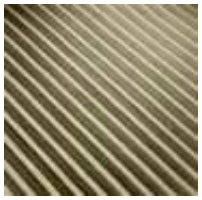
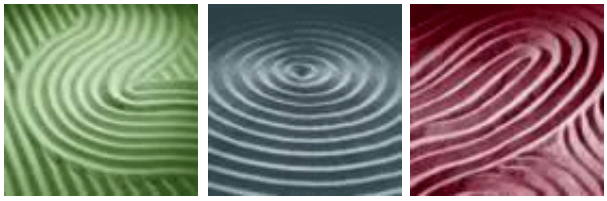


2500, 20 Queen Street West
Toronto, ON
Canada M5H 3S1
Tel. 416.595.8500
Fax. 416.595.8695
www.millerthomson.com



M I L L E R T H O M S O N L L P
Barristers & Solicitors, Patent & Trade-Mark Agents

TORONTO VANCOUVER CALGARY EDMONTON WATERLOO-WELLINGTON MARKHAM WHITEHORSE WASHINGTON, D.C.

"Please Add Me to Your Mail List" Building Customer Databases Under Canada's New Privacy Laws

by Paul D. Jones
February 19 2003

This article is provided as an information service only and is not meant as legal advice. Readers are cautioned not to act on the information provided without seeking specific legal advice with respect to their unique circumstances.
© Miller Thomson LLP 1998-2003

Table of Contents

"PLEASE ADD ME TO YOUR MAIL LIST"

Building Customer Databases under Canada's New Privacy Laws

by Paul Jones
Miller Thomson LLP

I. INTRODUCTION

The dramatic rise of e-commerce and the internet, and the increased use of computers have transformed concepts of customer goodwill. Previously the customer goodwill attached to a brand was often intangible, something that could only be estimated based on sales. Now, depending somewhat on the product, brand managers can more easily develop methods to build customer databases and focus their efforts on improving the relationship with targetted customers. Customers are not as anonymous as they once were.

While these possibilities have delighted marketing professionals, the same factors have contributed to heightened awareness and concerns amongst individuals worldwide regarding the information collected about them and its use. The first law attempting to regulate the collection and use of personal information in computer files was adopted by the German state of Hesse (the area around Frankfurt-am-Main) in 1970,[1] and the first national law was adopted by Sweden in 1973[2]. This was followed by a law in France[3] and the development of the OECD Guidelines[4].

In 1995 the Euorpean Union adopted what has come to be known as the E.U. Data Directive[5] to harmonize the national provisions within the European Union in order to facilitate transborder data flows within the Union. To ensure that the E.U. Data Directive would be effective, it provided that the transmission of personal information outside of the E.U. was only possible to countries where the law afforded similar protection to personal information. Procedures were also set out in the E.U. Data Directive for approving countries that had adequate data protection laws or for approving transfers on a case-by-case basis where data protection would be ensured by contract. As these provisions have significant implications for countries trading with the E.U., the adoption of the E.U. Data Directive has accelerated the adoption of privacy laws around the world, including in Canada.

---

[1] Now part of *Hessisches Datenschutzgesetz* (HDSG) in der Fassung vom 7 Januar 1999.

[2] *Datalagen*, SFS 1973:289

[3] *Loi No.-78-17 du 6 janvier 1978 relative á l'informatique, aux fichiers et aux libertés.*

[4] "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" as adopted by the Council of the Organization of Economic Co-operation and Development in September 23, 1980. Available on-line at www.oecd.org/dsti/sti/it/seur/prod/PRIV-EN.HIM.

[5] Directive 95/46/EC of the European Parliament and of the Council of 24 October, 1995, available on-line at http://europa.eu.int/eur-lex/en/lif/dat/1995/en_595L0046.html.

Although the common law in the United States long ago developed the tort of invasion of privacy, the federal government in the United States has not yet moved to codify general principles for the protection of personal information. The United States is the centre of the global internet industry, and many internet companies are concerned about the effect that such laws might have on their ability to develop e-commerce and internet marketing. The U.S. Federal Trade Commission reversed itself in May of 2000[6] and recommended that Congress enact legislation to ensure the adequate protection of consumer privacy on-line, because voluntary codes were not seen to be working. Since then a deadlock has developed in Congress over the type of consent that should be required for the use of personal information for marketing purposes, and the degree of access to be afforded to consumers.

There have been laws passed in the United States to protect personal information in areas where it appears to be particularly sensitive, such as video rentals[7], children[8], financial information[9], and health care information[10], and the U.S. Federal Trade Commission has developed a voluntary standard for privacy policies described as "Notice, Choice, Access and Security". The FTC has also prosecuted several internet companies under Section 5 of the *Federal Trade Commission Act* for failing to comply with their own written privacy policies as posted on their website.

A. BASIC PRINCIPLES

Different jurisdictions have developed different ways of describing or expressing the basic principles of their privacy legislation, but they all have similar elements. These elements may be described as follows:

1. Individuals must be given notice of the proposed collection, including use and disclosure, and the specific purposes.

2. In order for the data to be collected, used or disclosed, appropriate consent must be obtained with respect to the specified purposes.

3. The data collected must be protected by appropriate security.

---

[6] See Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace – A Report to Congress* (Washington, DC, Federal Trade Commission, May 22, 2000).

[7] *Video Privacy Protection Act of 1988 (the "Bork Bill")* 18 USC S.2710.

[8] *Children's Online Privacy Protection Act*, ("COPPA"), 15 U.S.C. §§6501-6506, 6502©, and 6505(d), and the *Children's Online Privacy Protection Rule,* 16 C.F.R. Part 312, in effect April, 2000.

[9] *Gramm-Leach-Bliley Act*, also known as the *Financial Services Moderization Act of 1999*, Pub. L. No. 106-102, 113 Stat. 1338 (1999), which became effective July 1, 2001.

[10] *Health Insurance Portability and Accountability Act of 1996* and the *Standards for Privacy of Individually Identifiable Health Information* (the "Privacy Rule") promulgated by the U.S. Department of Health and Hum Services as 45 CFR, Parts 1601 and 164, for compliance by April 14, 2003.

4. The individual must have access to the data collected, and to details of its use and disclosure.[11]

Variations exist in the method of ensuring compliance. In some jurisdictions registration is required in order to maintain databases of personal information and the registrar may take an activist role in ensuring compliance with the privacy principles. In other jurisdictions the primary responsibility for ensuring compliance rests with individuals through use of the courts or an administrative tribunal.

Privacy legislation is based on what might be called a "contract" model. As with contracts problems have developed with the nature of the consumer's understanding of the contract that is being proposed, the meaning of some of the terms, and the balancing of interests or fairness of the contract or consent. In traditional contract law these are often referred to as problems of "unconscionability" or "good faith". Thus significant variations are developing between jurisdictions with respect to the limitations or restrictions that they impose on privacy contracts. For example, as will be discussed later in this paper, a number of European jurisdictions prescribe various types of personal information that must be considered sensitive, and either require more explicit consent, or prohibit collection of such personal information altogether.

The United States Federal Trade Commission, as noted above, has set out its privacy principles most succinctly. In the United Kingdom the provisions of the E.U. Data Directive were summarized in eight data protection principles[12]. Canada has chosen to use ten privacy principles, adopted from the Canadian Standards Association ("CSA") Model Code[13], a voluntary code that had been developed by the private sector. A description of the ten principles is provided in Schedule A to this paper.

B. CANADA'S PRIVACY LAWS

English Canada does not have a tradition of protecting privacy. In contrast to the protections developed in civil law countries such as France, in the United Kingdom the basic common-law principle was that there is no right to privacy nor any action for invasion of privacy per se. In Canada, while the courts have never specifically stated the English position, they have been reluctant to found liability on a privacy right alone. Often, the issue has been avoided by the use of more established categories of torts.

---

[11] For an alternative discussion of the basics of fair information practices see Anne Cavoukian and Tyler J. Hamilton, *The Privacy Payoff: How Successful Businesses Build Customer Trust* (Toronto: McGraw-Hill Ryerson, 2002) at pp 44-55.

[12] See Schedule 1 of the *Data Protection Act 1998* (Chapter 29, London: The Stationery Office Ltd.). The eight principles are:) 1) personal data shall be processed fairly and lawfully; 2) personal data shall be obtained for lawful and specified purposes; 3) personal data shall be adequate, relevant and not excessive to the purposes; 4) personal data shall be relevant and kept up to date; 5) personal data shall not be retained for longer than is necessary; 6) personal data is to be processed in accordance with the rights in the legislation; 7) security measures shall be implemented; 8) personal data shall not be transferred outside the E.U. unless adequate protection is afforded.

[13] The code is now Schedule 1 of PIPEDA – "Principles Set Out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information, CAN/CSA-Q-830-96".

1. PIPEDA

Unlike the U.S., but like most of the other countries in the world, Canada has chosen to implement a general personal information protection law, the federal *Personal Information Protection and Electronic Documents Act*[14] (also known as "PIPEDA"). The objectives of the federal government were to strengthen e-commerce in Canada and to provide a legal framework that would comply with the E.U. Data Directive. Canadian companies did not appear to have the same concerns as their American counterparts, possibly because many already adhered to a voluntary code developed by the direct marketing industry and others in conjunction with the Canadian Standards Association and because Québec has had European style privacy protection since 1994.

Unfortunately privacy and personal information are not mentioned in the *Constitution Act, 1867*. While this would suggest that it is residually a provincial matter, with today's technology, much information is transferred electronically across provincial or national boundaries, which provides a basis for federal jurisdiction. Personal information and privacy are thus areas where there is often clearly overlapping federal and provincial jurisdiction, or concurrency. So long as there is no conflict between the federal and provincial laws in this area, and organization can comply with both laws, there may be no constitutional issues.

But because of Canada's constitutional division of powers the federal government was limited in the scope of the privacy law that it could enact. The provinces have exclusive jurisdiction over matters of private property and civil rights, while the federal government has a general power to regulate trade and commerce.

More importantly, the provinces, pursuant to Section 92(7)[15] of Canada *Constitution Act, 1867*, have exclusive jurisdiction over charitable and health related organizations. Accordingly the application of PIPEDA is limited to organizations and transactions within the ambit of the federal constitutional powers[16].

---

[14] S.C. 2000, c.5, as amended by S.C. 2000, c.17, s.97.

[15] *Constitution Act, 1867* (U.K.), 30 & 31 Vict., c.3, s.92(7); reprinted in R.S.C. 1985, App. II, No. 5. The provision reads as follows:

> "The Establishment, Maintenance, and Management of Hospitals, Asylums, Charities, and Eleemosynary Institutions in and for the Province, other than Marine Hospitals."

[16] Section 4(1) of PIPEDA provides that PIPEDA applies to personal information that:

i) the organization collects, uses or discloses in the course of commercial activities; or

ii) is about an employee of the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business.

The definition of the second group of organizations to which PIPEDA applies, the federal works or undertakings, is borrowed from the Canada Labour Code, and there is a significant body of case law determining whether federal or provincial labour laws apply to a particular group of employees. A quick test as to whether an organization falls into this group is to ask whether its employees are governed by federal or provincial labour law.

There is no policy basis in privacy laws for limiting their application to commercial activities and excluding hospitals and charities. Neither the E.U. Data Directive nor Québec's privacy legislation distinguish between commercial and non-commercial uses of information. As will be discussed, it is anticipated that this constitutional division of powers will make the interpretation of PIPEDA particularly problematic for marketing initiatives in the health and non-profit sectors.

Constitutional issues also led to another anomaly in the drafting of PIPEDA, namely the delay in its application to matters within a province. The federal trade and commerce power has an inherent conflict with the provincial jurisdiction over property and civil rights within a province. Initially the courts narrowed the federal trade and commerce power[17] but more recently in *General Motors v. City National Leasing*[18] established a new test for determining the appropriate exercise of the trade and commerce power by the federal government. The elements of the test were:

1. the presence of a general regulatory scheme;

2. the oversight of a regulatory agency;

3. a concern with trade as a whole, rather than with a particular industry;

4. the legislation should be of a nature that the provinces jointly or severally would be constitutionally incapable of enacting;

5. the failure to include one or more provinces or localities in a legislative scheme would jeopardize the successful operation of the scheme in other parts of the country.

As was illustrated by the concerns of the European Union with the possible avoidance of the personal information protection provided by E.U. Data Directive by the transfer of personal information outside the E.U., privacy protection in the age of computers and the internet requires legislation that deals with interprovincial and international transfers, which are the exclusive jurisdiction of the federal government. Thus condition four is satisfied, and possibly condition five. To ensure compliance with the fifth condition, the provinces were given three years to pass their own privacy legislation.

Determining the boundaries of the first group, organizations that undertake "commercial activities" is more difficult. PIPEDA defines this term as follows:

> "commercial activity" 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.

The definition appears to have been broadly drafted to specifically catch non-profit and charitable organizations trading in membership or fundraising lists.

[17] *Citizens' Insurance Co. v. Parsons* (1881) 7 App. Cas. 96. See Peter W. Hogg, *Constitutional Law of Canada – Looseleaf Edition* (Toronto: Carswell, 1997) at page 20-2 for a discussion of this case.

[18] [1989] 1 S.C.R. 641.

Another distinctive aspect of PIPEDA is that the CSA Model Code was not drafted with the precision expected in a statute. To deal with this problem, the federal government attached the CSA Model Code, without any changes or amendments, as a schedule (the "Schedule") to PIPEDA, and then included sections in PIPEDA that dealt with issues such as the application of the law, and amended the Schedule by including sections in PIPEDA that override specific provisions of the CSA Model Code.

The result has been that PIPEDA is unusually difficult to interpret. The language of the CSA Model Code, as a voluntary industry standard, is inherently vague. While some provisions, most notably the exceptions for obtaining consent, have been clarified, other important concepts, such as what is "sensitive" information, are left to the courts to determine. Even the process for seeking remedies is not clear, making it difficult to assess the risks of non-compliance. To add to the confusion, different lawyers often give differing opinions when interpreting PIPEDA. Ultimately clients will have to determine their own comfort level in difficult areas.

One of the more interesting provisions imposes limitations on the purposes for which an organization may collect, use or disclose personal information[19]. Such purposes must be ones that "... a reasonable person would consider appropriate in the circumstances." This restriction has been frequently cited by the federal Privacy Commissioner in his findings.

2. QUÉBEC

In civil matters such as privacy Québec follows the French civil code model, and the *Code civil du Québec*[20], Article 35, provides as follows:

> Art. 35 Toute personne a droit au respect de sa réputation et de sa vie privée.
>
> Nulle atteinte ne peut être portée à la vie privée d'une personne sans que celle-ci ou ses héritiers y consentent ou sans que la loi l'autorise.

Article 36 goes on to illustrate items that might be considered as invasion of the privacy of a person. They include entering or taking anything in a person's dwelling; intentionally intercepting or using the person's private communication; appropriating or using the person's image or voice while the person is in private premises; keeping the person's private life under observation by any means; using the person's name, image, likeness, or voice for a purpose other than providing legitimate information to the public; or using the person's correspondence, manuscripts or other personal documents.

To expand upon the provisions of the *Code civil*, in 1993 Québec also passed the *Loi sur la protection des renseignements personnels dans le secteur privée*[21].("Loi du

---

[19] Section 5(3).

[20] L.Q. 1991, c. 64.

[21] L.R.Q., c. P-39.1. On December 19, 2001 Bill 75, an *Act to amend the Act respecting the protection of personal information in the private sector*, was introduced in the National Assembly.

secteur privée") Under this law, there is no obligation to obtain a licence to collect personal information, however, pursuant to Section 70 of the Loi du secteur privée, every personal information agent, being the person who, on a commercial basis, personally or through a representative, establishes files on other persons, must register with the Commission d'accès à l'information du Québec. The Loi du secteur privée sets the standards with respect to the collection and use of personal information, including having a defined purpose or object; collecting only the necessary information; informing the person from whom the file is established; and obtaining consent for transferring such file to a third party.

In May, 2002 the federal Privacy Commissioner delivered a report to Parliament[22] regarding substantially similar provincial legislation and Québec's law in particular. While he found that the Loi du secteur privée is substantially similar to PIPEDA in terms of the extent to which it protects personal information, there are two important differences for marketers.

Article 22 of the Loi du secteur privée provides for the transfer to a third party, without the consent of the individuals concerned, of a "liste nominative" if by contract the third party is prohibited from using or disclosing the list for purposes other than commercial or philanthropic prospection; if the individuals have had a valid opportunity to opt-out of such transfer, and if the communication does not infringe on the privacy of the persons concerned. Nominative lists are lists of names, addresses or telephone numbers of individuals.

Care must be taken in relying upon the exemption if the source of the list would reveal significant or sensitive personal information about the individuals on the list. If the list was of persons who had visited a web site for AIDS sufferers, presumably the transfer of such list would not comply with the third condition, that the privacy of the individuals on the list not be infringed. In such circumstances consent to the communication or use of the personal information must be obtained pursuant to Art. 14 of the Loi du secteur privée. Article 14 provides that such consent must be "...manifeste, libre, éclairé et donné à des fins spécifiques." The federal Privacy Commissioner found that such requirement is at least as strong as the requirement in PIPEDA, and in practice it appears that the term "manifeste" is more likely to require explicit consent than implied consent. In other words it appears that reliance on implied consent, and thus use of "opt-out" provisions, is more restricted in Québec.

The Loi du secteur privée has been in force since January 1, 1994 and it is generally considered to be working well. On December 6, 2002 the Commission d'accès à l'information du Québec presented its 5 year report to the Québec Government[23]. Almost the entire report dealt with problems with the public sector legislation.

---

[22] The Privacy Commissioner of Canada, *Report to Parliament Concerning Substantially Similar Provincial Legislation* (Ottawa: Minister of Public Works and Government Services, 2002). The report is available online at www.privcom.gc.ca/legislation/leg-rp_e.asp.

[23] Commission d'accès à l'information du Québec, *Rapport sur la mise en oeuvre de Loi du secteur privée sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et*

3. OTHER PROVINCES

With the deadline for the application of PIPEDA within the provinces approaching, British Columbia, Alberta and possibly Manitoba are planning to introduce their own private sector privacy legislation to pre-empt the application of PIPEDA. B.C. released a consultation paper on May 13, 2002[24], and is holding a conference on privacy in mid-February.

Alberta is co-ordinating its developing of a law closely with B.C. Apparently the province hopes to introduce legislation in the Spring, launch public consultation over the summer, and pass the bill in the Fall. It appears that Manitoba has not yet commenced a consultation process.

Ontario released draft legislation for consultation in February of 2002, received numerous submissions, revised the draft, held consultations with key stakeholders again, but did not introduce the revised draft during the Fall 2002 session of the Legislature. While the official government position is that the bill will be introduced in the Spring session, there is considerable skepticism about the government's intentions[25]. If, as is anticipated by many, Ontario does not have privacy legislation passed by the Fall of 2003, PIPEDA will come into effect for "commercial activities" within the province on January 1, 2004.

But because PIPEDA's coverage is limited to that of the federal constitutional powers, large portions of the health and non-profit sectors may not be covered by privacy legislation[26]. More importantly in these sectors, many new fundraising initiatives will now be subject to a constitutional law analysis to determine the risk of PIPEDA applying to the activity.

It should also be noted that previously, to generally assist the development of a common law tort of invasion of privacy, four Canadian provinces[27] passed legislation simply providing that it is "... a tort, actionable without proof of damage, for a person, wilfully and without a claim of right, to violate the privacy of an individual". However these statutes have been rarely used. One of the reasons for this may be that in each

---

de Loi du secteur privée sur la protection des renseignements personnels dans le secteur privé (Québec: Commission d'accès à l'information du Québec, 2002). Available online at www.cai.gouv.qc.ca.

[24] "Privacy Protection in the Private Sector – British Columbia – Consultation Paper", Ministry of Management Services, Corporate Privacy and Information Access Branch, May 2002. Available online at www.mser.gov.bc.ca/foi_pop/psp/PSP-Consult.pdf.

[25] Ian Urquhart, "Why Tories are leery of privacy bill", *Toronto Star*, January 8, 2003.

[26] See the letter from Ann Cavoukian, Ontario's Information and Privacy Commissioner to Premier Ernie Eves dated December 16, 2002, lamenting the failure to introduce the privacy bill. Available online at www.ipc.on.ca/english/pubpres/reports/121602-let.htm.

[27] British Columbia in 1968, see the *Privacy Act*, R.S.B.C. 1979, c.336; Manitoba in 1970, see *The Privacy Act*, R.S.M. 1970, c.74; Saskatchewan in 1974, see *The Privacy Act*, R.S.S. 1978, c.P.24; and Newfoundland in 1981, see the *Privacy Act*, R.S.N. 1990, c.P-22. These were based in part on Sections 50 and 51 of the New York Civil Rights Law.

province actions for invasion of privacy must be brought in the superior trial court of the province, which requires significant initial expenditure by the complainant[28]. On the other hand, damages in privacy actions are uncertain. Damages are dependent on the facts in each particular case, and precise calculations in advance may be impossible.

In addition, Alberta[29] and Manitoba[30] have health specific privacy legislation in place, and Saskatchewan[31] has passed such legislation but not yet proclaimed it in force.

C. RECENT INTERNATIONAL DEVELOPMENTS

In the United States a change of administration at the federal level, and the effects of the attacks on September 11, 2001, appear to have slowed privacy developments. A visit to the website[32] of the Federal Trade Commission perhaps illustrates this trend best. Click on "Privacy Initiatives" and review the dates on the items posted. There are few items from 2002. The most significant recent FTC action was against marketers that collected extensive personal information from millions of high school students claiming that they would share the information only with educational institutions. Instead the lists were sold[33]. Otherwise much of the privacy focus in the U.S. is related to either the implementation of the HIPAA rules, or developing methods for controlling un-solicited e-mail marketing messages, known colloquially as "spam".

In Australia the effects of its adoption of private-sector privacy legislation are starting to be felt. It too was implemented in stages. The Privacy Commissioner is now starting to receive a significant volume of complaints[34].

While Japan's private-sector privacy legislation is still stuck in the Diet, Malaysia is proposing to introduce such legislation. And the People's Republic of China is changing faster than people realize. To develop the rule of law, and to develop their civil law system, China has been working for several years on the development of a Civil Code, similar to the ones used in most of Europe. On December 24, 2002 it was announced that a draft code containing nine chapters and 1,209 articles was submitted to the Standing Committee of the National People's Congress on December 23, 2002 for possible consideration when the full NPC meets in March 2003. Apparently, for the first

---

[28] See G.H.L. Fridman, *The Law of Torts in Canada, Volume 2* (Toronto: Carswell, 1990) at page 200-201; and Burns, "The Law and Privacy: The Canadian Experience" (1976), 54 C.B.R. 1 at 38.

[29] *Health Information Act*, R.S.A. 2000, c.H.5 in force April 25, 2001.

[30] *The Personal Health Information Act*, S.M. 1997, c.51-Cap. P 33.5, proclaimed in force December 11, 1997.

[31] *The Health Information Protection Act*, S.S. 1999, c.H.-0.021, not yet in force.

[32] www.ftc.gov.

[33] File No. 022-3005, *In the Matter of The National Research Center for College and University Admissions, Inc.; American Student List, LLC; and Don M. Munce*, available at www.ftc.gov/opa/2002/10/student1r.htm.

[34] Karen Dearne, "Privacy complaints deluge", *Australian IT*, January 28, 2003.

time in China, the draft code offers clear provisions on how to protect an individual's privacy[35].

Perhaps the most significant recent development is the release by the European Commission of a public consultation into the protection of personal data protection in the workplace[36] on October 31, 2002. The Data Protection Working Party, composed of representatives of the national data protection supervisory authorities, expressed considerable concern about the appropriateness of employers relying on employee's consent for collecting or using personal information. Such reliance "...should be confined to cases where the worker has a genuine free choice and is subsequently able to withdraw the consent without any detriment"[37]. In other words constraints are to be imposed on the unlimited freedom to contract with employees with respect to use of their personal information.

II. PERMISSION BASED MARKETING

Businesses have long had concerns about the effectiveness of their advertising and marketing expenditures. Using traditional methods such as flyer drops, direct mail and telemarketing a significant portion of the advertising expenditures were wasted on consumers who lived in the neighbourhood, or otherwise fit certain criteria for inclusion on a list, but who were not in the least interested in receiving the commercial messages for that product. To some extent the annoyance factor of these methods might have actually had a counter-productive effect.

The development of the internet and the spread of the use of computers have of course allowed marketers and advertisers to refine the methods that they use for selecting individual consumers to receive a particular message. And the use of e-mail has greatly reduced the costs of delivering messages, such that advertisers may find it cost effective to expect a very low response rate. As we all know, this has resulted it a deluge of unwanted e-mail messages that have been derogatively labelled as "spam".

But the development of the internet and the development of privacy laws together may hold significantly more positive promises for advertising and marketing strategies. As has been noted earlier, privacy laws are very similar to the type of regulated consumer contracts that are familiar in the sale of houses or cars. Businesses have the flexibility to collect, use and disclose an individual's personal information in a wide variety of ways, so long as they obtain the consent or permission of the individual. With many consumer contracts, there are concerns about unscrupulous businesses taking advantage of some consumer weakness. But as noted earlier, Section 5(3) of PIPEDA

---

[35] "Civil code document submitted", *China Daily*, Beijing, December 24, 2002. See also Nailene Chou Wiest, "Draft private property laws debated" *South China Morning Post*, Hong Kong, December 24, 2002, and "Private Property Owners Win with Reform", *People's Daily Online*, Beijing, December 24, 2002.

[36] See European Commission Consultation Document, "Second stage consultation of social partners on the protection of workers' personal data", October 31, 2002, available online at www.europa.eu.int/comm/employment_social/news/2002/oct/data_prot_en.pdf.

[37] *Ibid* at page 5.

limits the collection, use and disclosure of personal information to purposes that "... a reasonable person would consider appropriate in the circumstances.", and the European Union is considering similar limitations on consent with respect to employees.

But if a business is truly trying to develop a relationship with a customer, these constraints are not significant. Perceived compliance with privacy laws is a basic and necessary step in developing such relationships.

The economic potential for such relationships is very significant, not only in terms of customer loyalty, but also in the ability of the business to implement value-based pricing for different groups of customers. This has particular potential with respect to products and services delivered on-line and/or protected by copyright or patents[38]. However for consumers to participate in such a model, or in general in the internet economy, businesses will have to take into account consumer concerns regarding use of their personal information[39].

As the name implies, the key to "permission based" marketing lies in understanding the variables that go into obtaining effective and acceptable forms of consent from potential customers to form a relationship. The form of consent to be used varies dramatically depending on the sensitivity of the personal information being collected, and the purposes for which it will be collected, used or disclosed. Customers also have concerns regarding the security under which the information will be held, and their ability to access the information to monitor the relationship.

A. THE NATURE OF CONSENT

Consent in the privacy context is very much like the concept of consent with respect to the formation of contracts. There must be a meeting of the minds with respect to how the personal information will be collected, used or disclosed. In many commercial contexts such consent or agreement is evidenced by long written documents prepared by lawyers. Problems arise in commercial transactions that are routine and where the individual parties have significantly different values ascribed to the outcomes, such as, for example, a small supplier to a large automobile manufacturer.

Consumer transactions generally involve a larger proportion of less sophisticated and more vulnerable individuals than commercial transactions. Generally the ability of the vendor to come to a meeting of the minds with the consumer using long and complex written terms and conditions is limited not only by the inability of any set of terms and conditions fully foresee future developments, but also by the ability and/or willingness of the consumer to absorb all the complexities of the vendor's offer. In contract law these

---

[38] See in particular Jonathan D. Putnam, "The Economics of Digital Copyright in the Knowledge-Based Economy" a paper in progress presented at a luncheon seminar at the Centre for Innovation Law and Policy, Faculty of Law, University of Toronto, January 22, 2003. Many students expressed significant privacy concerns regarding the information about the individual's valuation of the products and services.

[39] See Europe Intelligence Wire, "Gates predicts boom, but warns on privacy, digital divide" *Computeruser.com*, February 4, 2003.

problems have led to judges trying to intervene on grounds such as unconscionability, fiduciary duty or good faith to correct perceived unfairness in the formation of the contract.

While obtaining consent under privacy laws has many of the same problems as in the formation of consumer contracts, the parameters of the variables and policy concerns are still being developed in this relatively new area of law. This, and perhaps the inherent nature of the concept of privacy, have led to concerns that privacy laws are very vague. Businesses feel frustrated when their lawyers cannot give them clear black and white answers as to whether or not a particular practice complies with the law. This was one of Ontario's criticisms of PIPEDA that was given as a reason for the drafting of an Ontario privacy law[40].

Such vagueness is not necessarily such a bad thing. While businesses are concerned that some of their practices may fall into a grey area with respect to compliance, an individual is also less likely to commence a costly court action if the chances of winning are less certain. While the consumer may complain, the most appropriate and cost-effective dispute resolution procedure for both parties in these circumstances is negotiation and mediation. And this is in fact what many Canadian privacy commissioners do.

The most significant variables to consider when obtaining consent under privacy laws are the sensitivity of the information, the purposes for which it will be used, and the security under which it will be held. These will be discussed in turn before discussing how to choose the appropriate form of consent.

B. WHAT IS "SENSITIVE INFORMATION"

The concept of "sensitive information" is important for determining the appropriate form of consent to be obtained, and the nature of the security to be used to protect the personal information. Obtaining the appropriate form of consent, either explicit or implicit, is the key to compliance with PIPEDA. If the consent is defective, then all uses of the personal information, whether it is properly protected or not, are a breach of the legislation. Further, security measures are among the more expensive requirements of PIPEDA. The choice of inappropriate provisions for security may lead to costly upgrading.

The concept of "sensitive information" is not defined in PIPEDA. However, Paragraph 4.3.4 of the Schedule states that:

> "Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context."

---

[40] Ontario Ministry of Consumer and Commercial Relations, *A Consultation Paper: Proposed Ontario Privacy Act* (Toronto: Ministry of Consumer and Commercial Relations, July 2000).

The next paragraph goes on to specify that the "reasonable expectations of the individual" are also relevant in obtaining consent, concerns about the sensitivity of different types of information vary with the culture. Differences between the attitudes of Europeans and Americans to the role of government in their lives exacerbated the negotiations over the Safe Harbour proposal for American compliance with the E.U. Data Directive. While Europeans believe that government has a duty to protect the privacy of its citizens, they find questions regarding political affiliation or ethnicity objectionable. Americans answer these questions regularly, but are sensitive about financial disclosure and have an inherent distrust of government's ability to protect their rights.

Other jurisdictions have specified certain types of information as being generally "sensitive", and built in protections, such as requirements for explicit consent or special handling. For example, the United Kingdom's *Data Protection Act, 1998* in Section 2 defines "sensitive personal data" to mean personal data consisting of information as to:

(a) the racial or ethnic origin of the data subject;
(b) his political opinions;
(c) his religious beliefs or other beliefs of a similar nature;
(d) whether he is a member of a trade union (within the meaning of the *Trade Union and Labour Relations Consolidation Act 1992*);
(e) his physical or mental health or condition;
(f) his sexual life;
(g) the commission or alleged commission by him of any offence; or
(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

Section 4 of the *Data Protection Act, 1998*, then refers to data protection principles that are set out in schedules. Schedule 3 applies only to sensitive personal data and requires that the data subject has given explicit consent to the processing of such data.

Australia has a similar list of prescribed types of sensitive information, that also includes information about the individual's "...lifestyle, character or reputation."[41] Organizations are prohibited from collecting such information unless they obtain consent. However there is an exemption for non-profit organizations that have only racial, ethnic, political, religious, philosophical, professional, trade, or trade union aims. These organizations may collect sensitive information about their members or other individuals with which they have regular contact if prior to collecting the information the organization undertakes to the individual that the information will not be disclosed without the individual's consent.

---

[41] *Privacy Amendment (Private Sector) Act 2000*, Act No. 155 of 2000, that came into force on December 21, 2001.

In the Spanish *Ley Orgánica 15/1999*[42], Article 7 sets out what is "specially protected" data. In this statute, the list is first divided according to those items, such as ideology, religion or beliefs, which are protected under the Constitution. These require the highest level of explicit consent. There is then a further category which includes data that will reveal the ideology, union affiliation, religion or beliefs, for which there are certain exceptions for the maintenance of lists by unions political parties, churches and other such groups. Personal information having reference to racial origin, health and sexual life can only be collected when for reasons of public policy, it is made possible by a law or by express consent. Finally, it is prohibited to create data files for the exclusive purpose of revealing the ideology, union affiliation, religion, beliefs, racial or ethnic origin or sexual life of an individual.

Similarly, the French *Loi No. 78-17 du 6 janvier 1978 relative á l'informatique, aux fichiers et aux libertés* in Article 31 prohibits maintenance of data files that will reveal racial origins, religious, philosophical or political opinions or union affiliations, or "... les moeurs ..." of individuals without the express agreement of the individual. However, the maintenance of membership lists by groups such as churches, political parties and unions is specifically allowed.

Section 28 of Germany's *Bundesdatenschutzgesetz*[43] sets out certain conditions for the storage, communication and use of data for an organization's own purposes. Previously some protection was given to sensitive personal information such as health matters, criminal offences, administrative offences, religious or political views and trade union status. Effective May 23, 2001 the *Bundesdatenschutzgesetz* was amended to include all of the categories of sensitive information contained in Article 8 of the E.U. Data Directive[44]. Now the collection of such data must be expressly approved by the data subject, and its processing requires a prior review by a data protection official.

From this simple survey, it is clear that many democratic countries regard information about an individual's religious, political or philosophical beliefs as being sensitive, and restrict its collection, use and disclosure.

Similar generally sensitive areas may be inferred in Canada from an examination of those rights and values that are specifically protected by law. If such rights and values have been given special protection, the collection of information about the exercise of that right or expression of that value may inhibit the exercise of the right or the expression of the value. Accordingly, the information may be considered "sensitive" as that term is used in PIPEDA. For example, to safeguard the freedom to vote according to one's own belief or conscience[45], Canada uses secret ballots. Privacy or secrecy is

---

42 *Ley Orgánica 15/1999, de 13 diciembre, de Protección de Datos de Carácter Personal.*

43 Vom 20.12.1990, BGBl. I S. 2594.

44 *Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze*, BGBl vom 22.05.2001 S.904.

45 As expressed in Sec. 3 of the *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the Canada Act, 1982 (U.K.), 1982, c.11.

considered key to the protection of the right to vote according to one's own conscience. The collection information on how people actually voted may be considered sensitive and require consent.

Section 2 of the *Canadian Charter of Rights and Freedoms*[46] provides a list of fundamental freedoms:

(a) freedom of conscience and religion;
(b) freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication;
(c) freedom of peaceful assembly; and
(d) freedom of association.

Further, Section 15(1) provides that every individual is equal before and under the law, without discrimination, including discrimination based on: race, national or ethnic origin, colour, religion, sex, age or mental or physical disability.

Any collection, use or disclosure of personal information dealing with these characteristics will most likely be regarded as sensitive, because if the information is used for the wrong purposes, such use would most likely violate the freedoms or rights that the individual has under the *Charter*.

Not all the rights provided in the *Charter* will be equally sensitive. It is posited that "sensitivity" will be based on the abilities of others to use such information to take any action harmful to the interests of the individual. For example, usually the sex of a person can be determined by simple observation, or inferred from the name. Therefore, a list of names identifying such persons as male or female may not be considered particularly sensitive.

However, a list of the names and addresses of the attendees at a local synagogue or mosque, or of the members of the Catholic Church that are also active in Campaign Life, would most likely be considered much more sensitive.

C. SENSITIVE AREAS

A considerable portion of the initial privacy concerns that arose out of the development of the internet and e-commerce were with respect to the use of cookies[47] and online

---

[46] *Ibid.*

[47] A "cookie" is a small text file placed on a consumer's computer hard drive by a web server. They were developed to allow user-side customization of web information. The cookie transmits information back to the server that placed it and, in general, can be read only by that server. Web servers automatically gain access to relevant cookies whenever the user establishes a connection to them, usually in the form of web requests. Technically all that they identify is a particular computer. For more information on cookies see for example: www.cookiecentral.com.

profiling[48]. However many consumers now realize that properly used, cookies contribute considerably to an enjoyable online experience. Ordinary consumer transactions, such as buying peanut butter, do not cause significant privacy concerns because the information about most people's peanut butter preferences is not particularly sensitive. Further for particularly desired goods, the development of a profile by the vendor may actually strengthen the relationship.

However to the extent that peanut butter (or some other good) is an indication of one's lifestyle choices, one's health, or even one's religious affiliation, there may be consumer concerns regarding the collection of information regarding purchases.

1. Personal Health Information

Health information is a complex area with respect to privacy concerns. The degree of sensitivity can vary greatly with the circumstances. While most health information can be regarded as having some degree of sensitivity, it is necessary for the person seeking consent to the use of the information to evaluate the sensitivity of the particular facts in their context before proceeding.

Applying the discussion earlier regarding the concept of sensitivity, medical conditions that reflect lifestyle choices or basic reproductive abilities and choices are generally considered very private and highly sensitive. Some medical conditions also have stigmas attached because of fear of infection, associations with class differences or poverty, mental disability, or even aesthetic concerns. There may be several factors associated with one medical condition, such as AIDS, and these can have a multiplier effect to heighten sensitivity.

But when dealing with human emotional responses, it is hard to find a reliable formula. Notwithstanding the fact that smoking has become increasingly stigmatized in North America, particularly among more mature groups, a diagnosis of lung cancer does not seem to be as sensitive a piece of personal information as a diagnosis of AIDS.

On the other hand, persons suffering from a particular medical condition are taking an increasingly pro-active approach in seeking out information about the condition and possible resolutions[49], including searching the internet. If the appropriate degree of care is used in obtaining consent and protecting the information, a very targeted marketing relationship can be developed[50].

---

[48] See for example U.S. Federal Trade Commission "Online Profiling: A Report to Congress" June, 2000, available on the FTC's website at: www.ftc.gov, and Jay Lyman, "Europe Proposes Banning Web Cookies", *E-Commerce Times*, November 1, 2001.

[49] See for example Julie Gilbert, Gale Murray and Ruth Corbin, *Consumers and Healthcare in Ontario: Are Patients Becoming Consumers* (Toronto: The Change Foundation, November 2001).

[50] For an example of how an established relationship for a sensitive condition can be compromised by poor security and training see FTC File No. 012 3214 *In the Matter of Eli Lilly and Company* released January 18, 2002, available online on the FTC web site, www.ftc.gov. Eli Lilly operated a web site for users of its anti-depressant drug Prozac.

Marketing in the health area also raises other concerns because societies and individuals vary in their acceptance of market principles in the sector. Canada has a tradition of having publicly funded healthcare, in contrast to the United States where private funding and a more open market for healthcare services is the norm. Certainly doctors in the two countries appear to be taking different approaches to direct-to-consumer advertising of pharmaceuticals. The U.S. Food and Drug Administration recently released a survey that it conducted of 500 physicians regarding direct-to-consumer ("DTC") advertising for prescription drugs. In their opinion

> The results confirm that DTC advertising, when done correctly, can serve positive public health functions such as increasing patient awareness of diseases that can be treated, and prompting thoughtful discussions with physicians that result in needed treatments being prescribed - often not the treatment in the DTC advertisement.[51]

In contrast in Canada, a recent editorial in the Canadian Medial Association Journal[52] commented on the problems of marketing pharmaceuticals in general by commencing with a quote from Ralph Nader's 1965 book, *Unsafe at Any Speed*:

> A great problem of contemporary life is how to control the power of economic interests which ignore the harmful effects of their applied science and technology.

While pharmaceutical companies finance most of the continuing education of physicians in Canada with respect to the use of new drugs, the concern is that patients will not receive a clear and unbiased description of the use and effects of their medications because of the inherent economic interest of the drug companies. The editorial specifically cites a problem with a drug for the management of asthma and the recommendations of a coroner's jury that pharmaceutical companies improve their product information.

In the health area, a lack of trust can exacerbate sensitivity concerns such that some individuals will seek to claim an interest in even their anonymized health information. While IMS Health Canada, a company that collects information as to doctor's prescribing habits, takes the position that such information about individual doctors is public information required by patients to become informed consumers of their doctors' services[53], the Canadian Medical Association and others have increasing discomfort

---

[51] U.S. Food and Drug Administration, "Food and Drugs Act Releases Preliminary Results of Physician Survey on Direct-to-Consumer Rx Drug Advertisements", on FDA Talk Paper T03-03, January 13, 2003.

[52] Editorial "Drug Marketing: Unsafe at any dose?" 167(9)CMAJ 981, October 29, 2002.

[53] See Anita D. Fineberg "The *Personal Information Protection and Electronic Documents Act*: Physician Prescription Data and Canadian Health System Review" 23(1) *Health Law in Canada* 1 (August, 2002) and Christopher Jones, T. Murray Rankin and James Rowan, "A Comparative Analysis of Law and Policy on Access to Health Care Provider Data: Do Physicians Have a Privacy Right Over the Prescriptions

with this position[54]. The concern is that the doctors are under a fiduciary duty to act in the best interests of their patients. The anonymized personal health information of their patients should not be collected without any consent and sold to drug companies to use in advancing their own self-interest in the sale of their products[55]. There is a conflict in interest between the doctor's duty to the patient and the drug companies desire to sell its product ahead of its competitors.

Notwithstanding the debate, the concerns illustrate one the more significant factors that marketers will have to take into account in the Canadian healthcare sector in building trust and obtaining consent to the collection, use and disclosure of personal health information.

2. Fundraising for Charities

Assuming that PIPEDA or another law applies to charitable and non-profit organizations, there is a great deal of variation among such organizations as to the sensitivity associated with their basic purposes. Many such organizations are formed around expressions of values or lifestyle choices that were discussed earlier as being inherently sensitive. In some countries there are restrictions on who may maintain a membership list for such an organization. However there are also many charitable and non-profit organizations in the arts. The more mainstream organizations in this group, such as for example a regional, government-funded art gallery, should not have particular concerns about sensitive information beyond those that an ordinary commercial enterprise would have. On the other hand where an arts group has expressly associated itself with particular political or social positions or groups, such as a theatre group that presents plays primarily by or about homosexuals, the information used in fundraising would have greater sensitivity.

The more interesting question with respect to fundraising is the nature of the consent needed for transfers of lists between groups. While lists are usually traded between organizations that appeal to similar groups, how similar is similar enough that an organization may rely upon opt-out or implied consent. When a private school sponsored a run for a charity, a sponsor's name and address were collected. However when the school then sent school newsletters to the sponsors, they received a

---

They Write?", 14 *Cdn. Journal of Admin. Law of Practice* 225 (2001). Ms. Fineberg is Corporate Counsel and Chief Privacy Officer for IMS Health Canada and Mr. Rankin's article was based on research initially carried on for IMS Health Canada. His article relies heavily on American cases and law journal articles. The Privacy Commissioner of Canada agreed with this position in PIPEDA Case Summary #15, "Privacy Commissioner releases his finding on the prescribing patterns of doctors", October 2, 2001. One complainant has sought judicial review of this decision in Federal Court, and the CMA is seeking intervenor status.

[54] See Paul Jones, "Striking the right balance", *Law Times*, December 10, 2001.

[55] See *R. v. Department of Health, ex parte Source Informatics Ltd.* [1999], 4 All E.R. 185 (QBD); [2000] 1 All E.R. 786 (CA). At trial the patients were found to have an interest in their anonymized health information, on appeal this decision was overturned.

vociferous complaint. The objectives of the school and the charity were not particularly similar.

On the other hand a hospital and its foundation obviously have very similar goals; such that most who would support one would also support the other. Accordingly Ontario's draft privacy law proposed a modified form of opt-out consent for such organizations[56].

3. Students

With respect to students, the sensitivity of their personal information more often arises from their age and status in society than from the nature of the personal information. Generally the concerns have arisen in the United States, and there is not evidence of widespread concern in Canada. In the U.S. the *Children's Online Privacy Protection Act* requires web sites targeting children under 13 years of age to obtain the parent's consent before collecting, using or disclosing personal information. There have been a number of prosecutions by the FTC under COPPA.

Some businesses have collected data about students and their families for years, primarily by representing to teachers that the information would be used to assist the student in applying for higher education, but also in exchange for donations to the school. As one U.S. Senator put it "They're basically selling access to kids without parents knowing about it"[57]. The concerns appear to also be based on the concerns about the presence of commercial market players in a non-profit environment with a captive and vulnerable market. As of the start of the school year for 2002-2003 in the United States certain ancillary provisions of the *No Child Left Behind Act*[58] come into effect allowing parents to exclude their children from personal data collection at school where the information is used for non-educational marketing. Schools must also notify parents of their right to opt-out their children. Linking and secondary marketing purposes would thus appear to make student information more sensitive.

Finally some parents may regard information regarding the student's progress to be sensitive personal information. A parent in Owasso, Oklahoma went to court to try to stop the practice of having students grade each others work. The parent alleged that her son was called names such as "stupid" and "dummy" as a result[59]. Ultimately the U.S. Supreme Court declined to stop the practice[60].

---

[56] Ontario Ministry of Consumer and Business Services, "A Consultation on the *Draft Privacy of Personal Information Act, 2002*" (Policy Branch, Ministry of Consumer and Business Services, Toronto, February, 2002), see Section 26 and commentary.

[57] Sen. Richard C. Shelby (R-Alabama) as quoted in Robert O'Harrow Jr., "Marketers May Face Student-Data Curbs" *Washington Post*, December 18, 2001.

[58] *No Child Left Behind Act of 2001*, Public Law 107-110, 107th Congress, First Session.

[59] Gaylord Shaw, "High Court to Hear Student Privacy Case: Does announcing grades violate rights?" *Newsday.com*, November 25, 2001.

[60] *Owasso Independent School District No. I-011, aka Owasso Public School, et. al. v. Falvo, Parent and Next Friend of Her Minor Children, Pletan et. al.*, 534 U.S. 426; 122 S.Ct. 934 (February 19, 2002).

4. Dealerships, Franchises and Brokerages

The concern in this areas, such as in automobile finance or insurance, is that one person who may be well known and trusted by the individual, collects the information for disclosure and use by other parties, such as the car manufacturer, and the auto finance company. The question is whether such disclosures between companies working under one brand with a standardized procedure is really very sensitive at all. It has been suggested that B.C.'s proposed privacy law may allow for groups of companies to form a unit for privacy consent and disclosure purposes.

Problems have arisen where the dealer or distributor is asked to forward customer information to the manufacturer/franchisor. If the dealers are concerned that their customers will be marketed to directly, they may resist by citing privacy concerns[61]. In either event problems in this area can be overcome by a careful drafting of the form of consent.

D. SENSITIVE PURPOSES

The intent of this discussion is to highlight general categories of purposes that may heighten sensitivity if included in the consent. Sensitive areas such as health and certain beliefs have already been discussed previously. The best illustration of how additional purposes can heighten sensitivity is the finding of the federal Privacy Commissioner in the Air Canada matter[62]. Air Canada not only used Aeroplan member's information for purposes of advertising products and making promotional offers, but it customized or "tailored" the members purchasing habits.

> Although in the Commissioner's view the practice of using plan members' information for purposes of advertising products, services, and special promotions remains unobjectional in itself, he was satisfied that a reasonable person would not expect such practice to extend to the "tailoring" of information to the individual's potentially sensitive personal or professional interests, uses of or preferences for certain products and services, and financial status, without the positive consent of the individual.

In other words, because Air Canada did more than simply save the personal information collected for future mailings, it could not rely on an opt-out form of consent. Rather opt-in consent was required.

Other practices that may also heighten sensitivity include linking of information from other transactions and sources, particularly if from outside the organization, disclosure

---

[61] See Connie Guglielmo, "Ransom: Customer Data", *Zdnet.com*, October 8, 2000 concerning a dispute in the Motorola dealer system.

[62] PIPEDA Case Summary #42: Air Canada allows 1% of Aeroplan membership to "opt-out" of information sharing practices, March 20, 2002.

to affiliated companies, disclosure to marketing "partners", and of course the sale of the information itself. Part of the art of preparing privacy consents is stating the purposes in sufficiently general terms to give the organization flexibility for the future without becoming so vague as to encompass almost any activity that the organization might wish. It would appear that broadening the purposes is likely to increase the sensitivity of the information and thus require more explicit consent.

An ongoing issue for all privacy consents arises when all the assets of the company are sold. In the United States, this issue first arose during the bankruptcy of Toysmart.com, an internet educational toy seller, when the company advertised its list of customers, reported to have about 190,000 names, for sale as one of its key assets[63]. The FTC and the attorney generals of several states intervened before the bankruptcy court, and eventually the data was simply destroyed. Toysmart's web site had promised that personal information would never be disclosed to third parties[64]. Since then there have been several similar cases, all in the United States[65]. What makes these cases particularly interesting is that the Mergers & Acquisitions Group of one major Toronto law firm has collectively taken the position that transfers of personal information during the sale of a business are reasonably expected by individuals and therefore implied consent is sufficient.

E. SECURITY AND ACCESS

Generally speaking Principle 7 of Schedule 1 to PIPEDA requires that the security measures employed be appropriate to the sensitivity of the personal information stored, rather than the other way around. However it can be argued that the degree to which the organization demonstrates that it has strong security measures in place, and the accuracy of the information and the nature of the uses and disclosures made can be easily verified will influence to some degree the level of the consent that is needed.

Certainly the principle behind the business plans of the private sector privacy seal programs such as TRUSTe, BBBOnline and WebTrust is that individuals will regard sites displaying these seals as more trustworthy in matters of privacy, and thus better places to do business.

F. APPROPRIATE CONSENT

Unfortunately there is no formula for interpreting the variables discussed earlier and arriving at a precise formulation for the appropriate level of consent required in a particular context. For lawyers guidance can best be obtained by remembering the basic principles of contract formation and the cases regarding tickets, exculpatory clauses and unconscionability. The quality (or enforceability) of the consent depends

---

[63] *In re Toysmart.com, LLC*, Case No. 00-13995-CJK (Bankr. E.D. Mass.).

[64] Paul Jones, "Privacy law will require new due diligence" *The Lawyers Weekly*, September 15, 2000.

[65] See *In re Egghead.com, Inc.*, Case No. 01-32125-SFC-11 (Bankr. N.D. Calif.); *In re Living.com, Inc.*, Case No. 00-12522 FRM (Bankr. W.D. Texas); and *In re eToys, Inc.*, Case Nos. 01-706 through 709 (MFW) (Bankr. D. Del.).

upon whether the material facts were indeed brought to the attention of the individual and whether the consent can be easily evidenced, or must be inferred from later actions.

Debate around the appropriate form of consent tends to adopt the wording used in the United States, namely "opt-in" as opposed to "opt-out". An "opt-in" consent would require some affirmative action, such as a signature or checking off a box. Inaction or neglect on the part of the individual assumes that they do not consent to the collection, use or disclosure proposed. In an "opt-out" consent the individuals who do not bother to react to the privacy notice are presumed to have consented to the collection, use, and disclosure proposed. It should also be noted that the term "opt-out" is also used in a separate context to describe the right of the individual to withdraw the consent iniitially obtained, or to "opt-out" at any time[66]. Care should be taken to ensure that the two uses are not confused.

In Canada the terms set out in Principle 3 of Schedule 1 to PIPEDA[67] are "express" and "implied" consent. To obtain "express" consent the individual generally must take some action to indicate consent to the specific terms of the privacy notice. For "implied" consent acquiescence with the terms of the privacy notice must be inferred from the surrounding circumstances and the subsequent course of conduct of the individual. While "opt-in" and "opt-out" are examples of "express" and "implied" consent respectively, they are not the only forms, nor even the dominant forms of either. A very common form of express consent is to have the individual write in the necessary personal information directly underneath the privacy notice, such as in a magazine subscription or a contest entry form. If the individual did not agree with the terms of the privacy notice presumably he or she would not have completed and returned the form.

In the U.S. marketing organizations have strongly opposed mandated "opt-in" consent for a variety of reasons[68]. It is argued that "Information is the life blood of the U.S. economy."[69] An "opt-in" system would increase the cost of doing business. It is also argued that consumers are in fact making informed choices and they do not value their privacy as highly as some privacy advocates would have us believe. As with the initial debate over cookies and online profiling, there is an advantage to the consumer in allowing such collection, and the consumer chooses to accept some loss of privacy in return for other benefits.

A major test of "opt-out" consent has been in the effectiveness of the annual privacy notices that financial institutions must mail to their customers under the *Gramm-Leach-Bliley Act*. Generally speaking the privacy notices have been overly broad, and long

---

[66] Principle 4.3.8 of Schedule 1 to PIPEDA.

[67] See in particular Principle 4.3.6.

[68] Fred H. Cate and Michael E. Staten, *Protecting Privacy in the New Millennium: THE FALLACY OF "OPT-IN"* (New York: Direct Marketing Association, 2001) formerly available online at www.the-dma.orga/isec/optin.shtml.

[69] *Ibid.*

and difficult to read, resulting in considerable criticism[70]. One bank said it would make two kinds of disclosures. The first was to "Financial Service Providers". The second was to "Non-financial Service Providers". Another had a list of categories of organizations with which it would share information. The final category was "Other"[71].

Complaints about the readability of the notices are legion, and one consultant analyzed 60 such notices using the Flesch Reading Ease Score[72]. He found that they were generally written at a 3rd-4th year college reading level, instead of the junior high school level that is recommended for materials written for the general public. Too many complicated sentences and uncommon words were used. Many saw the problem as being that the organizations have a conflict of interest. They have a financial incentive to create confusing privacy notices and difficult to follow opt-out procedures[73]. Or as Sen. Richard C. Shelby put it, "They're designed, I guess, not to be understood"[74].

Canada's federal Privacy Commissioner has voiced similar concerns, most notably in PIPEDA Case Summary #42, the Air Canada case.

> Opt-out consent is in effect the presumption of consent - the individual is presumed to give consent unless he or she takes action to negotiate it. I share the view that such presumption tends to put the responsibility on the wrong party.
>
> •••
>
> Accordingly, while acknowledging that the Act does provide for the use of opt-out consent in some circumstances, I intend, in this and all future deliberations on matters of consent, to ensure that such circumstances remain limited, with due regard both to the sensitivity of the information at issue and to the reasonable expectations of the individual.

---

[70] See John Swartz, "Privacy Policy Notices Are Called Too Common and Too Confusing", *New York Times*, May 7, 2001; Robert O'Harrow, Jr., "Privacy Notices Criticized: New Bulletins Unclear, Some Lawmakers Say", *Washington Post*, Friday, June 22, 2001; Mark K. Anderson, "Ignore This Letter, Please", *Wired News*, June 29, 2001; Brian Krebs, "State AGs Urge FTC To Require Stronger Privacy Notices", *Newsbytes*, February 15, 2002; Michael Bartlett, "Privacy Groups Blast Info Sharing By Financial Institutions", *Newsbytes*, May 2, 2002; In the Matter of Financial Services Modernization Act a Gramm-Leach-Bliley Act (GLBA) 15 USC § 1608-Comments of the Electronic Privacy Information Center, the Privacy Rights Clearinghouse, US PRG, and Consumers Union before the Department of Treasury, Washington DC, May 1, 2002; Joanna Glasner, "Survey: Opt-Out is a Cop-Out", *Wired News*, May 7, 2002; Russell Gold, "Privacy Notice Offers Little Help; Mailing From Banks, Retailers Lets You Protect Financial Data, but it's Hard to Decipher", *The Wall Street Journal*, May 30, 2002.

[71] Swartz, *supra*, note 70.

[72] Mark Hochhauser, "Lost in the Fine Print: Readability of Financial Privacy Notices", posted on the Privacy Rights Clearinghouse Website, July 2001.

[73] Bartlett, *supra*, note 70.

[74] O'Harrow, *supra*, note 70.

While "opt-out" provisions as a method for obtaining consent appear to have inherent structural problems that has caused some to disfavour them, implied consent in general is still available, as two recent Canadian privacy decisions have shown.

In *Marquis v. Journal de Québec*[75] the Québec Court of Appeal had to decide whether or not there was implied consent to publish the pictures and interview comments of two 17 year old hockey players regarding an obscene video that had been made of a team initiation ceremony. The action was brought under Article 35 of the *Code civil du Québec*[76], and Section 5 of *La Charte des droits et libertés de la personne*[77], but not under Québec's Loi du secteur privée[78], which requires that consent be "... manifeste, libre, éclairé ...", because it excludes journalistic activities. The journalist, accompanied by a photographer, had gone to the local high school and paid a classmate to point out members of the hockey team. There were different versions as to how the journalist identified himself, but it was found that the two young men voluntarily submitted to the interview. During the ten-minute interview the journalist took notes on a notepad, and the photographer took 14 close-up pictures. After the pictures and story were published the next day, the young men complained that they had not consented to the interview or the photographs or the publication.

At trial the judge found that they had consented to the interview and the taking of photographs but questioned whether such consent was also implied consent to publication. He stated that:

> A fortiori one must be careful with respect to breaches of the moral integrity of a person, breach of privacy, name, identity and invasion of the person or his or her image. *Any waiver to the right to privacy must be clear, subject to both full disclosure, and the free and informed consent of the waiving party*. Any implied waiver under these circumstances must be narrowly interpreted. We also refer to and concur with the comments of Allen M. Linden to the effect that "young people may nevertheless consent to breaches of this right even if they are minors, provided they understand exactly what they are consenting to".[79]

The trial judge then found that the individuals had not measured the consequences of their consent, and that given the importance of the privacy right, the individuals had not consented to the publication.

---

[75] *Journal de Québec v. Marquis et. al.* (2002), 219 D.L.R. (4th) (Cour d'appel du Québec).

[76] *Supra* note 20.

[77] L.R.Q., c. C-12.

[78] *Supra* note 21.

[79] *Supra* note 75, at 311. As cited in the Court of Appeal decision and translated for publication in the Dominion Law Reports. Emphasis in the original.

On appeal, the court agreed that there was no express consent to publication. However he found that consenting to an interview with the journalists is implied consent to publication and dissemination.

> In my view, publication and dissemination are so intrinsically linked to the nature of the event that it falls upon the person who wishes to prevent all or part of the publication or dissemination to set conditions prior to agreeing to the interview.[80]

With respect to the additional burden imposed on the journalist by the trial judge because the individuals were under age, the Court of Appeal did not find this factor materially significant as there were only months away from the age of majority.

The other case, *Thomas v. Robinson*[81], is to date the most significant decision of a tribunal with respect to PIPEDA, and from Ontario. In order to settle a shareholder's dispute, the court was asked to determine whether PIPEDA applied to a database of life insurance agents. Insurance companies employing such agents are required by law to screen applicant agents and to ensure that agents do in fact comply with the law. The business in dispute had performed that service for various insurance companies across Canada, conducting investigations and forwarding the information to the particular insurance company.

Unknown to the insurance companies and the agents investigated, the business also retained the information in the database, which expedited their future investigations. The judge ruled that although most of the database was compiled before PIPEDA came into effect, PIPEDA applied to the information on individuals collected outside of Ontario. The individuals had expressly in writing consented to the investigation, and to the relevant insurance company keeping a file on an ongoing basis, and to the use of subcontractors for the investigations. However there was no express consent to the subcontractors (being the business that was the subject of the shareholder's dispute) maintaining a file. The judge found that such consent could be implied and the general purpose for the collection and use of the information had been communicated to the individuals. However he advised that:

> If the information in the database is to be used in respect of a new application [by an insurance agent - thus requiring verification], then documentation supporting that new application should contain notice of the intention to use the **existing information** [emphasis added], and should seek the applicant-agent's consent.[82]

---

[80] *Ibid*, p. 315.

[81] *Thomas v. Robinson*, [2001] O.J. No. 4374, 2001 Carswell Ont. 3986, 34 C.C.L.I. (3d) 75 (Ont. S.C.J.) October 16, 2001.

[82] *Ibid*, p. 27.

This decision should give considerable reassurance to organizations having existing databases that to a large extent consent to the use of such databases will be implied.

In a number of decisions recently the Federal Privacy Commissioner has specified a further items to be added to the privacy notice and consent[83], particularly with respect to secondary marketing. This may be summarized as follows:

1. Make the purposes understandable.

2. Ensure that the intended uses and disclosures are well-defined in respect of:

   a) the types of information to be used or disclosed;

   b) the parties to which the information is to be disclosed; and

   c) the purposes for which information is to be disclosed.

3. Ensure that the individuals are notified of their opportunity to withdraw consent, and that the individual is provided with and notified directly of an easy, immediate, and inexpensive means of doing so.

4. If the service will be offered through a third party, the third party should be identified.

These are relatively basic procedures to follow to improve the quality of the consent. They are the material elements of any agreement between the parties for the use of personal information.

G. CONCLUSION

For marketers and advertisers who are prepared to adopt to a new competitive environment, Canada's new privacy laws may turn out to more of a blessing than a curse. The adoption of permission-based marketing will unleash significant opportunities for more effective and efficient targeting of marketing and advertising

---

[83] PIPEDA Case Summary #78, Alleged disclosure of personal information without consent for secondary marking purposes; PIPEDA Case Summary #79, Alleged disclosure of personal information without consent for secondary marketing by two telecommunications companies; PIPEDA Case Summary #82, Alleged disclosure of personal information for secondary marketing purposes by a bank; PIPEDA Case Summary #83 Alleged disclosure of personal information without consent for secondary marketing purposes by a bank; PIPEDA Case Summary #91, Marketing firm accused of improper disclosure of survey information.

resources, building better relationships, and developing pricing models that more closely reflect the value placed on the goods by different groups of customers.

In a wide variety of ordinary marketing transactions personal information and consent should not be that difficult to obtain for normal marketing purposes. The debate over "opt-in" consent vs. "opt-out" consent exaggerates the supposed difficulties. And appears from the limited evidence available to date that the courts are prepared to take a reasonable approach to reliance on implied consent.

SCHEDULE A

SUMMARY OF CANADA'S TEN PRIVACY PRINCIPLES

Principle 1 - Accountability

This Principle generally requires the designation of an individual or individuals who are accountable for the organization's compliance with PIPEDA. The organization is specifically held responsible for information that has been transferred to a third party for processing, which must be protected by contractual means. Organizations are required to implement policies and practices to give effect to the principles, including training staff. This Principle remains as set out in the CSA Model Code, and has not been modified by PIPEDA.

Principle 2 - Identifying Purposes

The purposes for which personal information is collected must be identified to the individual at or before the time that it is collected. Once this has been done the personal information cannot be used for a new or further purpose without the consent of the individual.

Section 5(3) of PIPEDA provides that "An organization may collect use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances". The Privacy Commissioner sees this Section as providing an outer limit on the purposes that may be used by an organization to justify data collection, use or disclosure. Obtaining the consent of the individual for the collection of personal information outside of these limits may be insufficient for compliance.

This Principle is also modified by Principles 4 and 5 regarding limiting collection, use, disclosure and retention.

Principle 3 - Consent

This Principle is generally regarded as the key to the protections in PIPEDA, and will be further discussed later in this paper.

Generally speaking personal information cannot be collected, used or disclosed without the knowledge or consent of the individual, unless there is a specific exemption provided for in PIPEDA. An organization may not, as a condition of the supply of a product or service, require such consent beyond what is required for a legitimate fulfilment of the transaction. The form of consent may be explicit or implicit, or "opt-in" or "opt-out", depending upon the sensitivity of the information. The concept of "sensitivity" is somewhat problematical and its implications for charitable organizations will be discussed in the next section. Because of this it is always more prudent to try to

obtain written consent. Finally consent can be withdrawn at any time, subject to legal or contractual restrictions and reasonable notice.

The federal Privacy Commissioner has made his antipathy to opt-out consent abundantly clear in his findings regarding Air Canada's Aeroplan Frequent Flyer Program, released March 20, 2002:

> "I should begin by making it clear that, like most other privacy advocates, I have a very low opinion of opt-out consent, which I consider to be a week form of consent reflecting at best a mere token observance of what is perhaps the most fundamental principle of privacy protection. Opt-out consent is in effect the presumption of consent – the individual is presumed to give consent unless he or she takes action to negate it. I share the view that such presumption tends to put the responsibility on the wrong party. I am also of the view that inviting people to opt-in to a thing, as opposed to putting them into the position of having to opt-out of it or suffer the consequences, is simply a matter of basic human decency.
>
> Accordingly, while acknowledging that the *Act* does provide for the use of opt-out consent in some circumstances, I intend, in this and all future deliberations on matters of consent, to ensure that such circumstances remain limited, with due regard both to the sensitivity of the information at issue and to the reasonable expectations of the individual. In other words, in interpreting Principle 4.3.7, I intend always to give full force to other relevant provisions of the *Act*, notably 4.3.4, 4.3.5 and 4.3.6 and section 5(3)."

Care must be taken in reading the specific sections of this Principle in the Schedule because it is extensively revised by Section 7 of PIPEDA, which provides the specific and only exceptions from obtaining consent for the collection, use, and disclosure of personal information.

Principle 4 - Limiting Collection

This Principle provides that the collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Purposes need to be reasonably specific. Information must be collected by fair and lawful means.

This principle is not modified by PIPEDA.

Principle 5 - Limiting Use, Disclosure and Retention

This Principle provides that personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the

individual or as required by law. Personal information shall be retained only as long as it is necessary for the fulfilment of those purposes. Organizations must develop guidelines with maximum and minimum retention periods.

This Principle is also modified by Section 7 of PIPEDA.

Principle 6 - Accuracy

Personal information shall be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.

However the extent to which this must be implemented depends upon the use of the information, taking account of the interests of the individual. While this Principle is vaguely worded, it is relevant mainly to organizations that collect information to make decisions that may affect the subject individual adversely.

This Principle is not modified by PIPEDA.

Principle 7 - Safeguards

Personal information is to be protected by security safeguards appropriate to the sensitivity of the information. As with Principle 3 - Consent, "sensitivity" is a key concept. The purpose of the safeguards is not just to protect against theft, but also to protect against unauthorized access, disclosure, copying or use. The methods of protection should include physical measures, such as locked filing cabinets and restricted access; organizational measures, such as security clearances and access on a "need-to-know" basis; and technological measures such as passwords and encryptions. How many charitable organizations currently maintain such safeguards? How many think they should? What would be the cost of implementation?

Principle 8 - Openness

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information. This Principle effectively requires the use of privacy statements by organizations operating in Canada, on websites, or on other material, including printed material, through which they collect personal information. It also requires that the privacy policy developed pursuant to Principle 1 be made available to individuals. Specifically the information to be made available shall include:

b) the name or title, and the address, of the person who is accountable pursuant to Principle 1;

c) the means of gaining access to personal information held by the organization;

d) a description of the type of personal information held by the organization, including a general account of its use.

e) a copy of any brochures or other information that explain the organization's policies, standards or codes; and

f) what personal information is made available to related organizations such as subsidiaries.

Principle 9 - Individual Access

Upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

This right of access is limited by the provisions of Sections 8 and 9 of PIPEDA, which set the terms for requesting access, and prescribe when access is prohibited[1], or may be refused by the organization holding the information[2].

In the United States the principle of access is one of the major concerns of those opposed to privacy legislation, because of the anticipated cost of complying with requests. Experience with privacy legislation in the United Kingdom tends to suggest that estimates of a deluge of requests, many of which are frivolous, are quite unfounded. But based on the experience in Québec, requests to see personal information are now an expected part of a dispute with an employee or other individual.

In PIPEDA such disclosure includes an account of the use that has been made of the information, and an account of the third parties to which the information has been disclosed. Such disclosure can be expensive to make if the files containing such information have not been properly structured in advance to record and summarize such information as use occurs.

The full cost of making such disclosure cannot be recovered from the person making the request. Paragraph 4.9.4 of this Principle provides that responses are to be at minimal or no cost to the individual[3]. Section 8(6) further specifies that the individual

---

[1] See Section 9(1) of PIPEDA.

[2] See Section 9(3) of PIPEDA.

[3] For a discussion of the interpretation of the provisions regarding costs see Paul Jones, *Privacy Law: A New Era*, a paper presented to the 12th Annual Meeting of the Canadian Corporate Counsel Association in Halifax, August 21-22, 2000, at pages 16 and 17.

may be required to pay only if the individual is notified in advance of the approximate cost and agrees to pay.

Principle 10 - Challenging Compliance

Any individual shall be able to address a challenge concerning compliance to the individual accountable for the organization's personal information.