Permission-Based Marketing Under Canada's New Privacy Laws

PAUL JONES

Franchisors doing business in Canada must generally develop privacy policies and implementation strategies, particularly with respect to marketing, designed to comply with Canada's new privacy laws. The primary change from previous practice is that franchisors now need the consent of their system's customers for all marketing activities that involve the collection, use, or disclosure of personal information. In the process, they may well be laying the groundwork for compliance with the privacy laws of other countries, particularly those in Europe.

In 1995, the European Union adopted what is known as the E.U. Data Directive,[1] which stipulates that the transmission of personal information outside the E.U. is possible only to countries where the law affords similar protection to personal data. The E.U. Data Directive also establishes procedures 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. Because of its significant implications for the E.U.'s trading partners, the E.U. Data Directive has accelerated the adoption of privacy laws around the world, including those in Canada.

This article begins by describing the basic nature of privacy laws followed by a review of Canada's current system of national and provincial privacy laws. Because permission-based marketing requires obtaining the appropriate consent from the customer, this article next examines the nature of consent, what constitutes "sensitive information," and management of "sensitive" areas and purposes. It concludes by reviewing appropriate forms of consent for various types of data.

What Is Privacy?

Privacy is notoriously difficult to define. Although Warren and Brandeis described it as the right to be let alone in their seminal 1890 article,[2] some have suggested that the concept goes further and that privacy is the right to control information about a person, even if the information has been stripped of all identifying data.[3] Prosser describes four basic kinds of privacy rights, including right of publicity, defamation, intentional infliction of emotional distress, and newsgathering.[4] The rights discussed in this article concern the privacy of personal information or the protection of what is known about individuals.

Different jurisdictions[5] have developed varying ways of describing or expressing the basic principles of such protection, but privacy legislation generally shares the following characteristics:

> Individuals must be given notice of the proposed collection, use, and disclosure to third parties of personal information as well as the specific purposes for collecting the information.
>
> In order for the data to be collected, used, or disclosed, appropriate consent must be obtained with respect to the specified purposes.
>
> The data collected must be protected by appropriate security.
>
> The individual must have access to the data collected and to the details of its use and disclosure.[6]

The methods of ensuring compliance also vary widely. 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.[7] In others, the primary responsibility for ensuring compliance rests with individuals through use of the courts or an administrative tribunal.[8]

Privacy legislation is based on a so-called contract model. The organization wishing to use personal information for a certain purpose makes an offer to an individual to use it under certain terms for the specified purposes. As with other consumer contracts, problems have developed with the nature of the consumer's understanding of the proposed contract, 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."

To address these concerns, jurisdictions have developed different ways to restrict privacy contracts. For example, a number of European countries specify various types of personal information that must be considered sensitive and either require more explicit consent for collection, use, or disclose of this type of personal information or prohibit its collection altogether.

Canadian Privacy Laws

English Canada does not have a tradition of protecting privacy although Québec has had European-style privacy protection in place since 1994. In contrast to the protections developed in civil law countries like France, in the United Kingdom, the basic common law principle is that there is neither right to privacy nor an action for invasion of privacy per se. In Canada, although the courts have never specifically accepted the English position, they have been reluctant to found liability on a privacy right alone and have avoided the problem by relying on the more established categories of torts, such as defamation, breach of confidence, or intentional infliction of emotional distress.[9]

In order to strengthen e-commerce in Canada and to provide a legal framework that complies with the E.U. Data Directive, Canada implemented a general personal information protection law, the federal Personal Information Protection and Electronic Documents Act (PIPEDA).[10] Canadian companies did not appear to have the same con-

Paul Jones is an attorney practicing in Toronto.

cerns as their American counterparts about the increased cost of doing business, possibly because many already adhered to a voluntary code developed by the direct marketing industry and others in conjunction with the Canadian Standards Association (CSA), a voluntary, private sector organization.

Canada has chosen to use ten privacy principles, adopted directly from the CSA Model Code,[11] as the basis for PIPEDA and the code is appended to the legislation as a schedule. These principles are (1) accountability, (2) identifying purposes, (3) consent, (4) limiting collection, (5) limiting use, disclosure, and retention, (6) accuracy, (7) safeguards, (8) openness, (9) individual access, and (10) challenging compliance. Franchisors and franchisees planning on doing business in Canada would be well advised to look at Schedule 1 to PIPEDA, which is available on the website of the Office of the Privacy Comissioner of Canada (www.privcom.gc.ca).

Constitutional Authority

One issue is whether Canada's federal legislature had authority to enact PIPEDA in the first place. Because the Constitution Act, 1867, does not mention privacy or personal information, regulation of this area is arguably a provincial matter. However, much information is transferred electronically across provincial or national boundaries, thereby strengthening the argument in favor of federal jurisdiction.

Nevertheless, 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, under section 92(7)[12] of Canada's 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.[13]

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 inherently conflicts with the provincial jurisdiction over property and civil rights. Initially, the courts narrowed the federal trade and commerce power,[14] but more recently *General Motors v. City National Leasing*[15] established a new five-prong test for determining the appropriate exercise of the trade and commerce power by the federal government. Two of the five prongs, as noted below, are directly relevant to the issues that PIPEDA raises:

> (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.

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 Canadian federal government. Thus, condition four and possibly condition five are satisfied. To ensure compliance with the fifth condition, the provinces were given three years to pass their own privacy legislation.

Another distinctive aspect of PIPEDA is that the CSA Model Code upon which it is based was not drafted with the precision expected in a statute. The federal government attached the CSA Model Code, without any changes or amendments, as a schedule to PIPEDA. The government 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. Although PIPEDA clarifies some provisions, most notably the exceptions for obtaining consent, 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 noncompliance. To add to the confusion, lawyers often give differing opinions when interpreting PIPEDA.

One of the more interesting provisions imposes limitations on the purposes for which an organization may collect, use, or disclose personal information.[16] 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 as placing a limit on the purposes for an organization's processing of personal information.[17]

Québec

In civil matters such as privacy, Québec follows the civil code model as found in France. Article 35 of the *Code civil du Québec*[18] specifically recognizes the right to privacy: "Every person has a right to the respect of his reputation and privacy. No one may invade the privacy of a person without the consent of the person unless authorized by law."

In 1993, Québec passed the *Loi sur la protection des renseignements personnels dans le secteur privée*[19] (*Loi du secteur privée*). The law imposes no obligation to obtain a license to collect personal information. Section 70 does mandate, however, that every personal information agent (the person who, on a commercial basis, personally or through a representative, establishes files on other people) register with the *Commission d'accès à l'information du Québec*. This is primarily a requirement for credit agencies. The law establishes standards covering the collection and use of personal information, including a defining the purpose of collection, collecting only necessary information for the specified purpose, informing the person of the collection, and obtaining consent for transferring the information to a third party.

On November 19, 2003,[20] the federal government declared that the *Loi du secteur privée* is substantially simi-

lar to PIPEDA to the extent that it protects personal information. However, franchisors should be aware of some significant differences, especially the following:

Article 8 imposes broader notification requirements than PIPEDA's Principle 8, requiring that people must be advised of the categories of persons within the organization who will have access to the information and where it will be kept.

Article 20 explicitly limits the access of employees and agents of a corporation to information that is necessary for them to perform their jobs.

Article 17 requires that franchisors that want to transfer information on Québec residents to take all reasonable steps to not to use the information for purposes other than the one for which it was collected or to disclose it to a third party.

A potential loophole appears in Article 22, which provides for the transfer to a third party, without consent, of lists of names, addresses, and phone numbers if the third party is prohibited by contract from using the list for purposes other than commercial or philanthropic solicitation; if the people on the list have had a valid opportunity to opt-out of the transfer; and if the communication does not infringe on the privacy of the individuals concerned.

Care must be taken in relying upon the exemption if the source of the list would reveal significant or sensitive personal information about the people on it. For example, if the list identifies visitors to a website for AIDS sufferers, presumably the transfer of such list would not comply with the third provision of Article 22 on infringement of privacy. Instead, a requirement in Article 14 that consent for all information, especially potentially sensitive data as in this hypothetical situation, be "manifest, free, enlightened, and given for specific purposes" is more likely to require explicit agreement rather than implicit consent.

British Columbia and Alberta

To date, British Columbia and Alberta are the only provinces to have passed laws specifically to take advantage of the exemption provisions of PIPEDA. The two provinces collaborated on the drafting of their laws, which are both known as the Personal Information Protection Act.[21] Both laws, which were intended as model statutes for other provinces, have been in effect since January 1, 2004. As of the date of writing, the federal government has not yet issued the necessary order-in-council exempting transactions within these provinces from the application of PIPEDA although notice of its intent to do so has been advertised in the *Canada Gazette.*[22]

The drafters of the Personal Information Protection Act attempted to avoid many of PIPEDA's problems by integrating the principles in the CSA Model Code into one comprehensive law. The laws also differ from PIPEDA in a number of other ways, as noted below:

Implicit Consent: The concept is defined in section 8 in both laws. An individual is deemed to consent if the purpose is obvious to a reasonable person and the individual gave the information voluntarily for that purpose.

Existing Databases: Both laws provide that information collected before the laws came into force may continue to be used for the purposes for which it was originally collected.

Employees: Both laws define "employee personal information" and provide that consent is not required for the collection, use, or disclosure of such information provided that it is used for personnel reasons only and that the employee is notified of the practice in advance.

Unincorporated Associations: Both laws provide that unincorporated associations, which include franchise systems, may be considered "organizations" for the purpose for the law. PIPEDA simply states that an "organization" includes associations, partnerships, people, and trade unions. In practice, the federal Privacy Commissioner has regarded separate legal entities as separate organizations.

Investigations: Both laws provide for the collection, use, and disclosure of personal information without consent for a broader range of investigatory purposes than is allowed under PIPEDA.

Sale of Business Assets: Both laws allow for the disclosure without consent of the personal information of customers, employees, offices, directors, and shareholders as part of the transfer of the assets of the business under certain conditions. These provisions were likely omitted from PIPEDA in error.

Neither law clarifies the standard for determining when the provincial law applies and when PIPEDA applies. The British Columbia law simply states that it does not apply if PIPEDA applies.[23]

The differences between these laws and PIPEDA may be important for franchisors, especially if franchisees develop their own privacy policies. The initial collection and use of individual customer information will be subject to the provincial laws only if it is carried out entirely within a province. However, PIPEDA governs any transfer of the information to the franchisor, even with the consent of the individual, if the transfer crosses a provincial or national boundary.

The enforcement of the laws in both provinces will be markedly different from that under PIPEDA. The federal Privacy Commissioner has no power to issue binding decisions and to date, has released only anonymous summaries of his findings. In British Columbia and Alberta, however, the privacy commissioners have the power to issue binding orders.[24] David Loukidelis, British Columbia's Information and Privacy Commissioner, also has publicly stated that he will publish his decisions in full and not anonymously.[25] Nevertheless, these provincial privacy commissioners do not have the power to award damages. Both laws provide that once a commissioner's order against an organization becomes final, the individual affected by the order has a cause of action against the organization for damages for actual harm that he or she has suffered.[26] Under PIPEDA, an individual seeking damages must initiate an action in Federal Court.

Other Provinces

In provinces other than Québec, British Columbia, and Alberta, PIPEDA generally came into effect with respect to the collection, use, or disclosure of personal data on January

1, 2004. Most commentators believe that PIPEDA does not apply to employment relations within a province, to charities, or to some aspects of health care. No other provinces have announced plans to adopt a privacy law of general application and thus obtain exemption from the application or PIPEDA. Ontario, Alberta, Manitoba, and Saskatchewan have adopted health-specific privacy laws.

Permission-Based Marketing

Businesses have long had concerns about the effectiveness of their advertising and marketing expenditures. The development of the Internet and the widespread use of computers have allowed marketers and advertisers to refine their methods for selecting individual consumers to receive a particular message. Businesses now have the flexibility to collect, use, and disclose an individual's personal information in a wide variety of ways if they obtain the consent or permission of the individual.

Section 5(3) of PIPEDA limits the collection, use, and disclosure of personal information to purposes that "a reasonable person would consider appropriate in the circumstances." These constraints should not be significant for businesses that are truly trying to develop relationships with customers. Compliance with privacy laws is a basic and necessary step in developing customer relationships.

Compliance with privacy laws is a basic and necessary step in developing customer relationships.

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 depends 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 about data security.

The Nature of Consent

Consent in the privacy context is similar to consent in 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. Consumer transactions typically involve 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 by the difficulty of predicting future developments and the willingness and ability of the consumer to comprehend the vendor's offer.

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, has led to complaints by business people when their lawyers cannot give them explicit answers about whether a particular practice complies with the law. This was one of the reasons cited by Ontario for the drafting of a separate privacy law in that province.[27]

Such vagueness is not necessarily such a bad thing. Although businesses are concerned that some of their practices may fall into a gray area with respect to compliance, people are less likely to sue 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. This is, in fact, how many Canadian privacy commissioners resolve disputes.

For marketers, the choice of the appropriate form of consent is critical to balancing privacy compliance with increased distribution and thus implementing permission-based marketing. If the choice discounts the privacy interests of the target population, customers may well be lost and, perhaps more importantly, the seller may be the subject of regulatory action and adverse publicity.

On the other hand, if the choice is too cautious, e.g., reliance on opt-in consent, potential recipients may be lost. Thus, 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 considering how to choose the appropriate form of consent.

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, even if it is properly protected, are a breach of the legislation. Further, the choice of inappropriate provisions for security may lead to costly upgrading.

The importance of the concept cannot be over emphasized. Concerns about the sensitivity of personal health information and linking have led to court decisions that have effectively granted "privacy" protection even though the information was stripped of all identifiable information in one case[28] and the individual was dead in another.[29]

PIPEDA does not define the term "sensitive information," noting in ¶4.3.4 of the appended schedule that "[a]lthough 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." The next paragraph specifies that the "reasonable expectations of the individual" are also relevant in

obtaining consent. For this reason, it is important to note that concerns about the sensitivity of different types of information vary with the culture.

As one example, differences between the attitudes of Europeans and Americans about the role of government in their lives exacerbated the negotiations over the Safe Harbor 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 object to questions about political affiliation or ethnicity. Americans answer these questions routinely, but are sensitive about financial disclosure and have an inherent distrust of government's ability to protect their rights.

Those areas that are considered generally sensitive in Canada may be inferred 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,[30] Canada uses secret ballots. Collecting information on how people actually voted may be considered sensitive and require consent.

Similarly, any collection, use, or disclosure of information concerning the fundamental freedoms identified under Section 2 of the Canadian Charter of Rights and Freedoms[31] or Section 15(1) will likely be regarded as sensitive. Section 2 enumerates freedom of conscience and religion; freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication; freedom of peaceful assembly; and freedom of association. Section 15(1) provides that all people are equal before the law without discrimination, including that based on race, national or ethnic origin, color, religion, sex, age, or mental or physical disability.

Not all the rights provided in the *Charter* are equally sensitive. "Sensitivity" is likely to be based on the abilities of others to use such information to take 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 and a list of names identifying such persons as male or female may not be considered particularly sensitive. However, a list of attendees at a local synagogue or mosque, or members of the Catholic Church who are also active in Campaign Life, would most likely be considered much more sensitive.

Other concerns may arise only if the information is transferred out of the jurisdiction. In British Columbia, a union was concerned about outsourcing and obtained an opinion from a lawyer with the American Civil Liberties Union regarding the implications of the USA Patriot Act[32] on information outsourced to a U.S. business for processing. The primary concern was that the U.S. government could access the information without the consent or knowledge of the individuals involved. The Office of the Information and Privacy Commissioner for British Columbia is now assessing these concerns,[33] and the Government of British Columbia has made a submission to the Commissioner stating that it will amend the public sector privacy legislation.[34] In the meantime, individuals in British Columbia are raising concerns regarding other cross-border transfers of personal information in other contexts such as education.

Generally Sensitive Areas

Initial privacy concerns about the development of the Internet and e-commerce centered in large part on the use of cookies[35] and online profiling.[36] Many consumers now realize, however, that if properly used, cookies contribute considerably to an enjoyable online experience. Ordinary consumer transactions do not cause significant privacy concerns because the information about most people's 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 some product is an indication of someone's lifestyle choices, health, or religious affiliation, consumers will have legitimate concerns about the collection of information regarding their purchases.

Personal Health Information

Health information is a complex area when it comes to privacy concerns. Applying the discussion earlier and in the side bar on page 103 regarding the concept of sensitivity, medical conditions that reflect lifestyle choices or basic reproductive abilities and choices are generally considered quite 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. Several of these factors may be associated with a specific medical condition, such as AIDS, and these can have a multiplier effect that only heightens sensitivity.

When dealing with human emotional responses, however, it is hard to find a reliable formula. Notwithstanding the stigma surrounding smoking in North America, a diagnosis of lung cancer does not seem to be as sensitive a piece of personal information as a diagnosis of AIDS. But people suffering from a medical condition are becoming more aggressive in seeking out information, including Internet searches, about their condition and possible treatments.[37] If the appropriate degree of care is used in obtaining consent and protecting the information, a tightly targeted marketing relationship can be developed.[38]

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 publicly funded health care in contrast to the United States where private funding and a more open market is the norm. Certainly doctors in the two countries appear to take different approaches to direct-to-consumer (DTC) advertising of pharmaceuticals. In a survey of 500 physicians, the U.S. Food and Drug Administration found that American

doctors reported DTC advertising to be helpful in prompting valuable discussions with their patients.[39]

The Canadian view was expressed in a 2003 editorial in the *Canadian Medical Association Journal* that expressed concern that patients would 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.[40] The editorial specifically cited a problem with an asthma medication and the recommendations of a coroner's jury that pharmaceutical companies improve their product information.

Lack of trust, particularly in such areas as health, can exacerbate sensitivity concerns to the degree that some individuals will claim an interest in even their health information even without personally identifiable data. IMS Health Canada, a company that collects information about doctors' prescribing habits, takes the position that such data are required by patients to become informed consumers.[41] The Canadian Medical Association and others argue that the anonymized personal health information of their patients should not be collected without consent and sold to drug companies to use in advancing their own self-interest in the sale of their products.[42]

Fundraising for Charities

In British Columbia and Québec, the privacy laws apply to charitable and nonprofit organizations. The more mainstream organizations in this group (e.g., a regional, government-funded art gallery) should not have particular concerns about sensitive information beyond those typical of a commercial enterprise. On the other hand, where an arts group has expressly associated itself with particular political or social positions or groups, such as a theater 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 necessary for transfers of lists between groups. When lists are traded between organizations that appeal to similar groups, the operative question becomes whether the degree of similarity is high 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. When, however, the school then sent school newsletters to the sponsors, they received a vociferous complaints. 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 people 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.[43]

Students

The sensitivity of information about students more often arises from their age and status in society than from the nature of the information. Generally, concerns over such information have arisen in the United States, and there is no evidence of widespread concern in Canada. In the United States, the Children's Online Privacy Protection Act requires websites targeting children under thirteen years of age to obtain the parent's consent before collecting, using, or disclosing personal information. Also in the United States, certain ancillary provisions of the No Child Left Behind Act[44] came into effect in September 2002, which allow parents to exclude their children from personal data collection at school where the information is used for noneducational marketing. Schools must also notify parents of their right to opt-out. In these situations, linking and secondary marketing purposes would thus appear to make student information more sensitive.

Other 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. The best illustration of how additional purposes can heighten sensitivity is the finding of the federal Privacy Commissioner in the Air Canada matter.[45] Air Canada not only used Aeroplan members' information for purposes of advertising products and making promotional offers, but it also 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 unobjectionable 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.[46]

Other practices that may also heighten sensitivity include linking of information from other transactions and sources, particularly if from outside the organization; disclosure 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 to pursue. 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 some 190,000 customers for sale as one of its key assets.[47] Toysmart's website had promised that personal information would never be disclosed to third parties.[48] The Federal Trade Commission and the attorneys general of several states intervened and eventually the data were destroyed.

Since then, there have been several similar cases, all in the United States.[49] What makes these cases particularly interesting is that the mergers and 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.

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. It can be argued, however, that where the organization demonstrates that it has strong security measures in place, and where the accuracy of the privacy policy and the nature of the uses and disclosures stated can be easily verified, these factors will influence the level (explicit or implied) of the consent that is needed.

Certainly, the principle underlying private sector privacy seal programs such as TRUSTe, BBBOnline, and WebTrust is that individuals will regard sites displaying these seals as more trustworthy and better places to do business. The primary concern of marketers will usually be the handling of information, such as payment data, that is likely to be the target of identity theft. Technological advances mean that reasonable security for online payment requires constant monitoring.

Canada's first privacy class action was filed in Regina, Saskatchewan, on February 3, 2003,[50] under that province's class action law, which came into force January 1, 2002.[51] The suit apparently did not rely on PIPEDA as a basis for liability, and Saskatchewan does not have a private sector privacy law of general application. It arose out of the loss of a hard drive containing financial and account information on an estimated one million people, thereby placing each of them at higher risk of identity theft.

What Is Appropriate Consent?

Unfortunately, there is no formula for identifying the appropriate level of consent required in a particular context. The basic principles of contract formation and the cases regarding tickets, exculpatory clauses, and unconscionability do, however, provide guidance. The quality (or enforceability) of the consent depends 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.

Canadians tend to borrow the wording used in the United States to describe the two basic forms of consent—opt-in as opposed to opt-out. An opt-in consent requires some affirmative action, such as a signature or checking off a box. Lack of response assumes that the individual does not consent to the proprosed collection, use, or disclosure of the information. In an opt-out consent, people who do not respond to the privacy notice are presumed to have consented to its collection, use, and disclosure. The term opt-out is also used in a separate context to describe the right of the individual to withdraw the consent initially obtained or to opt-out at any time.[52] 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[53] 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, or even the dominant, forms of either. A 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 people do not agree with the terms of the privacy notice, presumably they would not return the completed form.

In the United States, marketing organizations have strongly opposed mandated opt-in consent for a variety of reasons.[54] Maintaining that "information is the life blood of the U.S. economy,"[55] they contend that an opt-in system would increase the cost of doing business. They also posit that consumers are in fact making informed choices and 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. The privacy notices are overly broad, excessively long, and difficult to read, resulting in considerable criticism.[56] One study found that the notices were generally written at a third-to-fourth-year college reading level instead of the junior high school level that is recommended for materials written for the general public.[57] Some critics attribute the problem to an inherent conflict of interest; financial institutions have an incentive to create confusing privacy notices and difficult to follow opt-out procedures.[58]

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 negate it. I share the view that such presumption tends to put the responsibility on the wrong party." He went on to say that in future matters under review the opportunities for opt-out consent would be "limited" and permitted only after consideration of "due regard both to the sensitivity of the information at issue and to the reasonable expectations of the individual."

Since the Air Canada finding, the Privacy Commissioner's successor has specified a number of conditions an organization must meet to justify reliance upon the opt-out form of consent, including:

> (1) The personal information must be clearly nonsensitive 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 con-

sent to, secondary purposes and must notify the individual of this procedure at the time the personal information is collected.[59]

Despite the fact that opt-out provisions appear to have inherent structural problems, implied consent in general is still available, according to two recent Canadian court decisions. In *Marquis v. Journal de Québec*,[60] the Québec Court of Appeal considered whether two seventeen-year-old hockey players had impliedly consented to the publication of photographs and interview comments about 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*[61] and Section 5 of *La Charte des droits et libertés de la personne,*[62] but not under Québec's Loi du secteur privée,[63] which excludes journalistic activities.

During a ten-minute interview, a journalist took notes and a photographer took fourteen 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. 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, stating that "*[a]ny waiver to the right to privacy must be clear, subject to both full disclosure, and the free and informed consent of the waiving party.*"[64]

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

What Is Public in Toronto May Be Private in Berlin

Cultural background and national origin play a major role in what information people regard as "sensitive." This fact is perhaps best illustrated by a brief survey of how countries specify various types of personal information that must be considered sensitive and either require more explicit consent for collection, use, or disclose of this type of personal information or prohibit its collection altogether.

In brief, many democratic countries regard information about an individual's religious, political, or philosophical beliefs as being sensitive and restrict its collection, use, and disclosure, as noted below:

United Kingdom:. The U.K.'s Data Protection Act 1998 in section 2 defines "sensitive personal data" to mean personal data regarding: (a)the racial or ethnic origin of data subjects; (b)their political opinions; (c)their religious beliefs; (d)trade union membership (as defined by the Trade Union and Labour Relations Consolidation Act 1992); (e)their physical or mental health; (f)their sexual lives; (g)their actual or alleged commission of any crimes; or (h)the record of any judicial 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: Australia has a similar list of prescribed types of sensitive information, and Australia includes information about the individual's "lifestyle, character, or reputation."[1] Organizations are prohibited from collecting such information without consent. There is, however, an exemption for nonprofit 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 commits to the individual that the information will not be disclosed without the individual's consent.

Spain: *Ley Orgánica 15/1999,*[2] 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 Spain's Constitution. These require the highest level of explicit consent. There is then a further category that 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 about 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, the law prohibits creating data files for the exclusive purpose of revealing the ideology, union affiliation, religion, beliefs, racial or ethnic origin, or sexual life of an individual.

France: *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. The maintenance of membership lists, however, by groups such as churches, political parties, and unions is specifically allowed.

Germany: Section 28 of Germany's *Bundesdatenschutzgesetz*[3] 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 offenses, administrative offenses, 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.[4] 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.

Endnote

1. *Privacy Amendment (Private Sector) Act 2000,* Act No. 155 of 2000, that came into force on December 21, 2001.
2. *Ley Orgánica 15/1999, de 13 diciembre, de Protección de Datos de Carácter Personal.*
3. Vom 20.12.1990, BGBI. I S. 2594.
4. *Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze,* BGBI vom 22.05.2001 S.904.

On appeal, the court agreed that there was no express consent to publication. The appeal court found, however, that consenting to an interview with the journalists is implied consent to publication and dissemination.[65] 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 material as the complainants were only months away from the age of majority.

In *Thomas v. Robinson,*[66] to date the most significant judicial decision concerning PIPEDA, the court was asked to determine whether PIPEDA applied to a database of life insurance agents. Insurance companies 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 to expedite 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 applicants had consented in writing to the investigation as well as to the use of subcontractors for that purpose. They also agreed to the relevant insurance company's keeping a file on an ongoing basis.

There was, however, no express consent to the subcontractor maintaining a file. The judge found that such consent could be implied and that the general purpose for the collection and use of the information had been communicated to the individuals. He cautioned, however, that "If the information in the database is to be used in respect of a new application, then documentation supporting that new application should contain notice of the intention to use the existing information, and should seek the applicant-agent's consent."[67]

Thomas means that consent given prior to PIPEDA continues to be valid notwithstanding the coming into force of PIPEDA. The federal Privacy Commissioner has recently issued a fact sheet providing guidance with respect to dealing with pre-PIPEDA personal information.[68]

In a number of decisions, the federal Privacy Commissioner has also identified additional items to be added to the privacy notice and consent,[69] particularly with respect to secondary marketing. These include:

(1) Make the purposes understandable.

(2) Ensure that the intended uses and disclosures are well-defined in respect of: the types of information to be used or disclosed; the parties to which the information is to be disclosed; and the purposes for which information is to be disclosed.

(3) Ensure that the individuals are notified of their opportunity to withdraw consent and provided with 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 the material elements of any agreement between the parties for the use of personal information. A more recent example of what not to do when seeking consent for marketing purposes can be seen in PIPEDA Case Summary #244.[70]

Conclusion

For marketers and advertisers who are prepared to adopt to a new competitive environment, Canada's new privacy laws may turn out to be more of a blessing than a curse. The adoption of permission-based marketing will open up significant opportunities for more effective and efficient targeting of marketing and advertising 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 transactions, personal information and consent should not be that difficult to obtain for normal marketing purposes. The debate over opt-in consent versus opt-out consent exaggerates the supposed difficulties. Finally, the limited evidence available to date indicates that the courts are prepared to take a reasonable approach to the use of implied consent.

Endnotes

1. Data Protection Directive 95/46/EC (OJ L 281 Nov. 23, 1995) (gives EU citizens rights over the use and processing of their data, including rights of access, notice and choice, and the right of correction and deletion of data). LEXIS.com provides a useful summary of EU Directives, using the following path: Legal/Legal (excluding U.S.)/European Union/ Legislation & Regulations/Business Guide to EU Initiatives/Data Directive.

2. Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, IV(5) HARVARD LAW REVIEW (Dec. 15, 1890), *available at* faculty.uml.edu/sgallagher/harvard__law_review.htm.

3. *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) (trial court found that patients have an interest in their anonymized health information; decision overturned on appeal).

4. *See* William Prosser, *Privacy*, 48 CALIF. L.J. 383 (1960); *see also* RESTATEMENT (2D) OF TORTS § 652A (1977).

5. *See See* www. privacyinternational.org (current compendium of laws and regulations). Privacy International is a London (England)-based human rights group formed in 1990 "as a watchdog on surveillance and privacy invasions."

6. For an alternative discussion of the basics of fair information practices, *see* Anne Cavoukian & Tyler J. Hamilton, THE PRIVACY PAYOFF: HOW SUCCESSFUL BUSINESSES BUILD CUSTOMER TRUST 4455 (2002).

7. This model is used in most European countries (e.g., Commission Nationale de l'Informatique et des Libertés in France).

8. This approach is used in countries such as Canada, Australia, and New Zealand.

9. For a discussion of each of the categories, see Mark Berthold & Raymond Wacks, ch. 4, *Data Privacy and the Common Law*, *in* HONG KONG DATA PRIVACY LAW: TERRITORIAL REGULATION IN A BORDERLESS WORLD (Sweet & Maxwell Asia 2003).

10. S.C. 2000, c.5, as amended by S.C. 2000, c.17, s.97.

11. 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."

12. *Constitution Act, 1867* (U.K.), 30 & 31 Vict., c.3, s.92(7); reprinted in R.S.C. 1985, App. II, No. 5.

13. Section 4(1) of PIPEDA provides that the Act 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 Labor Code, and there is a significant body of case law determining whether federal or provincial labor 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 labor law. 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 nonprofit and charitable organizations trading in membership or fundraising lists.

14. Citizens' Insurance Co. v. Parsons (1881) 7 App. Cas. 96. *See* PETER W. HOGG, CONSTITUTIONAL LAW OF CANADA 20–2 (Toronto: Carswell 1997) (discussion of this case).

15. [1989] 1 S.C.R. 641.

16. PIPEDA § 5(3).

17. For example, subsection 5(3) was cited in PIPEDA Case Summaries #166, 188, 195, 202, 211, 217, 219, 264, 265, and 273.

18. L.Q. 1991, c. 64.

19. 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.

20. SOR/2003–374.

21. British Columbia: *Personal Information Protection Act,* Bill 38–2003; Alberta: *Personal Information Protection Act*, S.A., Ch. P-6.5.

22. Canada Gazette, Part I, Sat., Apr. 10, 2004; Vol. 138, No. 15.

23. Section 3(2)(c). On July 27, 2004, the Office of the Information and Privacy Commissioner of Alberta released a document entitled *Questions and Answers Regarding the Application of PIPEDA, Alberta and British Columbia's Personal Information Protection Acts (PIPAs)* by posting it at http://www.oipc.ab.ca. The document was prepared in consultation among the offices of the privacy commissioners of Alberta, British Columbia, and Canada.

24. Section 52, B.C.; section 52, Alberta.

25. David Loukidelis, Thoughts on Private Sector Privacy Regulation, Speech Presented to British Columbia Freedom of Information and Privacy Ass'n (Nov. 24, 2003), *available at* http://www.oipcbc.org/publications/speeches_presentations/FIPAPIPAspeech112403.pdf.

26. Section 57(1), B.C.; section 60(i), Alberta.

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

28. *See* Northwestern Mem. Hosp. v. Ashcroft, 362 F.3d 923 (7th Cir. 2004) (Posner, J.) ("Even if there would be no possibility that a patient's identity might be learned from a redacted medical record, there would be an invasion of privacy.")

29. *See* the decision of the Icelandic Supreme Court in Ragnhildur Gudmundsdottir v. The State of Iceland, No. 151/2003, decided Nov. 27, 2003 (plaintiff objected to the medical records of her deceased father being entered into Iceland's health sector database because of the potential that her privacy could be invaded by linking information in the database).

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

31. *Id.*

32. USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified in scattered sections of 8 U.S.C.).

33. Office of the Information and Privacy Commissioner for British Columbia, Request for Submissions: Assessing USA Patriot Act Implications for Privacy Compliance Under British Columbia's Freedom of Information and Protection of Privacy Act, May 28, 2004, *available at* www.oipc.bc.ca.

34. Government of British Columbia, Submission to the Information and Privacy Commissioner for British Columbia: Examination of USA PATRIOT ACT implications for personal information of British Columbia residents involved in outsourcing of government services to U.S.-linked service providers (Victoria, B.C.: Government of British Columbia, Ministry of the Attorney General, July 23, 2004).

35. *See, e.g.,* www.cookiecentral.com (additional information regarding cookies).

36. *See, e.g.,* FEDERAL TRADE COMM'N, ONLINE PROFILING: A REPORT TO CONGRESS (June 2000), *available at* www.ftc.gov; Jay Lyman, *Europe Proposes Banning Web Cookies*, E-COMMERCE TIMES, Nov. 1, 2001, *available at* www.newsfactor.com/perl/ story/14513.html#story-start.

37. *See, e.g.,* Julie Gilbert, Gale Murray & Ruth Corbin, *Consumers and Healthcare in Ontario: Are Patients Becoming Consumers* (Change Foundation, Nov. 2001), *available at* www.changefoundation.com.

38. *See* FTC File No. 012 3214 *In the Matter of Eli Lilly & Co.* (Jan. 18, 2002), *available at* www.ftc.gov/opa/2002/01/elililly.htm (major drug company agreed to settle FTC charges regarding the unauthorized disclosure of sensitive personal information collected from consumers through its Prozac.com website).

39. U.S. Food and Drug Admin., Food and Drugs Act Releases Preliminary Results of Physician Survey on Direct-to-Consumer Rx Drug Advertisements, FDA Talk Paper T03–03, Jan. 13, 2003, *available at* www.fda.gov/bbs/topics/ANSWERS/2003/ANS01189.html.

40. Editorial, *Drug Marketing: Unsafe at Any Dose?*, 167(9) CAN. MED. ASS'N J. 981, Oct. 29, 2002.

41. *See* Anita D. Fineberg, *The Personal Information Protection and Electronic Documents Act: Physician Prescription Data and Canadian Health System Reviews*, 23 HEALTH L. CAN. 1 (2002) (Fineberg is corporate counsel and chief privacy officer for IMS Health Canada); Christopher Jones, T. Murray Rankin & 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 They Write?*, 14 CAN. J. ADMIN. LAW. & PRAC. 225 (2001) (article was based on research initially carried on for IMS Health Canada.; 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 has intervener status.

42. *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).

43. Ontario Ministry of Consumer and Business Services, *A Consultation on the Draft Privacy of Personal Information Act, 2002* (2002) (section 26 and commentary), available at http://www.cbs.gov.on.ca/mcbs/english/pdf/56XSMB.pdf.

44. No Child Left Behind Act of 2001, Pub. L. No. 107–110, 115 Stat. 1425 (codified in scattered sections of 20 U.S.C.).

45. PIPEDA *Case Summary #42: Air Canada allows 1% of Aeroplan membership to opt-out of information sharing practices*, Mar. 20, 2002. All PIPEDA case summaries are posted at www.privcom.gc.ca/cf-dc/index2_e.asp.

46. *Id.*

47. *See* Federal Trade Comm'n, FTC Announces Settlement with Bankrupt Website, Toysmart.com, Regarding Alleged Privacy Policy Violations, *available at* www.ftc.gov/opa/2000/07/toysmart2.htm (July 21, 2000); Fed. Trade Comm'n v. Toysmart.com, LLC, 2000 U.S. Dist. LEXIS 21963 (Bankr. E.D. Mass. 2000).

48. Paul Jones, *Privacy Law Will Require New Due Diligence*, LAW. WKLY., Sept. 15, 2000.

49. *See In re* Egghead.com, Inc., Case No. 01–32125-SFC-11 (Bankr. N.D. Cal.); *In re* Living.com, Inc., Case No. 00–12522 FRM (Bankr. W.D. Tex.); *In re* eToys, Inc., Case Nos. 01–706 through 709 (MFW) (Bankr. D. Del.).

50. Richard Foot, *Class Action Says Firm "Negligent" in Data Loss*, CAN. NAT'L POST, Feb. 4, 2003.

51. *The Class Actions Act,* Ch. C-12.01, S.S., 2001.

52. Principle 4.3.8 of Schedule 1 to PIPEDA.

53. *See* Principle 4.3.6 (the way in which an organization seeks consent

may vary, depending on the circumstances and the type of information collected).

54. Fred H. Cate and Michael E. Staten, *Protecting Privacy in the New Millennium: The Fallacy of "Opt-In," available at* www.netcaucus.org/books/privacy2001/pdf/cate.pdf.

55. *Id.*

56. *See* John Swartz, *Privacy Policy Notices Are Called Too Common and Too Confusing*, N.Y. TIMES, May 7, 2001; Robert O'Harrow, Jr., *Privacy Notices Criticized: New Bulletins Unclear, Some Lawmakers Say*, WASH. POST, 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, Feb. 15, 2002; Michael Bartlett, *Privacy Groups Blast Info Sharing By Financial Institutions*, NEWSBYTES, May 2, 2002; Comment, In the Matter of Financial Services Modernization Act a Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. § 1608, Joint Statement of the Electronic Privacy Information Center, Privacy Rights Clearinghouse, US PRG, and Consumers Union Before the Department of Treasury, May 1, 2002, *available at* http://www.epic.org/privacy/financial/glb_comments.pdf; 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*, WALL ST. J., May 30, 2002.

57. Mark Hochhauser, *Lost in the Fine Print: Readability of Financial Privacy Notices*, *available at* www.privacyrights.org/ar/ GLB-Reading.htm.

58. Bartlett, *supra* note 30.

59. PIPEDA Case Summary #207, Cellphone company meets conditions for "opt-out" consent, Aug. 6, 2003, *available at* www.privcom.gc.ca/cf-dc/index2_e.asp.

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

61. L.Q. 1991, c. 64..

62. L.R.Q., c. C-12.

63. L.R.Q., c. P-39.1.

64. *Supra* note 34, at 311 (emphasis in the original).

65. *Ib*. at 315.

66. 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.

67. *Id*. at 27.

68. Office of the Privacy Commissioner of Canada, *Fact Sheet- Best Practices for dealing with pre-PIPEDA personal information (grandfathering)* (July 27, 2004), *available at* www.privcom.gc.ca/fs-fi/02_05_d_22_e.asp.

69. 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*.

70. PIPEDA Case Summary #244, *Alleged disclosure of personal information without consent for secondary marketing purposes by telecommunications company "A,"* Nov. 7, 2003, available at http://www.privcom.gc.ca/cf-dc/2003/cf-dc_031107_02_e.asp.