**IMPLEMENTING THE CANADIAN PRIVACY FRAMEWORK WHEN DOING BUSINESS ONLINE**

INTRODUCTION

The *Personal Information Protection and Electronic Documents Act* (*PIPEDA*) was introduced

- and applies to the private sector since January 2004. Implementing PIPEDA while doing business online bring many challenges. First, an organization doing business across Canada needs to comply with PIPEDA but also with other province's privacy legislation (such as the legislation in Quebec which was found to be substantially similar to PIPEDA, the Alberta legislation and the British Columbia one) and perhaps even with industry guidelines such as the *Canadian Code of Practice for Consumer Protection in Electronic Commerce* and CMA guidelines. Therefore, using the _____ privacy framework is useful. Second, it can be a real challenge to translate the legal framework into business practices which are specific to the online industry.

In the context of new technologies, it is sometimes difficult to pinpoint what constitutes personal or personally identifiable information (*PI*). For instance new types of data have emerged recently such as email addresses, clickstream, Internet Protocol (*IP*) address, and other data collected from various online tracking methods such as cookies, web bugs and spyware.

PIPEDA defines personal information *as information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization*.[1] Since the definition of personal information is drafted broadly, one needs to address whether email addresses, IP addresses and other data collected through online tracking methods should also be included in the definition of personal information.

The issue of considering email addresses as personal data is an important one. One may argue that email addresses could constitute personal information only if linked to an identifiable individual. This is problematic given that an email address, although usually used by one single individual, may belong to more than one individual. Also, there maybe a distinction to make between a personal e-mail address or a business on. Although *business* e-mail addresses are in certain cases either not regulated by privacy legislation (in certain Canadian provinces), or their status is unclear (such as in PIPEDA), e-mail addresses are usually considered personal information and PIPEDA[2] regulates the collection of e-mail addresses or at least of *personal* e-mail addresses.

There are also many issues that could result by considering email addresses as non-personal. For instance, many spammers are collecting email addresses from public spaces on the Internet and using them for unsolicited commercial emailings. Spam is such an enormous challenge that if we were to consider email addresses as non personal, it would give spammers free rein to collect emails addresses and purchase these addresses from third party lists, without the knowledge and consent of the online users. This practice constitutes unfair processing of personal data and is inconsistent with the *purpose* principle found in PIPEDA.

Some argue that data collected from automatic tracking methods constitutes personal information only if linked to an identifiable individual. Many if not most IP addresses are *dynamic* and changing every time a consumer connects to the Internet, as opposed to *static*, or unique to that consumer's computer. It is difficult to link dynamic IP addresses to individuals, although technically feasible when using an ISP log files. If static IP addresses were to be used, then they would be more likely to become personally identifiable because they would be linked to an individual's computer. In this case, an IP address would be considered PII.

Ad networks, while supplying banner ads, gather data about consumers who view their ads. This information is linked to the identification number of the advertising network's cookie on the consumer's computer. Other organizations use cookies in order to make the online session better to remember the users password during an online session, etc.) Cookies are small pieces

of code transferred from a web site to a home computer when a user is surfing or visiting a web site. Web sites often place them so that they can ensure that their server will recognize a specific online user through the many steps in a visit to a web site or even when the user returns to the web site and time has passed between visits. Many web sites use their own cookies to keep track of shopping carts, to remember the preferred language of the online user and to personalise the online users' experience on their web site.

Given that the information collected by cookies is usually anonymous, since it does not include the name of a specific person or an email address, it might not be considered personal information. At the same time, there are still privacy issues surrounding this type of data. The information or profiles derived from tracking online users' activities on the Internet may be linked or merged with the PI of these users (for example with the user's offline purchases, information collected directly or voluntarily from the users, for example through surveys and registration forms). In addition, certain non-PI data collected over time, although initially not considered personal data could eventually be considered personal data. For this reason, although this type of data is usually not considered PI, certain requirements such as the disclosure of the collection and obtaining the users' consent prior to the collection of this type of data might be necessary and PIPEDA may regulate this data.

## 1. Accountability

Organizations should mention in its privacy policy the name of the person who is accountable for the organization's compliance with PIPEDA. They must educate their employees about the importance of maintaining the confidentiality of personal information.[3] Some basic measures include the necessity for their employees to sign confidentiality, privacy and security agreements. In addition, for employees accessing subscriber files, stricter written contractual agreements, are needed to ensure that they understand that they are accountable for the business privacy and information practices.

In certain cases, organizations could transfer the data for processing or providing support for the internal operations of the web site or service, or for other purposes such as technical support and order fulfillment. These businesses should bear in mind that they are still responsible for personal information initially in their custody that has been transferred to a third party.[4] Organizations should take all reasonable steps to ensure third parties involved in a transaction, for example any party contracted to their organization to conduct activities such as data processing or data mining, also have adequate security measures.

Certain organization's website privacy policies advertise that they may share any of the personal information that they collect among affiliated or related entities or that they might disclose any of the personal information collected about the online user to other organizations with whom they have joint marketing agreements. Very often, web sites' statements are so broad on the transfer issue that it does not enable online consumers, who do not have the names of these other parties or marketers, to verify their privacy policies. These statements open the door for sharing consumers' personal data with many entities. As long as the consumer does not actively opt out of participation, there is the potential that personal information might be widely broadcast. The privacy policy should list and name each related or affiliated company or any other third party that could have access to the online user's personal data. Organizations should also not share the personal information with third parties unless these parties agree to be bound by the terms of its own privacy policy.

## 2. Identifying Purposes

### 2.1 Data Collected by Online Tracking Tools

Internet users are concerned that their online activities could be tracked over time. One way to collect personal information of online users is through cookies. Some recent technologies such as web bugs, spyware and other similar devices are also raising privacy concerns.

A *session* cookie, is just like any other cookie except that it is set to delete itself within a relatively short period of time, perhaps within ten minutes after an online user would leave a specific web site. This type of cookie is typically used for remembering information only for a short duration, such as what the online user has stored in his/her shopping cart. Since the session cookies are short lived, they do not have the same privacy implications.

Some web sites also rent out space on their web pages to third parties, often for placement of advertisements. Third party cookies are placed by entities other than the web site and can be used to collect information that would reflect activity at multiple web sites. The online advertising companies use these cookies to manage ad frequency, and to track the online user movements between the many sites in which they place advertisements, in order to learn about the online users' interests based on the sites that they visit or track their purchase in the context of "affiliate programs" used for online marketing referrals and e-commerce transactions.

Privacy concerns surround cookies as they may be used for illegitimate purpose such as collecting online users' personal data without their knowledge and without having first obtained the users' consent. Their use, even if legitimate, should be disclosed in the organization's website privacy policy.

A recent technology called *web bugs* (or special links in web pages) are used to track down the activities of an online user and gather information about the user through its computer. This technique allows web sites to track details about information such as when online users read their emails, and whom the online users might be forwarding messages to. Web sites might use web bugs to help track how many people have visited a particular web site or to track what kinds of browsers are being used, the web sites visited (content of the pages read) and for how long the user stayed on each page visited before clicking to another web page. A web site operator can use web bugs for legitimate purposes, such as counting the number of people who visit a web page. Given that web bugs can also be used to invade someone's privacy by collecting personal data without the user's knowledge or consent, their use should be disclosed in the organization's privacy policy.

Recently, a category of spying software called *spyware* has emerged. Spyware is usually downloaded into a computer when the user downloads free software from the Internet. Spyware is software that gathers information, monitors both online and offline user activities and uses the user's Internet connection to send the gathered data to another server on the Internet, without the online users knowledge or approval. In may cases, spyware gathers information about the online user and his/her activities, web-browsing habits or record his/her passwords, credit card information or other e-commerce data, so that it can know more about the online user. The downloading of such software into an online user's computer should be clearly disclosed to the online user.

### 2.2 Public Spaces on the Internet

Another way for organizations to collect personal information or email addresses of online users is by gathering information from public spaces on the Internet, such as public email directories, emailing lists, news groups, or even chat rooms. Certain tools are available on the Internet that may help marketers collect email addresses. These programs, for example, will search web

sites, which have to be specified in advance by a list of URLs, or keywords related to a predefined field of interest and, subsequently, will provide all email addresses found on the web sites/web pages.

Studies show that email addresses posted on web sites or in newsgroups attract the most spam. [5] [6]

The practice of collecting email addresses from public spaces on the Internet and using them for commercial emailings goes against the privacy framework. This practice could constitute unfair processing of personal data and would go against the *purpose* principle.[7] Online users usually disclose their email addresses for a specific purpose, such as participating in a newsgroup. This purpose is quite different from commercial emailing. Therefore, in order to make this type of collection legal, the consent of the individual is required before information can be used for a new purpose such as marketing to this user.

Also, in the U.S, the recent CAN-SPAM Act[8] is recommending that this type of data collection be illegal and bans sending commercial email to addresses that were gathered *using automated means*.

Organizations should therefore avoid collecting email addresses from public places on the Internet.

### 2.3 New purpose to be identified

#### 2.3.1 Secondary internal uses: Marketing Back

Internal secondary uses to data legitimately collected include marketing back to the consumers. It is debatable whether an organization could use data or an email address legitimately collected (such as when a user registers to a website or purchase something on the Internet) to promote future offerings. The purpose and use of the data collected would then be different that the purpose disclosed at the time of the collection (in the event that the organization privacy policy did not disclose the fact that personal data will be used for future promotional offerings). Many industry observers argue that a previous business relationship should entitle an online marketer to contact the user by email for commercial purposes, if certain requirements are respected, such as providing an opt-out mechanism.

Canadian Code of practice for Consumers Protection in Electronic Commerce recommends that the online vendor's policies on privacy and unsolicited email information be available to consumers before they engage in transactions.[9] Organizations should allow online users the opportunity of refusing the collection of their personal data and informing the web site that they do not wish to be solicited.

#### 2.3.2 Secondary external uses: Selling the data

External secondary uses, such as disclosing the collected information to third parties, go beyond the use for which the information was initially provided or collected. The online user's prior consent to this external secondary use is required since it will be used for purposes unrelated to those for which the information was initially obtained or described in the privacy policy.[10] CMA members should provide consumers with a meaningful opportunity to decline to have their name or other information used for any further marketing purposes by a third party.[11] This opportunity should be provided to the consumer before any information is transferred and should be repeated once every three years, at a minimum.

## 3. Consent

### 3.1 Depending on the type of collection/use made

#### 3.1.1 Purchase of Third Party List

The collection of personal data through the purchase of lists provided by third parties might be illegal. Personal data collected should not be transfered to third parties unless the customer has agreed to such transfer.[12] PIPEDA suggests that the consent to disclose personal information should be manifest, free, and enlightened and must be given for specific purposes, *except where inappropriate*.[13] As an example of a situation when the consent of the data subject would be inappropriate, PIPEDA suggests that it could be impractical for a direct-marketing firm that wishes to acquire a mailing list from another organization to obtain such consent. In this case, this law requires that the marketer that is providing the list to the third party marketer would be expected to obtain consent from the online user before disclosing personal information to the other party.

#### 3.1.2 Mail server or dictionary attacks

In certain cases, e-mail addresses may be gathered through mail server attacks or dictionary attacks. A dictionary attack occurs when a computer program goes through every possible combination of letters in an attempt to guess e-mail addresses. In February 2003, Microsoft filed a so-called John Doe suit in the federal court for the northern district of San Jose, California.[14] The suit did not name defendants, but allowed the plaintiff the power to issue subpoenas as part of the investigative phase of the trial. The defendants are accused of using a *dictionary attack* to discover active Hotmail accounts.[15] In this case, Microsoft alleged that the program guessed millions of random email addresses to see which ones were active. **[FOLLOW UP ON CASE]** This type of collection **[NOT COLLECTION PER SE]** should be illegal given that emails addresses, considered personal information, are collected without the online user's knowledge and prior consent.

### 3.2 Illegal to require consent as a condition of the supply of services

There has been an on-going debate whether an organization may refuse access to online services or products if online users do not consent to the use or disclosure of their personal information for purposes unrelated to such services or products.

The recent Canadian Code of Practice for Consumer Protection in Electronic Commerce states that online vendors should not, as a condition of sale, require consumers to consent to the collection, use or disclosure of personal information beyond what is necessary to complete the transaction.[16] This brings the issue on whether website registers may be illegal in certain cases. **[ELABORATE]**

### 3.3 Consent shall not be obtained through deception: Spyware

One of the privacy concerns with spyware is that depending on the browser's security settings, the software will either download silently on the online user's PC and without any online user action, or present an install dialogue. Online users may choose *I agree* thinking the browser is asking to download a legitimate page-display plugin. The use of spyware should be disclosed to online users in a clear matter.

Consent obtained in such case would be obtained through deception. Online users should be provided clear notice about the type of information collected about them and should be informed before a placement of such devices in their computers. Online users should be entitled to refuse this placement, even if these devices will be used for legitimate purposes.

### 3.4 The way to seek consent may vary depending on the circumstances

PIPEDA suggests that organizations could seek express consent (opt-in) from consumers for sensitive data, and provide implied consent (opt-out) when the information is less sensitive.[17] Individual identifiable data or PI is data that can identify a person directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural, or social identity. Identifiable data might often be linked or merged with existing data already placed in a cookie thereby providing for an identifiable profile of the person concerned. In this case, the consent of the online user is required. On the other hand, when the collected data, gathered though the identification number of an advertiser's cookie, is not linked to identifiable data, the user can be considered anonymous. In such case, the consent of the online user might be implied or obtained through an opt-out mechanism.

The notion of *consent* prior to data collection could be different if the web site is for children or the online services that will be provided is meant for children. The term child is usually defined as a child under 13 years of age. E-Businesses should obtain verifiable parental consent from the child's parent before collecting, using or disclosing personal information from a child, unless the collection is limited to specific circumstances detailed in the law. [18]

Organizations should take special care when dealing with children given that online activities directed at children impose a social responsibility. If there is a reasonable likelihood of collecting, using, or disclosing personal information from or about children, organizations may want to follow appropriate privacy practices. In Canada, this framework includes the Canadian Marketing Association's special considerations for children in its *Code of Ethics & Standards of Practice*[19] and the *Canadian Code of Practice for Consumer Protection in Electronic Commerce*.[20] This legal framework generally defines a child as someone who has not reached his/her 13th birthday.

The U.S. legal framework has a law specific to children's privacy on the Internet COPPA provides that a web site operator should make reasonable efforts (taking into consideration available technology) to ensure that before personal information is collected from a child, a parent receives notice of the operator's information practices and consents to those practices.[21] Methods to obtain verifiable parental consent include (i) providing a consent form to be signed by the parent and returned to the operator by postal mail or facsimile; (ii) requiring a parent to use a credit card in connection with a transaction; (iii) having a parent call a toll-free telephone number staffed by trained personnel; (iv) using a digital certificate that uses public key technology and (v) using email accompanied by a PIN or password obtained through one of the verification methods listed in the law.[22] These measures necessarily imply an opt-in mechanism.

There are certain exceptions from obtaining the parent's consent prior to the collection of the child's personal data. For instance, a web site operator does not need the prior consent of the parent when: (i) contacting and getting information from a child for the purpose of obtaining parental consent;[23] (ii) when responding to a *one-time* request initiated by a child with a promise to delete the information collected and not to recontact the child;[24] and (iii) when responding *more than once to a specific* request.[25] This would be the case if the web site operator responds following a subscription to a newsletter. In the latter case, the web site operator should notify the parent that it is communicating regularly with the child and give the parent the opportunity to stop the communication before sending or delivering a second communication to a child.

The *Canadian Code of Practice for Consumer Protection in Electronic Commerce* states that when contests or clubs are directed at children, vendors may collect children's personal information without parental consent. Online vendors could communicate directly with those children, when they collect the minimum amount of information required to:

- provide the club membership or to determine the winner of a contest;

- limit communications only to those required to provide the club membership;
- in the case of contests, only deal with the parents or guardians of the winner(s) and do not contact the winner(s);
- retain the information only as long as the children remain members of the club or until the conclusion of the contest; and
- make no use of the information other than to provide the club membership or to determine a contest winner.[26]

3.5 Right to withdraw consent at anytime

Online users should be provided with the right to withdraw their consent at any time. They should be informed that the revoking of the consent and the deleting of the users' personal data or refusal of accepting cookies may cause the organization's web site to lose its functionality or any special features that were set up for the user.

## 4. Limiting Collection

See Principles 2 and 3.

## 5. Limiting Use, Disclosure and Retention

PIPEDA states that organizations shall not be using/disclosing PI for purposes other than those for which it was collected, except with prior consent. An online user's personal information may, in some cases, be provided voluntarily by the user such as when he/she registers to a web site or buys products from an e-commerce web site. Online users might also take part in a game or competition provided that they deliver personal data as input for profiles. It could be viewed either as the price to pay to have access to certain information or online services. Despite the fact that users have provided the information voluntarily, a privacy breach might occur if the information collected is then used for a purpose not disclosed at the time of the collection, or is even transferred to an unauthorized party.

If, at the time of collection, the purpose of the collection and use of the data is made clear to the online user, then the consent of the user that voluntarily provided his/her data may be sufficient. On the other hand, if the personal information collected is to be used for a purpose not previously identified, the new purpose must be identified prior to use, and the consent of the online user is required before information can be used for that purpose.[27] Organizations should not assume that an online user that has provided personal data in the context of an online purchase expects that the data will be used for other purposes, although it is generally accepted that a previous business relationship with a specific user entitles an organization to contact this user for offering an advertisement by email upon certain requirements. In order to avoid breaching online users' privacy, organizations that initially collect personal data in the context of a transaction, should disclose that, they intend to use this data for other purposes such as marketing back to the user. Online users should also be provided with the opportunity to refuse such marketing and email solicitations.

PIPEDA also states that PI shall be retained only as long as necessary and if no longer required should be destroyed, erased, or made anonymous. It suggests that organizations should develop guidelines and implement procedures with respect to the minimum and maximum retention periods of PI. For instance, one of the requirements in the DoubleClick settlement is that after three months, data collected in connection with DoubleClick's DART ad serving will be moved offline.[28] This was noted to be an important change in the data minimization and purging policy.

The issue with this principle is the fact that it might against certain Limitations Act; -- E-commerce and online transactions.

## 6. Accuracy

PIPEDA states that PI shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used and that organizations should avoid collecting false/inaccurate data.

### 6.1 Website Registrations

Many web sites request that online users register and provide personal information in order to have access to certain information or products provided by the web site (i.e. the price to pay to obtain certain services or products on the Internet). Many online users provide false data about themselves when applying for a free email account or filling out a web site registration form, in order to access to these so called *free online services* as they perceive it as a simple way to protect their privacy. According to a study by Statistical Research, one in five online users have entered false information to retain their privacy.[29] This affects the quality of the data gathered by organizations.

### 6.2 Online personalization, data mining and advertising networks

PIPEDA's *data quality* principle states that organizations should collect personal information by lawful and fair means, and from reliable sources. This may raise concerns with regards to data being collected, in some cases using online tracking tools, and/or data mined using other technology tools.

Data mining or profiling helps marketers predict future behaviors and trends by discerning patterns from large amounts of data collected from online tracking tools such as cookies and other sources. Based on these assumptions, marketers would be able to deliver personalized online advertisements (i.e. banner ads) which match closely each consumer's interest. However, it is unclear whether this information collected from online tracking tools and other methods can be considered quality data. For instance, a home computer is usually used by different family members. The data collected can be related to many individuals, and therefore, not accurate for one specific individual or user.

PIPEDA states that an organization shall not routinely update PI, unless such a process is necessary to fulfil the purposes for which the PI was collected. It is also debatable whether the collection of data for profiling purposes would be considered as a "process is necessary to fulfill the purposes for which the PI was collected" unless the online user is clearly informed that information will be collected from him/her periodically in order to profile him/her.

## 7. Safeguards

### 7.1 Disclosure of the Security System

PIPEDA states that PI shall be protected against loss or theft, unauthorized access, disclosure, copying, use, or modification. The online user should be informed whether the data collected and stored is secure. Organizations should confirm and disclose in their privacy policy whether they have appropriate security measures in place to protect against the loss, misuse, or alteration of information collected from online users. Most privacy policies are confusing and convey little to the average consumer since it is difficult to communicate relevant and useful technical information in a short statement dealing with a subject as complex as security. Providing specific technical details about security in a privacy policy could be useful for hackers and even serve as an invitation. The privacy policy may for instance specify that the web site is using "*industry standards*" to reassure the online users.
Organizations should also avoid making statements such as "we use the highest security standards" since standards change all the time and it might bring unnecessary liability on the organization in case of a breach of its system.

7.2 Distribution and transfer of data.

PIPEDA specifies that the nature of the safeguards of the personal data collected vary depending on, amongst other things, its distribution.[30] The Canadian Code of Practice for Consumers Protection in Electronic Commerce suggests that organizations should ensure that third parties who are involved in transactions and have access to personal or payment information comply with the security provisions.[31]

Organization may further use a contract to provide a comparable level of protection (at least the same level of privacy protection as originally selected by the individual) while the information is being processed by a third party. Such contracts with business partners should include privacy protection requirements, comparable to the organization privacy policies and practices. Organizations sending personal data to jurisdictions with different and not comparable privacy protection regulation should also take special care in doing do.

7.3 Method of protection: Physical, organizational, technological measures

Physical measures include, for instance, locked computers with passwords and restricted access to offices. Other methods such as organizational and technological measures should also be implemented. Certain sensitive data or data that will not be frequently used on the computer could also be removed from the computer and saved in a secure area offline.

Organizations should also train their staff and introduce policies and guidelines restricting employee access to personal information for unrelated and non-business reasons and limiting access to information technology employees as well as implementing appropriate disciplinary measures for violation. Since the Internet does not sleep, neither should the technical staff responsible for security and systems should be monitored 24 hours a day.

Organizations in the U.S., especially since the events of September 11, 2001, have taken concrete steps to ensure security of their IT systems by naming a Chief Security Officer (*CSO*) or Chief Information Security Officer to plan and oversee information security for the entire corporation.

8. **Openness**

PIPEDA states that organizations should make “readily available” to individuals specific information about its PI handling practices.

8.1 Access to policy without unreasonable effort: Display of the policy.

In 2003, Industry Canada has concluded that, while the majority of ISPs and ESPs make some reference to the use of their subscribers’ addresses for commercial purposes in their *Terms of Agreement*, these provisions are often unclear and not displayed prominently.[32] Many online users would be surprised to discover that they have agreed, by default, to receive some form of commercial solicitation.

A privacy policy shall be clearly posted and be easily accessible. Organizations shall make their privacy policy easily accessible, at a reasonably early stage of the online users’ navigation, at a prominent place on the organization web site’s home page – or at least in a place that is easily accessible from the home page. The privacy policy should be available to online users before they are being asked to “register” to the website or upon being asked to submit PI. Online users may have, using a link to an organization’s website from another website, landed on the organization’s site – but not necessarily on the home page. A link to the privacy policy should be found at the bottom of each web site page, allowing it to be accessible from every web page and not just from the home page.

RECENT JURISPRUDENCE FOR LOCATION OF POLICY

8.2 Using a form generally understandable: Language and Length

The posting of a privacy policy could be viewed as an offer of a contractual relationship with a consumer. Legal counsel is more likely to draft a policy that anticipates any possible eventualities of an ongoing relationship governed by contract. The policy might be drafted with potential contract litigation in mind, employing language that is vague and open ended and that does not clearly delineate reliable information.

Privacy policies should be written using plain, clear, and comprehensive language instead of legal jargon and should take full advantage of visual design features that divide information up into pieces making it easy to find and to read. A privacy policy should also be written in the same language as the web site to which it relates and organizations should take into account their audience: a web site for professionals should not be drafted in the same way as a web site destined to children. The privacy policy should be simple and relatively short, given that it is meant for a general audience, not for lawyers. A policy should not be too long (i.e. not more than three or four pages).

8.3 Update of the Policy / notification of change.

The privacy policy should be updated as new online tracking technology methods evolve, new privacy practices are adopted and new privacy laws are enacted. Organizations should establish certain procedures in order to review their policy and ensure that such policy remains accurate.

Many organizations mention in their policy that: "this privacy policy may be amended from time to time". This imply that, whether an online user registers to use a free online service or purchase something from an online store, it should never neglect to check the privacy policy of the website periodically to ensure that the web site has not suddenly changed its policy. This type of amendment may not be valid depending on how the online user is informed of such amendment,

In Canada, the Ontario Superior Court of Justice has ruled in 2002 in *Kanitz v. Rogers Cable Inc.*[33] that the procedure of notifying users of changes to an online clickwrap user agreement through web posting was adequate.[34] The original user agreement stated that amendments to the agreement could be made at any time, with notice to customers on Rogers' web site. Rogers subsequently amended the agreement, adding the arbitration clause and posting notice of it on the Rogers' customer support web site. The plaintiffs argued that they were given inadequate notice of the amendment, because the process of finding the user agreement on the web site was burdensome and the amendment was buried in the agreement. The court found that although Rogers could have used a different procedure to alert its customers of the new terms, it was entitled to give notice through web site postings.

It might be interesting to note that in the U.S., a recent similar decision to *Kanitz v. Rogers Cable Inc*. raised the issue of whether online users can be unilaterally bound to future changes in user agreements. In *Comb* v. *PayPal Inc*.,[35] the judge concluded that the plaintiffs were not bound by an arbitration clause contained in an amended version of an online agreement, where the originals version of the agreement had been signed electronically by the plaintiffs.

Given that there are no relevant privacy policy jurisprudence regarding modification of terms, this ruling rendered in the context of a clickwrap agreement could be relevant to consider and understand the reasoning of the court with regards to the validity of changes made to an agreement through a web posting.

This type of procedure (web site posting) places the onus on the online users to refer back to the privacy policy web page to ensure that their personal data will not be used in a manner

materially different from that stated at the time of collection may in some cases be burdensome and inappropriate. This depends on the type of change made, the type of data (sensitive or not) collected and whether the organization has the email or mail addresses of its web site visitors or customers for whom it collected data.

When making changes that affect users' privacy, the key principle is to notify the relevant online users and then obtain permission. An online user who has agreed to the collection and processing of his/her personal data should not be required to follow up with the privacy policy of the organization. If an organization has its online visitors or customer's e-mail or home mail addresses, it should send them a notice informing them of these changes, especially if these changes affect the handling of their personal data.

Notwithstanding this requirement, online users should be informed of these changes through a posting on the web site home page and on the privacy policy. For instance, the policy could highlight the recent changes and detail what has been changed and on what date. In the event that the information collected is aggregated or not sensitive, a special link to the changes on the homepage of the web site operator, also present in a *What's New* section of the web site could be sufficient. Still, this notice should also be present on every page that requests or requires users to submit personal information. This should be done at least 30 days before the said update is intended to be effective. In the event of a change in its privacy policy, the organization should specify in the notice of update the reason for such change.

Given that a privacy policy is a promise made to the online user, the organization cannot modify its terms without first notifying the online user and obtaining his/her consent. In the event that the user refuses to agree to the changes, the personal information already collected by the organization prior to the notice of change should be preserved under the prior policy terms. Hence, when a web site changes its privacy policy, the suggested approach is to ensure that the change will only apply to information that is collected from that point forward.

## 9. Individual Access

PIPEDA states that upon request, informing individuals of the existence, use and disclosure of their PI, provide access to challenge the accuracy and completeness of the PI. When it comes to the Internet, all kinds of data can be collected. Deciding on whether access should be provided and, as the case may be, the type of data that should actually be covered by the access principle is a challenge.

### 9.1 Exceptions to the Access Requirement

PIPEDA states that exceptions to the access requirement should be limited and specific,[36] and the reasons for denying access should be provided to the online user upon request.[37] PIPEDA does not specify what would constitute these exceptions.

#### 9.1.1 Data Too Costly to Provide: Charging a fee

The general principle is that organizations could charge a fee, provided that it is not excessive. PIPEDA recommends that an organization responds to an online user's request at minimal or no cost to the user.[38]

Chris Jay Hoofnagle, Deputy Counsel, EPIC states that some of the reasons for denying access include the fact that the information is prohibitively costly to provide.[39] Tony Hadley, Vice President, Government Affairs of Experian, which assists organizations in personalizing and developing customer relationships, suggests that allowing access to marketing databases would be enormously expensive and that existing database architecture would have to be redesigned.[40]

An organization operating a web site could automatically record navigational or *clickstream* data as an online user moves from page to page on a given web site, either for statistical purposes to better design and manage the site or to automatically personalize the initial pages presented to the online user visitor based on such user's historical use of a web site. The costs of providing access to this type of information could be high. The OPA believes that there is little benefit, and much cost, in accumulating this data in a form that could be reviewed intelligibly by the individual at any moment.[41]

Certain members of the OCAOS suggested that ascertaining whether inferences are right or wrong would be difficult and costly with regards to correction of data resulting from data mining tools or inferred data.[42] Organizations should not refuse access on cost grounds, if the online user offers to pay the costs.

#### 9.1.2 Data Containing References to Others: Data derived from tracking tools

An organization could collect personal data through its web sites and/or banner ads, cookies or any other online tracking devices. A web site might automatically record navigational or *clickstream* data as an online user moves from page to page on a given web site. This data may be used by the web site operator either for statistical purposes, such as the management of the web site, or to personalize the initial pages presented to the online user visitor based on such user's previous use of a web site.

In order to authenticate the identity of the access requester, certain web sites require that the identifier (the number associated with the organization cookie) be provided in an access request. This method enables the organization to easily provide access to the online user requester to the data linked to that specific cookie. The privacy issue with this type of access is that the data collected through these devices does not necessarily belong to one single individual. The data collected relates to a computer that may or may not be used only by one person. Perhaps the computer is shared by co-workers, family members, etc. Whether the online users should be entitled to have access to this type of data is not clear.

The fact that this data is not necessarily unique to an individual entails that providing access to an online user to this data may breach the privacy of the other users of the same computer. The profile data, clickstream data and other data that could be collected might reveal significant private information. For instance, an employee's colleague sharing the computer could have a certain embarrassing disease and the data disclosed to the online users requesting the data would be disclosed, therefore embarrassing the co-worker and breaching his/her privacy. These types of privacy issues and potential risks to other online user's privacy need to be addressed in the online environment.

A solution could be that access be provided to an online user requesting it, if the web site is one of general interest and therefore the disclosure of data collected by a cookie would not be revealing anything private about the other computer's user(s).

#### 9.1.3 Commercial Proprietary Reasons: Data derived from data mining tools

Another type of data that presents privacy challenges includes data resulting from information collected either from sample data or from the user, and derived or calculated to result in a value applied to the data subject.[43] For instance, it could be used in evaluating the financial risk of an individual in the case of granting a loan to that person. Practical considerations, privacy and business issues are raised when providing access to this type of data-mined or inferred data.

For instance, the access privacy principle would enable an online user to be informed of the existence, use, and disclosure of his/her personal information and be given reasonable access to that information in order to correct or amend that information when it is inaccurate. The

organization may not be in a position to provide this data-mined or inferred data in an intelligible form to the users or at a low or reasonable cost. In addition, it might be impractical and difficult to enable a user to ascertain whether the inferences made and inferred using certain tools or calculations are relevant. These types of data are not usually susceptible to correction.

This type of inferred or derived information could also be in certain circumstances the result of a proprietary model and could provide a competitive advantage to the organization, for instance when the data is an indicator of an online user's future purchase behavior. Disclosing the assumptions or conclusions a business makes might undermine competition by inviting competitors to attempt reverse engineering to proprietary operations and allowing them to free-ride off the analytic work of rivals.

On the other hand, a refusal of access could be potentially harmful when the data is used to make a decision about the customer that would result in an important denial of services such as the granting of a loan. This opens the door for a case by case evaluation. In certain very limited cases, when the data is handled under separate laws or regulations such as credit loan decision, this data could be used to make decisions about individuals and should therefore be available to online users requesting it.

### 9.2 Right of access and correction time

PIPEDA suggests that, upon request, an organization should (i) inform an online user whether or not it holds personal information about him/her, (ii) indicate the source of this information and (iii) allow the user access to it.[44] It also states that organizations should provide an account for the use of this information and a list of the third parties to which it has been disclosed,[45] without specifying the appropriate type of access system.

Organizations should provide easy mechanisms for online consumers to make inquiries. An interface that is easy-to-use, not requiring any special training by a non-technical person would satisfy this requirement. The idea being that the access should not be more difficult than accessing any of the online services provided by the organization. The right of access in the case of children's personal data is logically granted to the parents and not to the child. According to the U.S. *Children's Online Privacy Protection Act*,[46] at the parent's request, web site operators should disclose the type of general and specific personal information they have collected online from children visiting their web sites.[47]

PIPEDA provides that once an online user makes a request to access his/her personal data, the web site operator should respond to the user and provide him/her with his/her data within a reasonable time.[48] Access and as the case may be, systems used for correcting the data, should be available during reasonable hours. It is one thing for the organization to address the access request in a timely manner, but it should also correct or destroy personal information found to be incorrect, incomplete, irrelevant, or inappropriate, as quickly as is reasonably possible.[49] In case of disagreement on the amendment or deletion, the web site should come up with a resolution process.

### 9.3 Access System and Authentication

Organizations should ensure that they are providing access to the individual to whom the personal data collected relates. Providing access to the wrong person could breach the individual's privacy. The objective is to allow online users to access their personal data without running the risk that other users gain access. Organizations should therefore implement appropriate authentication and verification systems for security purposes.

An organization that allows access to personal data to the wrong person might be held liable. Furthermore, the effort to achieve strong authentication could affect anonymity on the Internet.

The fewest difficulties of authentification would arise when an online user establishes an account with a web site. In this case, the online user could be given access to information about his/her account if he/she simply provided the information required to establish and secure the account.

Organizations could request online users to provide sufficient information to enable them to provide an account of the existence, use, and disclosure of personal information.[50] It is common practice both offline and online to request some additional piece of information that is harder to provide and more difficult to compromise. For instance, several organizations require online users to use a shared secret (password) to access an account.

It would be appropriate and secure to provide access to the data when the requester appears to be the account holder and has the password. Although it would enhance the authentication process to request additional verifiable information about recent account activity, the issue is that these users may not remember what was the most recent activity on the web site.

Finally, in the event that organizations collect certain additional data from the online user to authenticate the access requester, they should only use this information for the access purpose.[51] They cannot collect such information for any other purpose (such as marketing to this user).

The type of authentication system could vary depending on what kind of data is collected.

#### 9.3.1 Data collected through online tracking tools

Providing access to certain types of partially personalized data, such as clickstream, log data, or any data collected through cookies or other identifiers could create substantial authentication problems.

In order to authenticate the identity of the access requester, certain web sites require that the identifier (the number associated with the organization cookie) be provided in an access request. This method enables the organization to easily provide access to the online user requester to the data linked to that specific cookie. The privacy issue with this type of access is that the data collected through these devices does not necessarily belong to one single individual. The data collected relates to a computer that may or may not be used only by one person. Perhaps the computer is shared by co-workers, family members, etc. Whether the online users should be entitled to have access to this type of data is not clear.

Access could be provided to an online user requesting it using the number associated with the organizations cookie, if the web site is one of general interest and therefore the disclosure of data collected by a cookie would not be revealing anything private about the other computer's user(s).

Some argue that data collected from automatic tracking methods constitutes personal information only if linked to an identifiable individual. The NAI Principles states that network advertisers should provide consumers with reasonable access to PI *and other information that is associated with PI* retained by the network advertiser for profiling uses.[52] The term *other information that is associated with PI* is not defined in these principles so it is not useful to determine if organizations should provide access to online users to clickstream and data that relates to a computer. It is interesting to note that access was an issue that concerned the states' lawyers in the DoubleClick settlement. In preparing its settlement DoubleClick stated that if it was going to employ targeting based on anonymous user profiles, it would use reasonable efforts to develop technology that allows a user to safely view any categories associated with that user's ad serving cookie.[53]

Certain members of the ACOAS believe that whether the data provided can be corrected should be taken into consideration in determining whether access should be provided to certain types of data. They suggest that the case for access grows weaker as the likelihood of improving the accuracy of personal data declines and the cost of providing secure access increases:

> Rather than pay those costs and take those risks for a large body of mostly insignificant data, we should concentrate on providing access to data that is important and correctable.[54]

Their reasoning is based on the premise that there is no compelling reason to provide access to uncorrectable data and suspect that the real goal may be to raise the cost of maintaining personal data in order to reduce the data collected by web sites. This argument might be raised in order to deny access to this type of data.

#### 9.3.2 Authentication for parents

In the context of children's web sites, the U.S. legal framework suggest that web site operators should use reasonable efforts to ensure they are dealing with the parent before they provide access to the child's specific information.[55] There are several authentication methods available for web site operators. The FTC suggests that web site operators could: (i) obtain a signed form from the parent via postal mail or facsimile; (ii) accept and verify a credit card number; (iii) take calls from parents on a toll-free telephone number staffed by trained personnel; (iv) email accompanied by digital signature; or (v) email accompanied by a PIN or password obtained through one of the verification methods above.[56] Organizations operating web sites who follow one of these procedures acting in good faith to a request for parental access are protected from liability under U.S. federal and state law for inadvertent disclosures of a child's information to someone who purports to be a parent.[57]

## 10. Challenging Compliance

PIPEDA states that organizations should provide easily accessible and simple to use procedures to address a challenge concerning compliance with the PIPEDA principles and receive and respond to privacy complaints or inquiries. Organizations should investigate all complaints. If justified, they should take appropriate measures, such as amending their policies and practices.

Online privacy issues have led to the proliferation of privacy seals that are programs to highlight privacy protection. These seals are displayed by web sites to indicate that they have met standards of trustworthiness. The purpose is to increase consumer confidence in e-commerce. To earn a privacy seal, an organization needs to have a privacy policy, make it easily accessible online, provide its visitors or customers with a way to opt out of direct marketing and selling their information to third parties, as well as provide a way to access their information and file complaints. The major players that offer privacy seals include TRUSTe, BBBonline and CPA Webtrust:

Seals have been criticized for many reasons. Web sites with the same privacy seal may have widely different privacy policies and a privacy seal does not mean that the web site will refrain from sharing personal information with another company. However, seals can confirm/corroborate that the privacy policy of a given web site truly represents what the privacy practices of the organization are. This means that an organization could earn a privacy seal even if it shares personal and sensitive data as long as the privacy policy discloses it. Online users still have to read the privacy policy and a privacy seal is not a substitute for doing so. Some have also questioned the true independent nature of TRUSTe and BBBOnline given their affiliation with the private sector. Still, privacy seals are generally viewed by online users as a symbol of trust and therefore should be viewed as valuable privacy tools.

## CONCLUSION

1 Article 2 (1), Personal Information Protection and Electronic Documents Act, c. 5 (2000).

2 Personal information is defined as “information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization”. See Article 2 (1), Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada).

3 Schedule 1, Section 5, Article 4.7.4, Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada).

4 Schedule 1, Section 5, Article 4.1.3; Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada); and Principle 4.7, Canadian Code of Practice for Consumer Protection in Electronic Commerce (The), Working Group on Electronic Commerce and Consumer, Approved in Principle, January 2003.

5 Center for Democracy & Technology, Why Am I Getting All This Spam?, Unsolicited Commercial E-mail Research Six Month Report, March 2003.

6 Federal Trade Commission, Bureau of Consumer Protection, E-mail Harvesting: How Spammers Reap What You Show, FTC Consumer Alert. http://www.ftc.gov/bcp/conline/pubs/alerts/spamalrt.pdf (Last accessed on June 23, 2003)

7 Schedule 1, Section 5, Article 4.2.4, Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada).

8 CAN-SPAM Act of 2003, S. 877, 108th Congress, 1st Session (2003).

9 Principle 1.3 h), Canadian Code of Practice for Consumer Protection in Electronic Commerce (The), Working Group on Electronic Commerce and Consumer, Approved in Principle, January 2003.

10 Schedule 1, Section 5, Article 4.2.4, Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada).

11 Principles 1.1 and 1.2, Canadian Marketing Association, Code of Ethics & Standards of Practice. http://www.the-cma.org/consumer/ethics_2.cfm (Last accessed June 5, 2003)

12 Schedule 1, Section 5, Article 4.2.4, Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada).

13 Schedule 1, Section 5, Article 4.3, Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada).

14 Microsoft, Spiking the Spammers, February 12, 2003. http://www.microsoft.com/issues/essays/2003/02-12spam.asp (Last accessed on June 5, 2003)

15 Microsoft, Spiking the Spammers, February 12, 2003. www.microsoft.com/issues/essays/2003/02-12spam.asp (Last accessed on June 5, 2003)

16 Principle 4.5, Canadian Code of Practice for Consumer Protection in Electronic Commerce (The), Working Group on Electronic Commerce and Consumer, Approved in Principle, January 2003.

17 Schedule 1, Section 5, Article 4.3.6, Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada).

18 Sec. 312.5 (a) (2), The Children’s Online Privacy Protection Rule, 16 C.F.R. Part 312, November 3, 1999; Principle 8.3, Canadian Code of Practice for Consumer Protection in Electronic Commerce (The), Working Group on Electronic Commerce and Consumer, Approved in Principle, January 2003; and Article 15, Direct Marketing Association, Guidelines for Ethical Business Practice, April 2002. http://www.the-dma.org/guidelines/ethicalguidelines.shtml (Last accessed on June 5, 2003)

19 Canadian Marketing Association, Code of Ethics & Standards of Practice. http://www.the-cma.org/consumer/ethics_2.cfm (Last accessed June 5, 2003)

20 The Canadian Code of Practice for Consumer Protection in Electronic Commerce, Working Group on Electronic Commerce and Consumer, Approved in Principle, January 2003.

21 Sec. 312.5 (a) (2) (b), The Children’s Online Privacy Protection Rule, 16 C.F.R. Part 312, November 3, 1999.

22 Sec. 312.5 (b) (2), The Children’s Online Privacy Protection Rule, 16 C.F.R. Part 312, November 3, 1999.

23 Sec. 312.5 (c) (1), The Children’s Online Privacy Protection Rule, 16 C.F.R. Part 312, November 3, 1999; and Article 15, Direct Marketing Association, Guidelines for Ethical Business Practice, April 2002. http://www.the-dma.org/guidelines/ethicalguidelines.shtml (Last accessed on June 5, 2003)

24 Sec. 312.5 (c) (2),The Children’s Online Privacy Protection Rule, 16 C.F.R. Part 312, November 3, 1999.

25 Sec. 312.5 (c) (3), The Children’s Online Privacy Protection Rule, 16 C.F.R. Part 312, November 3, 1999; and Article 15, Direct Marketing Association, Guidelines for Ethical Business Practice, April 2002. http://www.the-dma.org/guidelines/ethicalguidelines.shtml (Last accessed on June 5, 2003)

26 Principle 8.5, Canadian Code of Practice for Consumer Protection in Electronic Commerce (The), Working Group on Electronic Commerce and Consumer, Approved in Principle, January 2003.

27 Schedule 1, Section 5, Article 4.2.4, Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada).

28 In the Matter of DoubleClick Inc., Agreement between The Attorneys General of the States of Arizona, California, Connecticut, Massachusetts, Michigan, New Jersey, New Mexico, New York, Vermont, and Washington and DoubleClick Inc., August 26, 2002.

29 Rachel Ross, One way to stymie e-spys: leave a "decoy" data trail, The Toronto Star (Canada), May 12, 2003.

30 Schedule 1, Section 5, Article 4.7.2, Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada).

31 Principle 5.2, Canadian Code of Practice for Consumer Protection in Electronic Commerce (The), Working Group on Electronic Commerce and Consumer, Approved in Principle, January 2003.

32 Industry Canada (The Working Group on Consumers and Electronic Commerce), E-mail marketing: Consumer choices and business opportunities, Discussion Paper, January, 2003.

33 Rogers Cable is a wholly owned subsidiary of Rogers Communications Inc. (Toronto: RCI.A and RCI.B; NYSE: RG) and is Canada's largest cable operator. http://www.rogers.com/ (Last accessed on June 5, 2003)

34 Kanitz v. Rogers Cable Inc., February 22, 2002 (Docket 01-CV-214404CP), Ontario Superior Court.

35 Comb v. PayPal Inc., N.D. Cal., No. C-02-1227 JF (PVT)

36 Schedule 1, Section 5, Article 4.9, Personal Information Protection and Electronic Documents Act, c. 5 (2000);

37 Schedule 1, Section 5, Article 4.9, Personal Information Protection and Electronic Documents Act, c. 5 (2000);

38 Schedule 1, Section 5, Article 4.9.4, Personal Information Protection and Electronic Documents Act, c. 5 (2000).

39 Hoofnagle, Chris Jay, Deputy Counsel, Electronic Privacy Information Center, Access Enhances Openness and Accountability, (section of the Center for Democracy & Technology, Considering Consumer Privacy Report), March 2003.

40 Hadley, Vice President, Government Affairs, Experian, Consumer Access to Marketing Data: Let's Look Before we Leap, (section of the Center for Democracy & Technology, Considering Consumer Privacy Report), March 2003.

41 Online Privacy Alliance (OPA), Online Consumer Privacy in the U.S. Submitted with the Comments of the Online Privacy Alliance, On the Draft International Safe Harbor Principles, legal framework White Paper, November 19, 1998. http://www.privacyalliance.org/news/12031998-5.shtml (Last accessed on June 5, 2003)

42 Federal Trade Commission, FTC Advisory Committee on Online Access and Security, Final Report, May 3, 2000. http://www.ftc.gov/acoas/papers/acoasdraft1.htm (Last Accessed on June 5, 2003)

43 The ACOAS Committee in its report on access, defined inferred data as information gathered from sample data, not the data subject, that is calculated to result in a value applied to the data subject. The term derived data was defined as information gathered from the subject that is calculated to result in a value applied to the data subject. See Federal Trade Commission, FTC Advisory Committee on Online Access and Security, Final Report, May 3, 2000, p. 8. http://www.ftc.gov/acoas/papers/acoasdraft1.htm (Last Accessed on June 5, 2003)

44 Schedule 1, Section 5, Article 4.9.1, Personal Information Protection and Electronic Documents Act, c. 5 (2000).

45 Schedule 1, Section 5, Article 4.9.1, Personal Information Protection and Electronic Documents Act, c. 5 (2000).

46 The Children's Online Privacy Protection Rule, 16 C.F.R. Part 312, November 3, 1999.

47 Sec. 312.6 (a) (1), The Children's Online Privacy Protection Rule, 16 C.F.R. Part 312, November 3, 1999.

48 Schedule 1, Section 5, Article 4.9.4, Personal Information Protection and Electronic Documents Act, c. 5 (2000).

49 Ann Cavoukian, Best Practices for Online Privacy Protection, Information and Privacy Commissioner (Ontario), June 2001.

50 Schedule 1, Section 5, Article 4.9.2, Personal Information Protection and Electronic Documents Act, c. 5 (2000).

51 Schedule 1, Section 5, Article 4.9.2, Personal Information Protection and Electronic Documents Act, c. 5 (2000).

52 Section IV, C, (1) (f), Network Advertising Initiative, Self-Regulatory Principles for Online Preference Marketing by Network Advertisers. http://www.networkadvertising.org/aboutnai_principles.asp(Last accessed on June 5, 2003)

53 In the Matter of DoubleClick Inc., Agreement between The Attorneys General of the States of Arizona, California, Connecticut, Massachusetts, Michigan, New Jersey, New Mexico, New York, Vermont, and Washington and DoubleClick Inc., August 26, 2002.

54 Federal Trade Commission, FTC Advisory Committee on Online Access and Security, Final Report, May 3, 2000, p. 20. http://www.ftc.gov/acoas/papers/acoasdraft1.htm (Last Accessed on June 5, 2003)

55 Sec. 312.6 (3) (i), The Children's Online Privacy Protection Rule, 16 C.F.R. Part 312, November 3, 1999.

56 Federal Trade Commission, How to Comply With The Children's Online Privacy Protection Rule, Guide. http://www.ftc.gov/bcp/conline/pubs/buspubs/coppa.htm (Last Accessed on June 5, 2003)

57 Sec. 312.6 (b), The Children's Online Privacy Protection Rule, 16 C.F.R. Part 312, November 3, 1999.