A Strategic Approach to Successful Compliance Under the Personal Information Protection and Electronic Documents Act – Focus on Enforcement and Remedies

Further to the substantive analysis of the policies and principles imbedded in the federal Personal Information Protection and Electronic Documents Act , S.C. 2000, c.5, as amended, (hereinafter referred to as 'PIPEDA'), the purpose of this follow-up paper is to examine the rather comprehensive remedial sections of the legislation. Extensive powers are given to investigate complaints, to audit the personal information management practices of organizations, to apply to Federal Court for hearings concerning complaints and to award damages, including damages for humiliation. Many organizations, large, medium and small, may very well be surprised, not only by their need to be ready for this law by January 1, 2004 (a scant month and a few days from time of writing), but also by the breadth and scope of the powers of enforcement of the Act.

Although the focus of this paper is remedies and enforcement, note that while compliance sections of the legislation are a legitimate motivator, the management professional will recognize the value of proactivity. It simply makes good business and management sense, in either the for-profit or not-for-profit sectors, to have systems in place and ready to comply with the law. Clients place a higher value on organizations that do not scramble to react to laws designed to protect their legitimate interests. Clients value those organizations that anticipate potential problems and are ready for them. They value businesses and support charities that place an emphasis on their privacy concerns. In sum, the coming into force of this Act presents a strategic opportunity to build trust and brand loyalty with your clientele. If the PIPEDA impacts your organization immediately, the remedial powers of the Commissioner are simply too serious to ignore.

Constituent Divisions - Content

Often the best way to understand a piece of legislation is to break it down into its constituent parts. With respect to PIPEDA, Division 1, "Protection of Personal Information", deals with the collection, use and disclosure of personal information. Previous papers of mine dealt with the essential elements of Division 1, which itself references Schedule I of the Act which is based upon the Canadian Standards Association's Ten Principles of Privacy Protection. Division 2, "Remedies", concerns the filing of complaints, the investigation powers of the Office of the Privacy Commissioner (hereinafter referred to as 'OPC' or 'the Commissioner'), dispute resolution mechanisms, the Commissioner's reporting function, the possibility of applying to Federal Court – Trial Division for a hearing and the remedies that the Court may give. Division 3, "Audits", deals with the power of the Commissioner to audit the personal information management practices of an organization if the Commissioner has reasonable grounds to believe the organization is violating a provision of Division 1. Division 4, "General", while dealing with a number of concepts, is relevant to this paper as it contains a 'whistle-blowing' section, as well as an offence and punishment section.

While the remedial parts of the legislation itself may make for dry reading, its potential impact upon your organization, as described in this paper, will keep your attention. I promise.

Non-Compliance: The Powers of the Office of the Privacy Commissioner
The Privacy Commissioner has five methods to ensure that organizations subject to the PIPEDA comply with it, as follows:

(i) investigating complaints;
(ii) conciliating and mediating complaints;
(iii) auditing personal information practices;
(iv) reporting abuses through its public fora; and/or
(v) seeking remedies in Court.

Note that one or more of these actions can be taken concurrently, demonstrating that the Commissioner has many arrows in his or her quiver to enforce compliance.

Investigations
The investigation process can begin in more than one way. Either an individual or the Commissioner may initiate a complaint about the activities of an organization. (s. 11) Complaints will focus on whether an organization contravened a provision of s.1 of the PIPEDA.

The breadth of the powers of the Commissioner for the purpose of investigating a complaint is most extensive, indeed, similar to a Superior Court of Record. For the purposes of an investigation, the Commissioner may:

(a) summon and enforce the appearance of persons before it;
(b) compel them to give oral and written evidence under oath;
(c) compel them to produce records and things (in the same manner of a Superior Court of Record);
(d) administer oaths;
(e) at any reasonable time, enter the organization's premises (other than a home);
(f) converse with persons on these premises;
(g) examine and obtain copies of records found on the entered premises.

Obviously, these powers, including even entering premises and copying files, are most intrusive. Many readers may likely be put in the mind of police or CCRA powers, when they read this s. 12 of the PIPEDA.

Files or other items, records or things may actually be taken, though they are to be returned with ten days. Of course, they may be taken again for another ten-day time period. Again, these are intrusive actions, to be sure.

Somewhat less intrusive is the power to mediate or conciliate between the parties, a power found in subsection.12(2). The OPC and all parties involved will appreciate this power, as it is almost always a beneficial (and less costly in terms of time and money) option to a more litigious approach to resolving disputes.

Commissioner's Report

There is an obligation put upon the OPC to produce a report, subsequent to the filing of a complaint. This Commissioner's Report must be produced within one year of the complaint being filed or initiated by the OPC, subject to certain few exceptions. (s. 13)

Complaints will centre on the improper collection, use or disclosure of personal information, failure to use appropriate safeguards to protect personal information, failure to provide an individual access to his/her personal information and the other items found in Schedule 1 to the PIPEDA, based upon the Canadian Standards Association principles delineated in the Appendix to this Paper and other papers I have written.

The Report will contain the Commissioner's findings and recommendations, any settlement that was reached between the parties, and the recourse, if any, that is available by application to a Court. Additionally, the Report will contain a request that the organization in question give the OPC notice of any action taken to implement the recommendations found in the Report, or a reason why no such action has been taken. Reports are sent to all parties involved expeditiously.

As to the limited exceptions where no Report is required to be tabled by the OPC, no report need be filed where the Commissioner is satisfied that:

(a) the complainant ought to first exhaust grievance or review procedures available;
(b) the complaint would best be remedied under the laws of Canada (or a Province);
(c) too long a delay has occurred between the time of the triggering event complained of and the date of the actual complaint;
(d) the complaint is "trivial, frivolous or vexatious or is made in bad faith". (s.13(2))

Court Hearings

In addition to the administrative law and the use of the OPC as a federal regulatory tribunal with certain powers of a Superior Court, access to the actual Courts is also contemplated. Either of the Complainant or the Commissioner may apply to the Federal Court-Trial Division, for a hearing in respect of which a complaint was filed.

Section 14 allows the complainant, after receiving the Commissioner's Report, to apply to the Federal Court for a hearing in respect of which a complaint was made, or that is referred to in the Report. It matters not whether the original complaint was initiated by an individual or by the Commissioner.

Matters subject of an application may include whether:

(a) an organization has properly exercised its responsibility for the personal information in its possession;
(b) an organization has properly identified and documented the purposes for which personal information is being collected, used or disclosed, at or before time of collection;

(c) an organization has refused to provide a service, because one refused to provide consent for the collection, use or disclosure of more information than is necessary for the specified purpose;
(d) an organization has collected more information than necessary or whether it was collected by fair and lawful means;
(e) information is accurate, up-to-date and complete;
(f) an organization has taken the necessary steps to safeguard the information;
(g) an organization has made specific information about its personal information management practices readily available;
(h) an organization has used or disclosed personal information for purposes other than those for which it was collected without the consent of the individual and in circumstances not contemplated by the PIPEDA;
(i) an individual was wrongly denied access to information about himself or herself;
(j) the information was collected, used or disclosed only for purposes that a reasonable person would consider appropriate;
(k) an organization has failed to grant access in an alternative fashion to a person with a sensory disability;
(l) an individual has been charged too much for access to information or was not notified in advance of the cost.

Other matters may be the subjects of an application, but it is manifest that the ever-important CSA principles are being protected. For those interested in more information, see the guide published by the OPC, found at www.privcom.gc.ca.

Section 15 permits the Commissioner, in respect of a complaint that he/she did not initiate,

(a) to apply to the Court for a hearing in respect of any matter, with the consent of the Complainant;
(b) appear before the Court on behalf of any complainant who has applied for a hearing; or
(c) with the leave of the Court, appear as a party to any hearing begun under s.14.

Remedies of the Court

The array of remedies the Federal Court possesses is broad. Some are laid out in s. 16, including :

(a) to order an organization to correct its practices;
(b) to order an organization to *publish a notice* of any action taken or proposed to be taken to correct its practices;
(c) award damages to the Complainant, *including damages for humiliation* that the Complainant has suffered.

So, it is evident that organizations that do not comply with the PIPEDA, are potentially in for a very public and expensive process. Even if damages are not high, in and of themselves, the fact that a company or other type of organization that has significant compliance problems, could suffer secondary business or reputational damage, is worth the attention of managers and boards of directors.

After all, who wants to do business with an organization that does not protect one's privacy? In a non-profit context, who wants to donate money to an organization, if they are not assured that their personal information is safeguarded? The public nature of the remedy may very well be the most stringent enforcement mechanism of all.

The Dreaded "A" Word

The word, "audit" strikes fear in the hearts of many. The Privacy Commissioner has audit powers, which are found in Division 3 of the PIPEDA, in sections 18 and 19. For the purposes of the legislation, the OPC has been given audit powers to ensure compliance.

The Commissioner may, on reasonable notice and at any reasonable time, audit the personal information management practices of an organization, "if the Commissioner has reasonable grounds to believe that the organization is contravening", any provision of Division 1 or the CSA's Ten Principles, found in Schedule 1 of the PIPEDA.

Following an audit, a process which gives the Commissioner or his/her delegate the broad powers given under the Investigation sections of the Act, the OPC shall provide to the audited organization a report that contains the findings of the audit and any recommendations the Commissioner deems appropriate. Also, subsection 20(2) allows the Commissioner to make public any information relating to the personal information management practices of an organization, if the Commissioner, "considers that it is in the public interest to do so".

Additionally, these Audit Reports may be included in the OPC's Annual Report to Parliament, and so, will have the potential to be public again and potentially most embarrassing to the non-compliant firm.

Protection for "Whistle-Blowers"

Another interesting provision in the PIPEDA, one designed to promote enforcement of the Act, is found in sections 27 and 27.1. Anyone who believes that a provision of the Act has been violated or is about to be violated, may notify the Commissioner of the details of the matter and request that their identity be kept confidential.

Also, "no employer (or organization utilizing the services of an independent contractor) shall dismiss, suspend, demote, discipline, harass or otherwise disadvantage an employee (or, independent contractor) or deny the employee a benefit of employment", by reason that the employee, acting in good faith and on the basis of reasonable belief has disclosed a contravention or intention to contravene the PIPEDA, or has refused an order to contravene the Act. (Section 27.1)

Again, it can be seen that having strict privacy codes in place, actively and adequately protecting personal information and educating management and staff of your organization about the new laws, will do away with the need for employees to feel stuck between complying with the law and doing their jobs.

Having a good plan in place, having regular education updates, having sound privacy policies, practices and systems from the outset of its impact on your organization, will vitiate, or at least mitigate concern about penalties and enforcement.

Offences and Punishment Provision – Section 28

Section 28 of PIPEDA sets out that anyone who destroys personal information that an individual has requested (done either through negligence or through an intent to avoid the OPC discovering that said information was being held or used inappropriately), who retaliates against an employee contrary to the goals of the "whistle-blowing sections, or who obstructs an audit or investigation, is guilty of,

(a) a summary conviction offence and liable to a maximum fine of $10,000; or
(b) an indictable offence and liable to a maximum fine of $100,000.

Depending upon the seriousness of the breach, the penalties can increase from mere compliance orders, to severe financial penalties, to public humiliation and possible damage to the marketability of one's business and one's very own reputation.

Conclusions

In summary, it is evident that the Personal Information Protection and Electronic Documents Act has teeth. It is most definitely NOT a law to be ignored, even if your organization is not immediately impacted by it. Fines are potentially substantial, audit and investigatory powers of the Privacy Commissioner are extensive and intrusive and include the power to delve deeply into your organizations' personal information management practices. Possibly, most effective of all, is the power to make public, information about an organization's personal information management practices, so to protect the public interest. The risk of embarrassing your organization's board or management is real.

From a positive strategic perspective, though, developing good privacy practice and procedures will enhance an organization's standing. It will build client loyalty. Competence is attractive. In the non-profit context, donors give to competent entities that can make a positive difference in people's lives. Competitive advantage, no matter the market, will accrue to the organization that has good privacy policies in place. Particularly in a culture that so highly values privacy, a PIPEDA-compliant firm, well prepared for the law, will build trust in all of its constituencies. Non-profits and charities exist, in large part, upon the trust that the public places in them. Having privacy-compliant systems in place, even before they have to be there, is just another practice to demonstrate that trust in your organization is earned and well-deserved.

Jeffrey H. McCully, Barrister & Solicitor, is also Chair of the CAGP's National Capital Roundtable. He can be reached at jmccully@scotmor.ca.