

Submission to a House of Commons Standing Committee
on Access to Information, Privacy and Ethics (ETHI)

**Statutory review of the Personal Information Protection
and Electronic Document Act (PIPEDA)**

November 22nd 2006

Dr. Colin J. Bennett
Chair
Political Science Department
University of Victoria
PO Box 3050 STN CSC
Victoria BC V8W 2Y2
CANADA
(250) 721-7495
cjb@uvic.ca
<http://web.uvic.ca/poli/bennett>

signature

I. INTRODUCTION

My name is Colin Bennett, currently Professor and Chair of the Political Science Department at the University of Victoria. For over 20 years, I have been researching the issue of personal privacy protection in Western societies: the spread of surveillance; the nature and extent of public concern; and the content and effectiveness of privacy protection laws and other approaches.

I am the author of *Regulating Privacy: Data Protection and Public Policy in Europe and the United States (1992)*,¹ the co-editor of *Visions of Privacy: Policy Choices for the Digital Age (1999)*,² and more recently co-author of *The Governance of Privacy: Policy Instruments in Global Perspective*.³ I have also written many academic articles on these subjects, and occasionally offered journalistic commentary. I am the author of several reports on privacy protection within Canada (to the Canadian Standards Association,⁴ and to Industry Canada⁵). I have also written reports on international privacy protection issues – to the Standards Council of Canada on the need for an international standard for the protection of personal information,⁶ and to the European Commission, on the implementation of the “adequacy” provisions within the EU's 1995 Data Protection Directive.⁷ I have also been a complainant under PIPEDA.

I wish first to review the essential aims of information privacy law, and then provide a brief sketch of the worldwide development of these laws in order to demonstrate that PIPEDA is one of a family of statutes, and that Canada was relatively late in legislating a set of privacy standards for its private sector. I will then review the development of privacy protection law in Canada and discuss the powers of the Commissioner in comparative perspective, with reference to a personal experience as a complainant. In conclusion I make a number of recommendations for reform.⁸

THE AIMS OF INFORMATION PRIVACY LAW

We can distinguish between three overlapping motivations for the assertion of privacy claims: *humanistic, political and instrumental*.⁹

Firstly, privacy claims are made for fundamentally humanistic reasons to protect the dignity, individuality, integrity or private personality of each and every one of us, regardless of wider implications or consequences. The basic issue is the loss of human dignity, respect and autonomy that results when one loses control over the circumstances under which one's space, behavior, decisions or personal information is intruded upon. These conceptions are at the heart of the privacy movement in virtually every democratic state.

A second dimension, however, is explicitly political. Privacy plays an important role within liberal democratic theory, and is a prerequisite for liberal democratic societies: it prevents the total politicizing of life; it promotes the freedom of association; it shields scholarship and science from unnecessary interference by government; it permits the use of a secret ballot and protects the voting process by forbidding government surveillance of a citizen's past voting record; it restrains improper police conduct such as physical brutality, compulsory self-incrimination and unreasonable searches and

seizures; and it serves also to shield those institutions, such as the press, that operate to keep government accountable.¹⁰

A third, a somewhat different, purpose is an instrumental or strategic one. The promotion of privacy may also serve to ensure that, “the right people use the right data for the right purposes.”¹¹ When anyone of those conditions is absent, critical rights, interests and services might be jeopardized. This is an explicit concern about information, but it expresses a fundamental assumption that if you can protect the information on which decisions are made about individuals, you can also protect the fairness, integrity and effectiveness of that decision-making process and increase trust in institutions and technologies. (This goal is apparent in the stated purpose of PIPEDA to promote electronic commerce).

Whether justified in philosophical, political or utilitarian terms, privacy is almost always seen as a claim, right of interest of individuals that is threatened by a pervasive set of social and technological forces.

Despite the association of privacy issues with technology in recent decades, privacy concerns go back centuries. And specific problems about how certain types of personal information in certain contexts, particularly medical contexts, have been the subject of claim and counterclaim, and regulatory and judicial decision-making for a very long time.

Privacy protection as a *public policy question*, however, is of more recent vintage. The issue came to the agenda of advanced industrial states in the late 1960s because of two main characteristics of post-industrialism – bureaucratization and information technology. When those forces reached a critical point in the 1960s and 1970s with the expansion of the state and the computerization of state functions, many Western societies attempted to develop a coordinated public policy approach.

That coordination was provided by the doctrine of *fair information principles*, the historical origins of which can be briefly traced to policy analysis in Europe and the United States in the late 1960s and early 1970s.¹² Those experts who were attempting to resolve this issue in national arenas shared a strong desire to draw lessons from their counterparts overseas. This intense process of lesson-drawing produced an international consensus on how best to resolve the privacy problem through public policy.

While the codification of the principles may vary, they essentially boil down to the following tenets.¹³ An organization (public or private):

- must be *accountable* for all the personal information in its possession
- should *identify the purposes* for which the information is processed at or before the time of collection
- should only collect personal information with the *knowledge and consent* of the individual (except under specified circumstances)
- should *limit the collection* of personal information to that which is necessary for pursuing the identified purposes
- should not use or disclose personal information for purposes other than those identified, except with the consent of the individual (*the finality principle*)
- should *retain* information only as long as necessary
- should ensure that personal information is kept *accurate, complete and up-to-date*

- should protect personal information with appropriate *security safeguards*
- should be *open* about its policies and practices and maintain no secret information system
- should allow data subjects *access* to their personal information, with an ability to amend it is inaccurate, incomplete or obsolete.

These principles are, however, relative. However conceptualized, privacy is not an absolute right; it must be balanced against correlative rights and obligations to the community. Privacy protection, therefore, is the “process of finding appropriate balances between privacy and multiple competing interests.”¹⁴

The fair information principles appear either explicitly or implicitly within all national data protection laws' (Privacy' Acts), including those in the USA, Australia, New Zealand and Canada . They appear in self-regulatory codes and standards, such as that published by the Canadian Standards Association, which forms the basis of PIPEDA, and most especially they appear in international agreements.

The increasing ease with which personal data might be transmitted outside the borders of the country of origin has produced an interesting history of international harmonization efforts, and a concomitant effort to regulate transborder data flows. In the 1980s, these harmonization efforts were reflected in two international agreements: the 1981 *Guidelines from the Organization for Economic Cooperation and Development*;¹⁵ and the 1981 *Convention* from the Council of Europe.¹⁶ In the 1990s, they were extended through the 1995 *Directive on Data Protection* from the European Union which attempts to harmonize European data protection law according to a higher standard of protection, and to impose that standard on any country within which personal data on European citizens might be processed.¹⁷

II. THE DEVELOPMENT OF CANADIAN PRIVACY LAW

The forces that brought the privacy issue to the agenda in Canada were generally the same as those in other countries: the computerization of personal information systems (especially in the public sector), the development of a universal identifier (the Social Insurance Number) and a growing sense of alienation from the agencies of government. In the 1970s, there followed a quiet but wide-ranging debate about the privacy issue.¹⁸

The first privacy legislation at the federal level was actually contained in Part IV of the 1977 Canadian *Human Rights Act*, which established the office of the Privacy Commissioner. Parallel debates over a federal access to information act in the early 1980s raised immediate questions about the compatibility between such legislation and the privacy standards within Part IV. The current 1982 *Privacy Act*, therefore, flows from a belief that data protection should be a corollary to freedom of information, and that the various exemptions in both pieces of legislation should be internally consistent. PIPEDA, incorporating an *Access to Information Act* and a revised *Privacy Act*, thus institutionalized the Canadian innovation of legislating access to information and privacy protection within the same statutory framework. This model was later copied by the provinces and territories.

With respect to the private sector, however, there existed only a few isolated statutes relating to specific sectors, such as consumer credit industry, and a sprinkling of

common law remedies and constitutional provisions of potential relevance. Privacy protection in the private sector was largely dependent on the implementation of a set of voluntary and sectoral codes of practice developed according to the framework of the 1981 *OECD Guidelines*.¹⁹ The passage in 1993 of Quebec's *An Act Respecting the protection of personal information in the private sector*, gave effect to the information privacy rights incorporated in the new Civil Code, and made Quebec the first jurisdiction in North America to produce comprehensive data protection rules for the private sector.

Throughout the 1990s, a number of political, international, technological and legislative developments convinced federal policy makers that this incoherent policy could not be allowed to continue. First, the passage of a *Data Protection Directive* from the European Union meant that no jurisdiction in Canada (save Quebec) could plausibly claim an “adequate level of protection” and therefore safely process personal data transmitted from EU countries. Second, the passage of the Quebec legislation created an “unlevel playing field” within the Canadian federation, creating uncertainties and transaction costs for businesses that operate in different provinces. Third, the publication of a series of public opinion surveys demonstrated that the general public regards privacy protection as a matter of major concern.²⁰ Fourth, the commercialization of some governmental functions had undermined the implementation of public sector data protection law and the ability of Canada’s privacy commissioners to ensure the protection of personal data when it is transferred to a private contractor. Finally, the debates over the development and character of the Canadian “information highway” exposed the need for a common set of “rules of the road” for the networked and distributed computing and communications environment of the 21st century.²¹

The result was the *Protection of Personal Information and Electronic Documents Act* (PIPEDA) which came into force on January 1, 2001.²² While this law filled in some very important gaps in the existing patchwork of federal and provincial statutes, it did not, and could not, regulate the entire Canadian private sector. On January 1, 2001 only the following businesses were forced to comply: banks, telecommunications, broadcasting, airlines, and transportation companies, as well as any company that transfers personal information across provincial or international borders for commercial reasons. After 3 years, the law applied to all commercial activities by the private sector, including companies under provincial or territorial jurisdiction, unless they are covered by “substantially similar” provincial or territorial law. The federal government declared the 1993 private sector legislation in Quebec as meeting this standard. Both BC and Alberta since passed similar legislation. In other provinces, PIPEDA applies by default.

In conclusion, the relative lateness of Canadian efforts to regulate the private sector has meant that federal and provincial legislation has been forced to comply with already established international standards. Although our law has been shaped by some distinctively Canadian concerns and interests, the committee needs to be very aware of the inescapable international context within which PIPEDA was developed, and in which it now operates.

THE POWERS OF THE PRIVACY COMMISSIONER

Despite very similar statutory principles, information privacy law varies with regard to the policy instruments established for oversight and regulation. Most countries, including Canada (but with the notable exception of the United States), have set up small privacy

or data protection agencies with varying oversight, advisory or regulatory powers. Some of these agencies have strong enforcement and regulatory powers and a few act as more advisory “ombudsman-like” bodies. Some are headed by a collective commission (such as in France), others by a single “Privacy Commissioner” or “Data Protection Commissioner.” In some regulatory regimes, instruments of “self-regulation” (such as company codes of practice) play a more important role than in others.

Any regulatory privacy protection scheme therefore needs to ascertain the correct mix of the following seven functions and ensure that the mix is compatible with existing constitutional and administrative legal requirements:

- 1) The Receipt, Investigation and Resolution of Complaints
- 2) Audit Powers
- 3) Enforcement Powers
- 4) The Receipt, Verification and Approval of Privacy Codes
- 5) Advice on the Privacy Implications of New Technologies
- 6) Public Education and Research
- 7) Sanctions and Remedies

One of the effects of the 1995 European Data Protection Directive has been to extend the process of policy convergence beyond the level of basic statutory principles, by pushing for greater conformity in the ways in which these principles are enforced through a “supervisory authority.” The principle of independent oversight is also regarded as a test of the “adequacy” of data protection in non-European countries.

There has been much debate in Canada about whether the so-called “ombudsman” model (advisory, with no direct enforcement power) is appropriate for the regulation of business. At the time of promulgation, I was persuaded by the then Privacy Commissioner, and others, that there was no need to give the Commissioner order-making powers and that the model provided under the *Privacy Act* would suffice.

However, experience has shown that there are some serious problems with the implementation of PIPEDA, and that it is difficult to identify whether the cause is: 1) weaknesses in the drafting of the Act itself; 2) the Privacy Commissioner’s interpretation of various provisions of the law; 3) the lessened credibility and esteem of the office as a result of the highly publicized problems of Commissioner Radwanski; or 4) wider political pressures associated with the perceived need for heightened levels of surveillance in order to wage the “war on terror.” This committee should certainly consider carefully the larger and more difficult context within which privacy law has to be implemented in Canada today.

Nevertheless, I am persuaded that the Commissioner should be given the kinds of order-making powers enjoyed by her counterparts in BC, Alberta and Quebec, and in most other foreign jurisdictions. A model that emphasizes dispute resolution among parties is not suitable for the development and clarification of law. Indeed, I believe that the desire to obtain remedy or redress for an aggrieved party is not the major motivation behind most PIPEDA cases.

I have been a complainant under PIPEDA and I would like briefly to recount this story. In November 2001, I received a consumer product survey through the mail which I believed was not in compliance with PIPEDA. Back in 1997, there was a small controversy about the same survey, and so at that time the company was put on notice that what they were doing

was not privacy-friendly. When I received the same survey 4 years later, without any evidence that the company had changed its practices, I was irritated and I complained to the Office of the Privacy Commissioner. I objected to three things: 1) the fact that the survey was distributed as a “fact-finding survey” about consumption habits, with very little indication that the information collected was going to be used for direct-marketing; 2) the position and clarity of the opt-in/opt-out box (to receive marketing solicitations); and 3) the fact that there was no indication of how to contact the company if one had questions/complaints – no responsible person listed, no website, no 1-800 number etc. These are some quite precise but general issues of legal compliance that had little to do with my privacy rights. I was not interested in personal redress or remedy, but with getting this company to change its practices and thereby advance some clarity in the law. This was not a dispute between two parties but a matter of policy that required examination and ruling.

A year later, after considerable resistance by the company, Commissioner Radwanski issued his finding and agreed with my complaint in every respect and in one regard he went even further, suggesting that the company was being deceptive. I received the full finding, and it was summarized and published as Case no. 91 on the Privacy Commissioner’s website. However, the name of the company was not revealed, resulting in some discussion between myself and the Commissioner’s office. My main concern had always been that the company corrects its practices, and I made that fact known. Besides, I really do not think it should be up to the complainant to make the decision about whether and how to disclose that a company is not privacy compliant.

As many have remarked, one of the arguments behind the “Ombudsman” model for compliance is that the desire to avoid adverse publicity is a significant incentive for any company to comply with the law. If a company knows that it will not be named, and therefore will not be subject to public scrutiny, then it will have less incentive to obey the Commissioner’s recommendations. The potential strength of the Ombudsman model is not felt when a non-compliant organization is not named.

That is exactly what happened in this case. There was a long period of resistance, including correspondence from the company’s lawyers objecting to some of the Commissioner’s findings and basically telling him that they will sort out these issues in consultation with me and the Canadian Marketing Association. It was not for another two years, and prompted by the receipt of another complaint about the same organization, that the Commissioner’s office could assure me that changes were being made to this survey, supposedly consistent with Commissioner Radwanski’s report. Much of this subsequent negotiation was not public, *and yet this was not a private matter*. Hundreds, if not thousands of Canadian households were affected. And yet, I am absolutely sure that the public information arising from this case provides very little guidance to other companies and individuals about the proper parameters of the law.

The lesson I draw from this case is that complaints-resolution is a very tedious, lengthy and inefficient method by which to raise privacy standards. I had no intention of going to Federal Court for a *de novo* hearing over this matter, and I certainly did not have the resources. The company knew that. It could, therefore, stall. If the Commissioner had been able to issue a binding enforcement order in 2001, then the resolution would have been speedier and the law clearer, not only for individuals but also for organizations. I am now persuaded that the presence of ultimate enforcement powers creates the necessary incentives for compliance and the effective resolution of complaints. We

need some serious jurisprudence about private sector compliance in which the context and the nature of the dispute can be more fully understood through published orders.²³

No doubt, the addition of enforcement powers would be seen as a significant change in the operation and culture of the Office of the Privacy Commissioner of Canada. No doubt it would attract opposition from the business community. There will be arguments that the time is not right. But the arguments in favour are now overwhelming and, I think, supported by most outside experts. Giving the Privacy Commissioner order-making powers and confining recourse to the Federal court to appeal would: 1) give the Commissioner some “teeth” and facilitate mediation; 2) cut into the costs and delays under the current process; 3) force respondents to challenge unfavorable results in court; 4) foster a proper jurisprudence that would guide business and facilitate the development of clear guidance notices; and 5) bring the Federal regime into line with the dominant model in the provinces.²⁴

One model would be that contained in the Alberta and BC *Personal Information Protection Acts* (PIPA). These Commissioners have the power to conduct written or oral inquiries if mediation does not occur, or is unsuccessful. Under the Alberta legislation, these should take place within 90 days and must dispose of the issue by making an order.²⁵ Either party then has 45 days to request judicial review. Neither law contemplates inquiries as anything other than a last resort. The early experience is that the existence of this power provides a very powerful motivation for mediation and compliance.

A second model has been proposed by the Canadian Bar Association and involves the establishment of a Tribunal, similar to that adopted by the Canadian Human Rights Commission. This has the advantage of maintaining the current powers of the Privacy Commissioner as an investigator and advocate, and elevates the more judicial role to a specialist tribunal. “Well-founded” complaints would be referred to the Tribunal for final disposition. This model, it is argued, allows for a speedier and less costly review than would occur in the Federal Courts. This model exists under the UK Data Protection Act, where a Data Protection Tribunal is empowered to review the decisions of the Information Commissioner.

This Committee should certainly examine this option, but I am not persuaded that it is necessary. I understand that the Canadian Human Rights Tribunal still experiences significant delays, and that a good number of their decisions are appealed to the Federal Court in any case. I do not support a Tribunal if it is just another layer of adjudication on the way to the Federal court.²⁶

It should also be noted that the introduction of enforcement powers would settle the debate about the “naming of names”, as has been the practice under the implementation of Alberta’s PIPA. At the moment, Section 20(1) of PIPEDA, obliging confidentiality, is interpreted by the Privacy Commissioner as overriding Section 20(2), which allows for the Commissioner to make public “any information relating to the personal management practices of an organization if the Commissioner considers that it is in the public interest to do so.” There is a lot of confusion about these sections. In my view, Section 20(2) currently allows the Commissioner to name the respondents whether or not the complaint is well-founded.

LEGISLATING TO THE CSA STANDARD

The most notable Canadian innovation in privacy law has been the integration of a standard within federal legislation. There was an explicit reason why the drafters of PIPEDA decided to legislate by reference to CSA's *Model Code for the Protection of Personal Information*. First, it was believed that, as the private sector had already negotiated this standard, that the legislation would be doing nothing more than forcing companies to "live up to their own rules." Secondly, and this point has been forgotten, the CSA standard is in itself a crucial mechanism to ensure compliance.

Unfortunately, there has been a tendency to ignore this instrument and conclude that the standard has "done its job" by providing a template upon which the legislation is based. I think such a view ignores the crucial role that the standard can play in supervising compliance with PIPEDA.

A mechanism is currently in place to ensure that organizations "say what they do, and do what they say." Registration to Q-830 should be encouraged for Canadian companies, and more crucially for organizations overseas to whom personal data has been transferred. Once an organization is registered to the standard, the *CSA Model Code* ceases to be a "voluntary" mechanism. That organization would have to produce a code and a related set of operational guidelines and be subjected to *regular and independent auditing* of its practices by an accredited registrar. Moreover, the sanction becomes, not only a fine, but an obligation to change practices after audit. This technique has been used to enforce environmental regulation, by obliging registration to the ISO-14000 standards. There is no reason why it cannot also be used to contribute to the enforcement of PIPEDA. It is an important technique that an under-resourced Office of the Privacy Commissioner can use in order to ensure a good level of compliance.

As currently drafted, PIPEDA regards the CSA standard as a template, rather than a method of enforcement. I would like to see a more explicit recognition (probably in section 24) that the Commissioner may require registration to the Q-830 standard through an accredited registration body, where there is evidence of non-compliance with the privacy principles in Schedule 1. This may also be stated more explicitly in section 18 (2), in which the Commissioner is empowered to delegate the powers of audit.

Moreover, I would have thought that any organization that has registered to the standard would have a powerful argument in the case of any investigation by the Commissioner of its practices. The demonstration that a code of practice is indeed complied with throughout the organization should have powerful evidentiary force. This should not exempt them from the provisions of PIPEDA, but it should carry evidentiary weight in any investigations by, or proceedings before, the Commissioner or the courts.

Registration to the CSA standard would also assist in the interpretation and enforcement of Principle 4.1.3 which requires organizations to "use contractual or other means to provide a comparable level of protection while the information is being processed by a third party." It could also assist with the tricky question of how to assure comparable levels of protection when personal data processing is outsourced to an overseas organization by a Canadian company. Contracts could, and should, reference the standard, registration to which is a condition for continual processing of Canadian personal data. This is an innovative solution, and one that has rarely if ever been contemplated.

This approach would only partially address the more controversial question of access to Canadian data by other governments for law enforcement and investigative purposes. Here I am in agreement with the position of CIPPIC. Subsection 7(3)(c.1) should be amended to make it clear that they apply to Canadian government institutions, not to foreign government agencies. With this amendment, then all requests by foreign governments for data about Canadians for investigative purposes would have to go through equivalent Canadian government agencies. It should also be remembered that protections against the onward transfer of personal data are critical in terms of Canada's relationship with the EU. The EU's Data protection Directive of 1995 prohibits transfers of personal data to countries which do not demonstrate "adequate" levels of data protection. Canada's laws have been declared adequate, even though there is no equivalent provision in PIPEDA.

IS PIPEDA WORKING?

This committee will receive a great deal of advice about the wording of PIPEDA – about its scope, about the definitions and about the various exemptions. While legislative language is, of course, critical, I would like to remind the committee that the effectiveness of the law will be more dependent on a number of other factors. I stated in my testimony in 1998 on the original Bill C-54 that compliance depends:

- *On the ability of the regime to encourage the voluntary adoption of information privacy principles.* This goal requires voluntary action from the "bottom-up" as well as regulatory action from the top-down.
- *On the use of the entire repertoire of possible policy instruments.* Although these hearings are concentrating on the content of the law, it should never be forgotten that any privacy protection regime has to rely on codes and standards, on the application of privacy-enhancing technologies and on the actions of an informed and vigilant citizenry. Each is a necessary condition for privacy protection on the information highway; none is a sufficient condition.
- *On the ability of the Privacy Commissioner to apply an "ounce of prevention."* Complaints resolution, investigation and individual redress are important, but more crucial powers are those that are general and anticipatory, rather than specific and remedial.
- *On the level of policy harmonization within Canada, and between Canadian policy and international standards.* The interconnected, dynamic, complicated and multi-faceted nature of personal data processing and communications places a heavy responsibility on government to ensure a level of harmonization within the Canadian federation, and between Canada and the international data protection standard contained within the European Union's 1995 Data Protection Directive.

By these standards, has this law been effective? Levels of compliance obviously vary. I believe that businesses in Canada can be divided into three general groups. Firstly, there are those large, high-profile companies who have in fact been leaders on the issue. These were the organizations which developed early codes of practice through their trade associations, and which in the mid-1990s participated in the development of the CSA's

Model Code for the Protection of Personal Information. My impression is that, while these businesses certainly face important challenges, they are generally compliant. But they are compliant not because of PIPEDA, but because they largely raised their standards before the Act was promulgated. A second category of business is the “free-rider”, the company that deliberately attempts to make money out of the processing of personal information without the individual’s knowledge and consent. My impression is also that many of these businesses have either been exposed as a result of PIPEDA, or have been put out of business.

By far the largest category are those in the middle – companies that process the full range of consumer and employee information, but who have never really been concerned about the issue, nor have they been pressed to be concerned either by their trade associations, by the Office of the Privacy Commissioner, by privacy advocates or by the media. They may have made an early effort to get a privacy policy, and appoint a responsible person, but have had no further exposure to the issue. It is my impression that the main problem lies in this group of companies. For these organizations, “privacy compliance has ceased to be a serious legal obligation.”²⁷

This Committee will no doubt receive some testimony from the business sector that it is a heavy-handed and intrusive piece of burdensome regulation. And no doubt some companies have had to change their practices and spend money to do so. But the reality is the opposite. In comparison with other privacy and data protection laws around the world, PIPEDA adopts a quite light mode of regulation. It depends upon the building of compliance from the bottom-up. Indeed the entire regime was founded on the theory that the CSA standard built upon existing codes of practice and the legislative framework should build upon the CSA standard. I have argued that this kind of approach had a chance of encouraging a more effective system of privacy protection than would a top-down command and sanction model enforced through law alone. I am still of that view but I also think the law needs to be reformed, particularly with respect to the Privacy Commissioner’s powers.

Recommendations

Here I repeat my recommendations above, but also add a few brief remarks about some of the issues identified in the Privacy Commissioner’s consultation document.

- 1) Provide the Office of the Privacy Commissioner with order-making powers similar to those enjoyed by the Information and Privacy Commissioners of Alberta and BC.
- 2) Subsection 7(3)(c.1) should be amended to make it clear that they apply to Canadian government institutions, not to foreign government agencies.
- 3) Provide more explicit recognition (probably in section 24) that the Commissioner may require registration to the Q-830 standard through an accredited registration body, where there is evidence of non-compliance with the privacy principles in Schedule 1. This may also be stated more explicitly in section 18 (2), in which the Commissioner is empowered to delegate his powers of audit.
- 4) The law clearly needs to be amended to deal with privacy breach notifications, and the committee will hear a lot of testimony on this subject. Having observed

how these laws do not work in the United States, I am in favour of a model which obliges organizations to notify the Privacy Commissioner about the loss or theft of personal information. The Privacy Commissioner would then have the authority to order the organization to notify affected individuals after a risk analysis.

- 5) The *Public Safety Act* amendments to PIPEDA have the potential to circumvent the carefully constructed consent regime and the separation between the private sector and law enforcement. The *public safety* amendments allow private organizations to collect and disclose personal information to law enforcement agencies without consent and put them in a position of acting as agents of the state. Section 7(1)(e) should either be rescinded completely or more narrowly drafted.
- 6) PIPEDA should also be amended to regulate willful *attempts* to collect personal information without consent.
- 7) PIPEDA should be amended to explicitly permit the Privacy Commissioner to share information and cooperate in investigations with counterparts in other countries and provinces that do not have “substantially similar” legislation.
- 8) PIPEDA should be amended to permit class action complaints and suits. PIPEDA’s enforcement regime (Section 12) is designed to serve only individual complainants. This focus on individual complaints and court actions does not reflect the social and collective impact of privacy invasions. I am therefore in agreement with CIPPIC that representative complainants and plaintiffs should be able to bring class actions for privacy breaches.

ENDNOTES

¹ *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Cornell University Press, 1992).

² *Visions of Privacy: Policy Choices for the Digital Age* (University of Toronto Press, 1999) (with Rebecca Grant).

³ Colin J. Bennett and Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (Cambridge: MIT Press, 2006).

⁴ *Implementing Privacy Codes of Practice* (Rexdale: Canadian Standards Association, PLUS 8830, August 1995).

⁵ *Regulating Privacy in Canada: An Analysis of Oversight and Enforcement in the Private Sector* (Industry Canada, 1996) at: <http://web.uvic.ca/bennett/>

⁶ Prospects for an International Standard for the Protection of Personal Information: A Report to the Standards Council of Canada (Ottawa: Standards Council of Canada, 1997) at: <http://www.cous.uvic.ca/poli/bennett/research/ISO.htm>

⁷ *Application of a Methodology designed to Assess the Adequacy of the Level of Protection of Individuals with regard to Processing Personal Data: Test of the Method on Several Categories of Transfer* (European Commission Tender No. XV/97/18/D, September 1998) (with Charles D. Raab, Robert M. Gellman and Nigel Waters)

<http://europa.eu.int/comm/dg15/en/media/dataprot/studies/adequat.htm>

⁸ I will be submitting a more thorough written set of recommendations.

⁹ *Regulating Privacy*, pp. 22-37.

¹⁰ Alan F. Westin, *Privacy and Freedom*, (New York: Atheneum), p. 25.

¹¹ Paul Sieghart, *Privacy and Computers* (London: Latimer, 1976), p. 76.

¹² Bennett, *Regulating Privacy*, pp. 95-115.

¹³ Bennett and Grant eds. *Visions of Privacy*, p. 6.

¹⁴ <http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html>

¹⁵ Organization for Economic Cooperation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Paris: OECD 1981.

¹⁶ Council of Europe. *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*. Strasbourg: Council of Europe, 1981.

¹⁷ Articles 25 and 26 of the Directive stipulate that personal data on Europeans should only flow outside the boundaries of the Union to countries that can guarantee an "adequate level of protection." European Union, *Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data*. Brussels: OJ No. L281.24 October 1995. (The EU Data Protection Directive).

¹⁸ Colin J. Bennett, "The Formation of a Canadian Privacy Policy: The Art and Craft of Lesson-Drawing" *Canadian Public Administration* 33 (1990): 551-570.

¹⁹ See, Colin J. Bennett, *Implementing Privacy Codes of Practice: A Report to the Canadian Standards Association* (Rexdale: CSA, PLUS 8830, 1995).

²⁰ Principally, Ekos and Associates, *Privacy Revealed: The Canadian Privacy Survey* (Ottawa: Ekos, 1993).

²¹ Information Highway Advisory Council, *Communication, Community, Content: The Challenge of the Information Highway* (Ottawa: Minister of Supply and Services Canada, 1995).

²² See <http://e-com.ic.gc.ca> for a copy of the legislation and related official documents and news releases.

²³ Murray Long and Associates Inc. *Response to the Privacy Commissioner of Canada PIPEDA Review Discussion Document* September 14, 2006), p. 7.

²⁴ Christopher Berzins, "Reviewing Pipedata: A Chance to Change Direction," Ontario Bar Association journal at: <http://www.oba.org/En/pri/jun06/Reviewing.aspx>

²⁵ Section 52(3) of Alberta's Personal Information Protection Act states: "If the inquiry relates to any matter other than a matter referred to in subsection (2), the Commissioner may by order do one or more of the following: (a) confirm that a duty imposed by this Act or the regulations has been performed or require that a duty imposed by this Act or the regulations be performed; (b) confirm or reduce a time period that was extended under section 31; (c) confirm, excuse or reduce a fee, or order a refund of a fee, in the appropriate circumstances; (d) confirm a decision not to correct personal information or specify how personal information is to be corrected; (e) require an organization to stop collecting, using or disclosing personal information in contravention of this Act or in circumstances that are not in compliance with this Act; (f) confirm a decision of an organization to collect, use or disclose personal information; (g) require an organization to destroy personal information collected in contravention of this Act or in circumstances that are not in compliance with this Act; (h) with respect to a personal information code established under Part 6 by a professional regulatory organization, require the professional regulatory organization to amend or otherwise change the personal information code so that it is consistent with the purposes and intent of sections 1 to 35.

²⁶ See the arguments of Murray Long, "Response to the Privacy Commissioner of Canada," p. 4

²⁷ John Lawford, *Consumer Privacy under PIPEDA: How are we Doing?* (Public Interest Advocacy Centre: November 2004).