



BC FREEDOM OF
INFORMATION
AND PRIVACY
ASSOCIATION



Statutory Review of the Personal Information Protection and Electronic Documents Act (PIPEDA)

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

November 2006

**A joint submission of
BC Freedom of Information and Privacy Association
and
BC Civil Liberties Association**

FIPA and BCCLA wish to acknowledge the Law Foundation of British Columbia for their ongoing support of the activities of FIPA and BCCLA in the areas of law reform, research and public education



**BC Freedom of Information
and Privacy Association**

103 - 1093 West Broadway
Vancouver, BC V6H 1E2
Ph: 604-739-9788 • Fax: 604-739-9148
Email: info@fipa.bc.ca
Web: www.fipa.bc.ca

BC Civil Liberties Association

550 – 1188 West Georgia Street
Vancouver, BC V6E 4A2
Ph: 604-687-2919 • Fax: 604-687-3045
Email: info@bccla.org
Web: www.bccla.org

Table of Contents

Introduction.....	1
Renewing the Commitment to the Protection of Privacy.....	2
Summary of Recommendations.....	12

Introduction

On February 9, 1999, I appeared before the Standing Committee on Industry to present my views, on behalf of Electronic Frontier Canada, on Bill C-54, PIPEDA. We supported Bill C-54 in principle. Now, on behalf of BC FIPA and the BCCLA I wish to renew our support of privacy protection in Canada by means of PIPEDA. However, there are a number of issues which must be addressed in order to ensure that the privacy of Canadians continues to be protected by this important piece of Federal legislation.

In this submission, we will address a number of issues related to both the legislation itself and the operation of the Office of the Privacy Commissioner (OPC) of Canada.

It is important to emphasize that privacy rights are increasingly under attack and a necessary bulwark in defense of these rights is at the very least adequate legislation supported by a vigorous agency to defend privacy rights and to draw attention to current and anticipated problems. The most important recommendation is that the current Ombudsman model for conflict regulation, employed by the OPC be replaced providing the Commissioner with order-making powers.

I should mention that I received a research grant from the Office of the Privacy Commissioner, August 2005 to April 2006, to explore privacy issues in the workplace. I am the author of *The Social Impact of Computers*¹ and several book chapters, refereed papers, and invited presentations on privacy issues. In addition, I have appeared before Parliamentary committees, in Ottawa and in Vancouver.

Dr. Richard S. Rosenberg
President, BC Freedom of Information and Privacy Association
Board of Directors, BC Civil Liberties Association
Professor Emeritus
Department of Computer Science
University of British Columbia
2366 Main Mall
Vancouver, BC V6T 1Z4
rosen@cs.ubc.ca

¹ Richard S. Rosenberg. *The Social Impact of Computers*, 3rd Edition, San Diego, CA: Elsevier Academic Press, 2004, 733pp.

Renewing the Commitment to the Protection of Privacy

Background

The BC Freedom of Information and Privacy Association (FIPA) is a non-profit society established in 1991 for the purpose of advancing freedom of information, open and accountable government, and privacy rights in Canada. We serve a wide variety of individuals and organizations through programs of public education, legal aid, research, public interest advocacy and law reform.

The B.C. Civil Liberties Association was established in 1962 and is the oldest and most active civil liberties group in Canada. We are funded by the Law Foundation of B.C. and by citizens who believe in what we do. We are a group of citizens who volunteer our energy and talents to fulfill our mandate: to preserve, defend, maintain and extend civil liberties and human rights in British Columbia and across Canada.

For both these organizations, and indeed for all Canadians, privacy rights are a hallmark of a democratic society and must be defended at all costs. The passage of PIPEDA was a major step in this defense, but more needs to be done as the assault on privacy is unrelenting, given the growth of electronic commerce, the online activities of Canadians, the endless appetite of government for information about its citizens, and the special needs of the 'war against terrorism'. Early in November 2006, the British Broadcasting Corporation reported that Richard Thomas, the Information Commissioner, had referred to Britain as, "waking up to a surveillance society that is all around us." Some of its characteristics are given as follows: ²

By 2016 shoppers could be scanned as they enter stores, schools could bring in cards allowing parents to monitor what their children eat, and jobs may be refused to applicants who are seen as a health risk.

A somewhat more detailed scenario, taken from the same report, and described in the Guardian, presents a chilly future. ³

A teenager enters a record shop and a scanner hidden in the doorway instantly reads data secreted in electronic tags embedded in his clothes. The scanner clocks the brand of clothing and where it was purchased, flashing to a database which analyses what type of person would have bought that line of clothing and predicts what other products that person would like to buy. In an instant, adverts for those products are beamed to eye-level billboards for the teenager to see.

² "Britain is 'surveillance society.' BBC News, November 2, 2006. Available at <http://news.bbc.co.uk/go/pr/fr/-/1/hi/uk/6108496.stm>

³ Rob Evans and Alex Mostrous, "Spy Planes, clothes scanners and secret cameras: Britain's surveillance future," Guardian Unlimited, November 2, 2006. Available at <http://www.guardian.co.uk/humanrights/story/0,,1037192,00.html>

The report referred to above, *A Report on the Surveillance Society*, provides a grim vision of a technological future, with privacy a major casualty. Consider the following: ⁴

To think in terms of surveillance society is to choose an angle of vision, a way of seeing our contemporary world. It is to throw into sharp relief not only the daily encounters, but the massive surveillance systems that now underpin modern existence. It is not just that CCTV may capture our image several hundred times a day, that check-out clerks want to see our loyalty cards in the supermarket or that we need a coded access card to get into the office in the morning. It is that these systems represent a basic, complex infrastructure which assumes that gathering and processing personal data is vital to contemporary living.

One additional selection may be helpful in shaping our views of the process that is currently taking place. ⁵

Conventionally, to speak of surveillance society is to invoke something sinister, smacking of dictators and totalitarianism. We will come to Big Brother in a moment but the surveillance society is better thought of as the outcome of modern organizational practices, businesses, government and the military than as a covert conspiracy. Surveillance may be viewed as progress towards efficient administration, in Max Weber's view, a benefit for the development of Western capitalism and the modern nation-state.

To set the context for some of the remarks to follow, let me turn to some comments I made a little more than six years ago, about the time PIPEDA was approved, at a meeting of a Special Committee on Information Privacy in the Private Sector, of the BC legislature. ⁶

These very few examples are indicative of the continuous stream of reports on yet another way that personal privacy has been violated and furthermore, they provide yet additional counterexamples to the argument that it is in the self-interest of business to respect the privacy concerns of its customers. I would reword this argument to read that it is in the self-interest of business to appear to respect the genuine privacy concerns of its customers. Whether or not the B.C. Legislature crafts its own version of privacy protection in the private sector, it should be aware of the scope and diversity of such assaults on personal privacy. Some old and some new terms and expressions should also be kept in mind, such as cookies, Carnivore (FBI variety), TrustE, on-line profiling, data mining, online privacy policies, Big Brotherware, Intel serial number, DoubleClick, Toysmart, Echelon, Coremetrics, Human Resources Development Canada's Longitudinal Labour Force File, and Britain's Regulation of Investigatory Powers Act (RIP).

⁴ David Murakami Wood (Eds.). *A Report on the Surveillance Society*, A Report for the Information Commissioner by the Surveillance Studies Network, September 2006. Available at <http://www.guardian.co.uk/humanrights/story/0,,1937192,00.html>

⁵ *Ibid.*

⁶ Richard S. Rosenberg. Submission to the B.C. Special Committee on Information Privacy in the Private Sector, September 21, 2000.

Of course, BC eventually adopted its own private sector legislation, the Personal Information Protection Act, as did Alberta.

Let me conclude this introduction with a strong defense of privacy as a fundamental right in a democratic society. It is unfortunate that privacy was not explicitly included as a basic right for Canadians in the Charter of Rights and Freedoms (1982). Nevertheless, since then the Supreme Court has "accorded privacy constitutional protection as a fundamental human right."⁷ In somewhat more detail:⁸

The function of the *Charter*, according to then Chief Justice Dickson, in *Hunter v. Southam*, "is to provide ... for the unremitting protection of individual rights and liberties."⁹ Privacy, grounded in individual moral and physical autonomy, is fundamental to *Charter* values of dignity and autonomy of the individual.¹⁰ Section 7 of the *Charter* provides that "everyone has the right to life, liberty and security of the person..." Privacy, the Supreme Court has said, is at the heart of liberty in a modern state, and the limits the *Charter* imposes on government to pry into the lives of its citizens go to the essence of a democratic state.¹¹

In 1928, U.S. Supreme Court Justice Louis Brandeis put it best in an often-quoted passage from a dissenting opinion:

The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness.... They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They confirmed, as against the Government the right to be let alone—the most comprehensive of rights and the right most valued by civilized men. To protect that right every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.¹²

Issues of Concern

In the main body of this submission, we will depend on a document circulated by the Office of the Privacy Commissioner (OPC) of Canada, namely, the PIPEDA Review Discussion Document,¹³ which solicited comments from interested parties on a variety of important and topical issues, in anticipation of the PIPEDA review. Our concerns will include both issues related to PIPEDA itself as well as the administration of the Act by the OPC.

⁷ Richard S. Rosenberg and Susan Prosser. Health Information in Canada: Can Privacy Be Protected? A Draft Report, August 2000, for B.C. Freedom of Information and Privacy Association, pp. 133

⁸ *Ibid.*

⁹ *Hunter v. Southam*, [1984] 2 S.C.R. 145, p. 160.

¹⁰ *R. v. Osolin* (1994), 109 D.L.R. (4th) 478

¹¹ *Dyment*, p. 513.

¹² Justice Louis D. Brandeis, Dissenting, *Olmstead v. United States*, 277 U.S. 438, 1928

¹³ "Protecting Privacy in an Intrusive World," PIPEDA Review Discussion Document, Privacy Commissioner of Canada, July 2006. Available at

http://www.privcom.gc.ca/information/pub/pipeda_review_060718_e.pdf

1. Publicizing Complaints

For the most part, the OPC has decided not to reveal the names of complainants nor the organization and companies against which complaints have been launched. It does appear that under the current regimen, there is little cost to companies that do not resolve their privacy issues. Not properly implementing a required privacy regimen is just a small cost of doing business. Public attention would be a much more effective means to achieve compliance.

2. A Much More Effective Education Function

The OPC could serve a more effective role than it has up to now, namely, to bring the Office and its role under PIPEDA to the attention of the Canadian public. In my classes and talks I have rarely found anyone who knows about Canada's privacy law, his or her rights under the law, the existence of the OPC, the current Privacy Commissioner, and the activities of the OPC.

It is probably the case that financial limitations prevent the OPC from effectively bringing its existence and function to the attention of the Canadian public. It is necessary that Parliament recognize the importance of the OPC and provide a sufficient budget for it to exercise its responsibilities in an effective manner.

3. Response of Companies to Breaches of their Security

What if anything should companies be required to do when their security barriers are breached, with the resulting release of personal information? Such events have become fairly frequent with most of the attention directed towards companies whose primary activity is the collection, compilation, and marketing of personal information. When PIPEDA came into effect, the term 'identity theft' probably was little known; now ID theft is well known as one of the major crimes associated with Internet technology.

Consider the chart below, which features some of the major recent cases of security breaches in the U.S. and keep in mind that it is likely that information about Canadians was included in the files of credit card companies.¹⁴

Note that the number affected refers to the total number of records that were estimated to have been released, not necessarily subsequently misused.

¹⁴ Gary Rivlin. "Keeping Your Enemies Close," *The New York Times*, November 12, 2006, pp. BU Pages 1, 9-10. Available at <http://www.nytimes.com/2006/11/12/business/yourmoney/12choice.html?ref=business>

SOME SECURITY BREACHES

Name	Date	Number Affected
Choicepoint	February 2005	163,000
CitiFinancial	June 2005	3.9 million
CardSystems Solutions	June 2005	40 million
Office of the Ohio Secretary of State	April 2006	7.7 million
U.S. Department of Veterans' Affairs	May 2006	28.8 million
Chase Card Services	September 2006	2.6 million

It is no wonder that identity theft has become the crime of choice of the "Information Age." A number of U.S. states have passed notification laws to inform individuals that their personal information has been breached; California was the first of these. A legislative summary follows: ¹⁵

Effective July 1, 2003, Senate Bill 1386, the Security Breach Information Act, attempts to stem the growth of identity theft by mandating the public disclosure of computer security breaches in which confidential information of any California resident may have been compromised. The California law defines personal information as a last name paired with a first name or first initial and one of the following: a social security number, a driver's license or California Identification Card number, or a number from a bank account, credit card or debit card, along with a password or security code that would give access to the account. (SB 1386 exempts personal information that a company has stored in an encrypted format.)

Finally, affected customers must be informed as quickly as possible by written notification or electronic notice on the company's website or Email notice when the agency has a provided customer address. ¹⁶ Canada should follow suit.

4. Transborder Data Flows of Personal Information of Canadians

The OPC has brought this issue to the attention of the Canadian public, especially with regard to the possible access of the personal information of Canadians, held in the U.S., by the FBI under the USA PATRIOT Act. In 2004, this issue arose in BC because the government had outsourced medical records to the subsidiary of the MAXIMUS corporation, a U.S. company. After the BC Information and Privacy Commissioner, David Loukidelis, issued a report on the

¹⁵ The Security Breach Information Act (SB 1386). Available at <http://www.watchfire.com/securityzone/sb1386.aspx>

¹⁶ *Ibid.*

issues raised by this action, the BC government introduced and passed legislation, with the following requirements: ¹⁷

- No remote access to data from outside of Canada.
- Special restrictions on data access and supervision requirements of US employees.
- All employees and sub-contractors who have access to data will sign non-disclosure agreements with the province.
- A whistleblower hotline will be available for employees.
- The Province can take over the operations of MAXIMUS BC in the event of potential disclosure of personal information.

It is important that the Federal Government provide sufficient, additional strength to PIPEDA to deal with this class of issues. However, the question remains how the personal information of Canadians is to be protected when that information resides outside Canada, more specifically in the U.S., which does not have a federal law protecting individual privacy in the private sector. Furthermore, as mentioned above, the USA PATRIOT Act overrides any possible privacy protection.

5. Workplace Privacy Issues

Material in this section will be taken from a report written by Vance Lockton and Richard S. Rosenberg, ¹⁸ which begins as follows:

Do Canadian employees lose fundamental human rights when they enter the workplace? The quick answer to this question is 'no'; however, this response deserves some consideration. Workers are frequently faced with background checks, drug and medical tests, and/or routine electronic surveillance of their actions, both in the physical and the online worlds. Companies looking to protect themselves from litigation or costly medical claims, as well as to maintain the proper corporate image, are increasingly scrutinizing employees' off-duty activities as well. At what point, though, does this monitoring invade the individual's right to privacy (as defined by the U.N.'s Declaration of Human Rights)? To what extent are Canadians willing to allow corporate interests to supercede those of the individual? Also, should they choose to oppose surveillance, what legal protections do Canadian employees have?

¹⁷ Government Moves to Improve MSP and Pharmacare Services. News Release, Minister of Health Services, Province of British Columbia, November 4, 2004. Available at <http://www.healthservices.gov.bc.ca/cpa/mediasite/pdf/2004HSER0073-000919.pdf>

¹⁸ Vance Lockton and Richard S. Rosenberg. A Preliminary Exploration of Workplace Privacy Issues in Canada, Office of the Privacy Commissioner of Canada Contributions Program, April 2006. Available at <http://www.cs.ubc.ca/~lockton/workplace.pdf>

Furthermore, PIPEDA does not cover information collected by employers about non-federally regulated private sector employees. "In fact, with the exception of workers in B.C., Alberta and Quebec, each of which has passed its own privacy legislation, Canadian private sector employees have little to no protections for their privacy rights." Two main relevant parts of PIPEDA are as follows: ¹⁹

- Section 5(3): An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate under the circumstances.
- Section 7(1)(b): [An organization may collect personal information without the knowledge or consent of the individual only if] it is reasonable to expect that the collection with the knowledge or consent of the individual would compromise the availability or the accuracy of the information and the collection is reasonable for purposes relating to investigating a breach of an agreement or a contravention of the laws of Canada or a province.

There are two important differences between the Personal Information Protection Acts (PIPAs) of BC and Alberta and PIPEDA that are relevant to workplace privacy issues, ²⁰

- First, the PIPAs are not restricted to public works; they apply instead to "all organizations." Thus, companies in the private sector in both Alberta and BC cannot collect employee personal information without reason or justification; all the standards of reasonable collection, use and disclosure provided by PIPEDA for public sector employees are in force.
- Secondly, an interesting clause in both PIPAs concerns the collection, use and disclosure, without consent, of employee personal data, essentially stating that consent is not required for reasonable collection of information, so long as notification is given.

Workplace privacy issues should, therefore, be re-examined.

6. The Development of the Electronic Medical Record (EMR) and its Privacy Implications

It will be recalled that when PIPEDA was enacted, the application of the law to the protection of medical records was postponed for one year in order to provide for additional consultation to deal with any special issues associated with such records. PIPEDA now applies to medical records, but no changes seem to have taken place. It should be acknowledged that medical information is the most sensitive of all personal information and therefore must be accorded the highest level of protection. The courts have recognized the

¹⁹ *Ibid.*, pp.18-19.

²⁰ *Ibid.*, p. 20

sanctity of the doctor-patient relationship and it is central to the Hippocratic Oath, namely,²¹

What I may see or hear in the course of treatment or even outside of treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself holding such things shameful to be spoken about.

Currently, across the country, provincial Ministries of Health, with the financial assistance of the Federal Government, are in the process of developing the complex Information Technology systems necessary to implement a comprehensive medical information system dependent on the Electronic Medical Record (EMR). The crucial privacy issues arising from these major projects focus on who has access to an individual's medical record; whether the medical record can be partitioned into different levels of privacy protection and accordingly different levels of access; and whether access can depend, for very sensitive parts of the EMR, solely on the patient himself or herself.

The Code of Ethics of the Canadian Medical Association speaks specifically of the patient's privacy rights as follows:²²

Respect the patient's right to confidentiality except when this right conflicts with your responsibility to the law, or when the maintenance of confidentiality would result in a significant risk of substantial harm to others or to the patient if the patient is incompetent; in such cases, take all reasonable steps to inform the patient that confidentiality will be breached.

It is therefore necessary to revisit the special qualities of health records, as implemented in the EMR, with respect to their privacy protection. One model incorporates the idea of a 'lock box' containing the most sensitive health information possessed by an individual. Thus while other parts of the EMR may be available to legitimate requests, without the individual's specific approval, information in the lock box requires obtaining the patient's explicit approval every time it is requested.

7. The Challenges of Emerging Privacy-Threatening Technologies

Protection of privacy in the face of emerging technologies has become a recurring theme of our time and is likely to continue without diminishing. Such an environment may represent a continuous series of challenges to privacy legislation which must be interpreted in the context of an environment unforeseen and only dimly appreciated in the early stages. For example, consider Radio Frequency Identification, or RFID, "a technology which has been receiving considerable attention as of late. It is a fairly simple technology

²¹ Patient Confidentiality and Preventing Harm to Others, HIV/AIDS and the Privacy of Health Information, 2002-2004. <http://www.aidslaw.ca/publications/interfaces/downloadFile.php?ref=187>

²² *Ibid.*

involving radio wave communication between a microchip and an electronic reader, in which an identification number stored on the chip is transmitted and processed; it can frequently be found in inventory tracking and access control systems.”²³

What is particularly interesting about RFID technology is that from initial applications in inventory control, a basic non-privacy threatening use, very soon new applications in passports and implantable identification chips began to appear. These applications offer challenges from expanded personal marketing, to a lack of anonymity in a number of applications, and more specifically, in human tracking. RFID is typical of new technologies in the privacy threats that seem to emerge beyond initial applications. It demands careful study and subsequent action, including limiting retail use, prevention of hidden readers, and also the prevention of RFID chips in driver’s licenses:²⁴

RFID is a new type of threat to personal information and must be treated as such; indeed, it must be recognized that existing privacy legislation is not adequate. New laws must be passed to control the use of RFID if it is to be welcomed by an already skeptical public; the three points of necessary legislation listed above will be a necessary beginning to the control process.

Earlier this year, the following story appeared:²⁵

A Cincinnati video surveillance company City Watcher.com now requires employees to use VeriChip (<http://www.verichipcoro.com>) human implantable microchips to enter a secure data centre. Until now, the employees entered the data centre with a VeriChip housed in a heart-shaped plastic casing that hangs from their keychain. The VeriChip is a glass encapsulated RFID tag that is injected into the triceps area of the arm to uniquely identify individuals. The tag can be read by radio waves from a few inches away.

Can existing privacy legislation deal with such challenges? If not the research supported by the OPC must be expanded in order to be properly prepared.

8. Current Views of Some Aspects of Consent in PIPEDA

In a discussion document released in July 2006,²⁶ the OPC attempted to solicit views from Canadians about its operation as well as the effectiveness of PIPEDA, in anticipation of the forthcoming mandatory review. Of all the issues presented, almost half of the space was dedicated to a variety of issues related to consent. These issues included the following:²⁷

²³ Vance Lockton and Richard S. Rosenberg. RFID: The Next Serious Threat to Privacy, *Ethics and Information Technology*, Vol. 7, No. 4, December 2005, pp. 221-231.

²⁴ *Ibid.*

²⁵ Jan Libbenga. Video Surveillance Outfit Chips Workers, *The Register*, February 10, 2006.

Available at http://www.theregister.co.uk/2006/02/10/employees_chipped/

²⁶ *Op. cit.* “Protecting Privacy in an Intrusive World.”

²⁷ *Ibid.*

Reconciling the consent principle with the realities and demands of the commercial environment presents several challenges. The following discussion examines specific areas of concern relating to consent: employer/employee relationships; collection of personal information and disclosure to law enforcement and national security agencies; disclosure to investigative bodies; attempted collection, use and disclosure; individual, family and public interest exceptions to consent requirements; and blanket consent.

For the present, we will focus on two areas: (b) collection and disclosure for law enforcement and national security purposes and (d) attempted collection without consent. Is the authority to collect personal information without the knowledge or consent of the individual in section 7(1)(e) broader than necessary? If so, how might the provision be amended to limit the authority for organizations, subject to PIPEDA, to collect information? We are of the opinion that the authority to collect personal information without the knowledge or consent of the individual in section 7(1)(e) is too broad.

In sections 7(3)(c.1)(i) and (ii) where law enforcement and investigations are discussed, we are of the opinion that private companies should insist on seeing a court order from a law enforcement or investigative agency (except in exceptional and urgent cases) before disclosing any personal information. Insistence on a court order subjects the information request to a public review process and also protects the organization from subsequent litigation. A yet unspecified list of government institutions will have the right to compel disclosure of information about individuals without even their knowledge to administer any law. Even if such information may be disclosed without consent, we question the absence of knowledge in the case of an administrative purpose

After a commercial organization has collected the information, there are no restrictions on the organization for use of the collected information. We recommend that a clause be added to restrict use of collected information under section 7(1)(e). It seems that section 7(1)(e) was created by Parliament with the intention of it applying only to a narrow field of information linked to national security interests." ²⁸

What about collection without consent? Should PIPEDA be amended to regulate willful attempts to collect personal information without consent? Despite the fact that no personal information may actually have been collected, attempted collection signifies motive of the company to contravene PIPEDA. The privacy rights of the individual are being put at risk, and therefore attempted collection should be considered an offence under PIPEDA.

There are other areas of concern and a comprehensive examination should be undertaken

²⁸ Murray Long, from the newsletter, *Privacy Scan: Analysis and Insight into Bill C-6, the Personal Information Protection and Electronic Documents Act*, March 26, 2000.

9. The Ombudsman Model Versus Order-Making Powers

The OPC of Canada is committed to the Ombudsman model of mediation. Complaints are heard, meetings are held, and non-binding recommendations are issued, with the names of all parties almost always concealed. If dissatisfied, a complainant can bring the case to the Federal Court, at his or her own expense. Has this model been effective? There is some disagreement in public responses to this question. Certainly the OPC seems to be committed to its current mode of operation. It is significant that in the three other provinces in Canada with their own version of PIPEDA, British Columbia, Alberta, and Quebec, the model used involves order-making powers. That is, complaints are heard, decisions, with legal force, are made public and parties are named. Thus the full force of public scrutiny serves as a constant light shining on the privacy practices of companies and organizations. Negative publicity is not something that is in their self interest.

Unlike Canada and the European Union, the U.S. does not have a general Federal privacy protection law for the private sector, and limited coverage for the public sector. Arguments against the enactment of such a law from U.S. companies have focused on the impact of negative publicity with the common call, "Let the marketplace decide."²⁹ It is important to note that in a research project for the BC Civil Liberties Association, Kirk Tousaw recommends that, "The Commissioner should be explicitly given the power to issue orders that are able to be filed with the Federal Court and made immediately enforceable."³⁰

Thus the single most important recommendation made in this submission is that the OPC be give order-making power.

Summary of Recommendations

1. The OPC should publicize the complaints it deals with.
2. The OPC should undertake an ongoing program to publicize its activities as a means of educating the Canadian public about its privacy rights and protections.
3. Companies and agencies should be required to inform their clients about security breaches that threaten their personal privacy.

²⁹ R. S. Rosenberg. Privacy protection on the Internet: The marketplace versus the state. *Wiring the World: The Impact of Information Technology on Society*, IEEE Society on Social Implications of Technology, Indiana University South Bend, June 12-13, 1998, pp. 138-147. Available at: <http://www.ntia.doc.gov/ntiahome/privacy/files/5com.txt>

³⁰ Kirk Tousaw. Securing Compliance, Protecting Privacy. The PIPEDA Enforcement Evaluation Research Project, Submitted by the BCCLA to the OPC of Canada, March 2006. Available at <http://www.bccla.org/othercontent/FINAL%20Report.April06.pdf>

4. The Federal Government must explore ways to provide protection for the personal information of Canadians which may reside outside of Canada.
5. PIPEDA must be amended to provide more workplace privacy protection for those workers under federal privacy jurisdiction.
6. Personal medical information as captured in the Electronic Medical Record must be given greater protection, with individuals having a final right of consent for disclosure of particularly sensitive information.
7. The challenges of emerging privacy-threatening technologies must be confronted as soon as possible
8. Some of the sections of PIPEDA dealing with consent must be reviewed as increasingly the rights of citizens are abrogated by external needs such as the Anti-terrorism Act and the Public Safety Act.
9. Given the experience with the current Ombudsman model in the OPC, it is recommended that the Commissioner be given order-making powers such as those available to the Commissioners in BC, Alberta, and Quebec.