Canadian Internet Policy and Public Interest Clinic
Clinique d'intérêt public et de politique d'internet du Canada

Submission to the House of Commons Standing Committee on Access to Information, Privacy and Ethics

on

the *Privacy Act*

May 06, 2008

Canadian Internet Policy and Public Interest Clinic (CIPPIC)
University of Ottawa, Faculty of Law
57 Louis Pasteur, Ottawa, ON K1N 6N5
tel: 613-562-5800 x2553
fax: 613-562-5417
www.cippic.ca

Executive Summary

The *Privacy Act* is badly out-of-date and does not adequately protect Canadians from inappropriate collection, use and disclosure of their personal information by the federal government. It is in need of a thorough review and overhaul.

This submission highlights some of the reforms needed in order to address deficiencies in the Act. It is not intended to be comprehensive. Specific recommendations include:

To achieve transparency and accountability:

1. Limit subs.8(2)(f) to agreements or arrangements that are in writing, that have been authorized by an Act of Parliament, and that are listed in a regulation under the *Privacy Act*;

2. Amend subs.8(2) to require notice of uses and disclosures not originally contemplated when the information was collected, except where inappropriate;

3. Strengthen annual reporting requirements of government agencies under s.72 as recommended by the Privacy Commissioner;

4. Supplement s.63 with a clause permitting disclosures in the public interest.

To protect Canadians from abusive treatment by foreign states:

5. Consider adopting an "adequacy" or "comparable protection" standard for disclosures to foreign entities;

6. Limit the exception in subs.8(2)(c) to *Canadian* courts, persons or bodies;

7. Limit information disclosure and subsequent use under subs.8(2)(f) to the precise purpose identified by the disclosing agency, to the data necessary for that purpose, and to the body disclosed to;

8. Require that institutions disclosing personal data to a foreign entity:
    a. identify the precise purpose for which the data will be disclosed and limit its subsequent use by the foreign entity to that purpose;
    b. limit the personal data disclosed to that necessary for the purposes identified;
    c. restrict further disclosure to third parties.

9. Consider legislating additional protections against direct access by foreign governments to personal data about Canadians held by private companies to which the federal government has outsourced data processing activities.

To make the Act enforceable:

10. Give the Privacy Commissioner order-making powers;

11. Expand s.41 of the *Act* so as to make all rights, not just access to information rights, enforceable;

12. Provide for redress in cases involving harm. Consider adopting a provision under which individuals are entitled to a minimum of $1,000 in damages, as well as legal fees, for intentional or willful government violations of the *Act*.

To prevent over-collection of personal data:

13. Amend s.4 of the *Act* to require that "No personal information shall be collected by a government institution unless it relates directly to *and is necessary for* an operating program or activity of the institution".

To protect against inappropriate surveillance where data is not recorded:

14. Amend the definition of "personal information" in s.3 of the Act to delete the phrase "*that is recorded in any form*".

To ensure that privacy impacts are fully considered before implementation of government programs and services:

15. Adopt a new provision requiring Privacy Impact Assessments of new programs and services prior to implementation.

To provide stronger incentives for effective security measures and to allow individuals to mitigate potential harms from security breaches:

16. Enact a new provision requiring that government bodies:
    (a) take reasonable security measures to protect personal data from unauthorized access, use or disclosure; and
    (b) notify affected individuals of security breaches exposing their data to potentially harmful uses.

CIPPIC

The Canadian Internet Policy and Public Interest Clinic (CIPPIC), based at the University of Ottawa, Faculty of Law, seeks to ensure balance in policy and law-making processes by representing under-represented interests on issues that arise as a result of new technologies. Law students work under the supervision of the Clinic director and staff counsel on projects and cases involving the intersection of law, technology and the public interest. CIPPIC engages in policy development, legislative advocacy, public education, client advice, and precedent-setting litigation. Issues addressed include privacy, copyright, free speech, domain name governance, and consumer e-commerce. Many clients come to the clinic for advice on privacy-related matters.

Philippa Lawson, Director of CIPPIC, is a nationally recognized privacy lawyer and advocate. She has worked with Canadian and international consumer organizations since the early 1990s on many privacy-related issues, including implementation of federal private sector data protection legislation ("PIPEDA"). Prior to starting up CIPPIC in 2003, she was senior counsel for the Public Interest Advocacy Centre. Ms. Lawson is actively engaged in privacy-related research and advocacy from the public interest perspective, and is a frequent speaker on privacy-related issues at conferences and workshops in Canada and internationally.

In addition to its extensive research and advocacy on private sector data protection law in Canada, CIPPIC has investigated and filed complaints under the federal *Privacy Act*, and has analysed the effectiveness of public sector data protection legislation in the context of its research on identity theft, internet security, foreign outsourcing, and general rights to privacy in the context of new technologies. For more information, see www.cippic.ca (under "Projects – Privacy").

The *Privacy Act*: Overdue for Reform

Introduction

The federal *Privacy Act* was introduced in the early 1980s, before the revolutionizing effect of computers and related new technologies had taken hold on society. Twenty-five years later, we are in a different world – one in which governments (as well as private corporations and individuals) have the ability to collect, retain, access, manipulate, use and disclose personal data in ways that were previously unimaginable. Technology has provided government with a remarkably enhanced ability to profile and monitor citizens using data gathered from both public and private sources. It is up to Canadian legislators to ensure that we have appropriate legal constraints in place to prevent the abuse of such technical powers.

It is surprising that the Canadian government has not seen fit to update the *Privacy Act* despite repeated calls by Privacy Commissioners over the past quarter century, despite a 1987 Standing Committee Report calling for specific reforms[1], despite provincial public sector laws that are stronger than the federal statute, and, now, despite a private sector law that gives consumers more rights and remedies against corporate privacy invasions than the *Privacy Act* gives citizens against privacy invasions by the federal government.

Unlike the private sector, government has a special trust relationship with its citizenry. The federal government collects and uses often highly sensitive personal information about individuals in order to deliver public services and programs. Individuals, for the most part, have no choice in this matter – they are required to hand over their information and must trust the government to protect it from abuse. At the same time, the potential for abuse is higher than ever, given ever-increasing technological capabilities and political pressures. In this context, it is critical that Canada have a strong legislative framework governing public sector collection, use and disclosure of personal data. The *Privacy Act*, as currently drafted, fails to do the job.

We applaud this Committee in undertaking a review of this important piece of legislation, and sincerely hope that this review marks the beginning of a serious initiative by Parliament to reform a statute in dire need of attention.

General Reform Agenda

The Privacy Commissioner has provided a roadmap to the reforms needed in order to bring the *Privacy Act* into the 21st century. Her June 2006 report *Government Accountability for Personal Information: Reforming the Privacy Act*, together with her April 2008 *Addendum*, sets out the rationale for reform in a number key areas, as well as

[1] *Open and Shut; Enhancing the Right to Know and the Right to Privacy*, Report of the Standing Committee on Justice and Soclicitor general on the Review of the *Access to Information* and the *Privacy Act* (March 1987).

specific proposals for legislative change. These documents provide the Committee with an excellent basis on which to move forward quickly with much-needed law reform.

As the Privacy Commissioner has set out in her June 2006 report, the *Privacy Act* needs a complete overhaul. Although some "quick fix" amendments are better than none, the legislative deficiencies in this case are so numerous and substantial as to warrant a thorough re-examination of the statute. We urge this Committee to take on the task, and to devote the time and resources necessary to do it properly. In particular, **we call on the ETHI Committee to undertake a full review of the *Privacy Act* with a view to recommending amendments by the end of 2008.**

CIPPIC's Interest in Public Sector Privacy Law

As a clinic that serves the Canadian public and whose mission is to ensure that the public interest is robustly represented in policy-making on issues arising from the use of new technologies, CIPPIC is concerned about both corporate and state surveillance made possible by new technologies. Unless law-makers keep up with the pace of technological development, we will continue to race headlong into a surveillance society determined not by what we decide is socially desirable but by what is technologically possible and useful from state and corporate perspectives.

This Committee recently undertook a major review of private sector data protection legislation ("PIPEDA") that was only a few years old. Now is the time to undertake a similar review of much older public sector data protection legislation.

As noted above, CIPPIC has worked on a number of issues involving the federal *Privacy Act*. Some issues (e.g., online publication of personal data by federal boards and tribunals; outsourcing of government activities involving sensitive personal data to foreign companies; sharing of personal data with foreign governments) came to us from clients or members of the public. Others (e.g., limits on government collection, use and disclosure of personal data; sale of aggregated census data to commercial data-brokers who re-personalize it for marketing purposes; obligations on government to keep personal data secure and to inform individuals of security breaches that expose their personal data to potential abuse) have arisen in the context of policy research on issues such as identity theft and consumer profiling. Our analysis of the *Privacy Act* in these contexts has highlighted a number of deficiencies.

Deficiencies in the *Privacy Act*

We have not undertaken a thorough review of the Act, and are not in a position at this time to propose a comprehensive set of proposed reforms. Instead, our proposals focus on those deficiencies of the statute that have become apparent to us in our work. These are not presented in any particular order of priority, and do not represent the full suite of amendments that are needed, We believe that the priority of this Committee should be to launch a thorough review of the Act with the intention of presenting Parliament with a full set of amendments by the end of 2008.

1. Accountability / Transparency

It is often extremely difficult – if indeed possible - for citizens and public interest advocates to figure out the extent to which the federal government is collecting, using and disclosing personal information of Canadians for particular purposes.

Disclosures to foreign states and bodies

This is especially true with respect to national security and trans-border data flows. We have been unable, for example, to identify and review the many information-sharing agreements and arrangements that exist between Canada and foreign governments, in order to determine whether Canadians are significantly better protected from foreign state surveillance when their data is held by Canadian entities (vs. foreign) entities.

Although the *Privacy Act* contains a number of provisions designed specifically to ensure transparency of government data management practices, it allows for non-consensual use and disclosure of personal information "under an agreement or arrangement between the Government of Canada…and the government of a foreign state….for the purpose of administering or enforcing any law…" (s.8(2)(f)).

In other words, the *Privacy Act* allows government bodies to share personal information about Canadians with foreign states for purposes that could be at odds with fundamental principles of democracy and human rights, and to do so without even the limited transparency that would be achieved through requirements that such agreements and arrangements be made in writing and authorized by legislation.

Subs.8(2)(f) should be limited to agreements or arrangements that are in writing, that have been authorized by an Act of Parliament, and that are listed in a regulation under the *Privacy Act*.

Notice of Secondary Uses and Disclosures

Unlike PIPEDA, the *Privacy Act* permits secondary uses and disclosures of personal data without the individual's knowledge or consent, as long as such uses and disclosures are "consistent" with the purpose for which the data was originally collected. We share the Privacy Commissioner's concern that the term "consistent use" is far too broad and should be replaced with a narrower test. Whatever the test, however, individuals deserve to be notified of new uses and disclosures that they would not reasonably expect based on the initial collection. If consent is not required, at least notice should be required for all "consistent uses" other than those for which such notice would be counter-productive.

Subs.8(2) should be amended to require notice of uses and disclosures not originally contemplated when the information was collected, except where inappropriate.

Require public reporting of PIAs, data-matching, and data-sharing programs

Canadians deserve to know how their personal information is being handled, used and disclosed by the federal government. They should be given an opportunity to review proposals for new programs, services or activities that involve data-matching, data-sharing or other privacy implications. We therefore strongly support the Privacy Commisisoner's recommendation to **strengthen annual reporting requirements of government agencies under s.72**.

Authorize the Commissioner to disclose information in the public interest

Canada's private sector data protection law authorizes the Commissioner to disclose information about organization practices if she "considers that it is in the public interest to do so" (subs.20(2)). The *Privacy Act* should contain a similar power, so that the Privacy Commissioner can report in a timely way on relevant issues arising from her investigations. In particular, **s.63 should be supplemented with a clause permitting disclosures in the public interest.**

2. Trans-Border Data Flows: Protect Against Foreign Government Abuses

In addition to lack of transparency with respect to data-sharing with foreign states, the *Privacy Act* lacks basic safeguards against abuse by foreign states of such data. Unlike Quebec and Europe, Canada does not limit data-sharing to jurisdictions with comparable or adequate data protection laws, with the result that Canadians are more vulnerable to unacceptable treatment by foreign entities on the basis of information provided by the Canadian government to such entities. **Consideration should be given to adopting an "adequacy" or "comparable protection" standard for disclosures to foreign entities.**

At a minimum, the *Privacy Act* should:

- **require that the disclosing institution identify the precise purpose for which the data will be disclosed and limit its subsequent use by the foreign entity to that purpose;**
- **limit the personal data disclosed to that necessary for the purposes identified;**
- **restrict further disclosure to third parties.**

Moreover, subs.8(2)(c) allows for secret disclosures of personal data "for the purpose for the purpose of complying with a subpoena or warrant issued or order made by a court, person or body with jurisdiction…", without limiting such bodies to *Canadian* courts, persons or bodies. In other words, the *Act* permits Canadian institutions to hand over data about Canadians to foreign states in response to foreign state orders that may not meet basic standards of justice under Canadian law.

Subs.8(2) should be amended so as to:

- **limit the exception in subs.8(2)(c) to *Canadian* courts, persons or bodies with jurisdiction;**
- **limit information disclosure and subsequent use under subs.8(2)(f) to the precise purpose identified by the disclosing agency, to the data necessary for that purpose, and to the body disclosed to.**

Many Canadians are justifiably concerned about the *USA PATRIOT Act* and the rights that it confers on U.S. law enforcement officials to secretly access personal information held by private entities for the purpose of counter-terrorism. In fact, surveys conducted for the Office of the Privacy Commissioner indicate high levels of concern by most Canadians about government outsourcing to foreign companies.[2] The *Privacy Act* offers no protection against such disclosures. Indeed, it does not even state that government institutions are responsible for protecting personal data transferred to third parties for processing (as PIPEDA does in respect of private sector organizations).

In contrast, the governments of British Columbia and Nova Scotia have enacted statutory protections against foreign state access to citizen data held by private organizations to which the government has outsourced.[3] Treasury Board has developed a strategy to address these concerns, but as with all such policies, the strategy has no legislative clout.

Serious consideration should be given to legislating protections such as those adopted by the B.C. government to protect against direct access by foreign governments to personal data about Canadians held by private companies to which the federal government has outsourced data processing activities.

3. Make the Act Enforceable

The *Privacy Act* has been recognized by the Supreme Court of Canada as "quasi-constitutional" legislation, given the role that privacy plays in the preservation of a free and democratic society.[4] It is particularly strange, then, that neither the Privacy Commissioner nor individual Canadians are able to enforce their rights under it, except with respect to access to information requests.

Both the Privacy Commissioner and individual citizens should be able to enforce the Act and seek redress in appropriate cases. Without an enforcement regime for privacy violations, individuals have no way of obtaining remedies for harmful breaches, and the government is insulated from the consequences of its wrongful or negligent acts.

---

[2] EKOS Research Associates, *Revising the Privacy Landscape a Year Later* (March 2006); <http://www.privcom.gc.ca/information/survey/2006/ekos_2006_e.asp>

[3] See Privacy Commissioner of Canada, *Proposed Immediate Changes to the Privacy Act* (April 29, 2008), Recommendation Number 10.

[4] *Canada (Information Commissioner) v. Canada (Commissioner of the Royal Canadian Mounted Police)*, [2003] 1 S.C.C. 66; *Lavigne v. Canada (Office of the Commissioner of Official Languages),* [2002] 2 S.C.C. 773; and *H.J. Heinz Co. of Canada Ltd. v. Canada (Attorney General),* [2006] 1 S.C.R. 441.

At a minimum, the Privacy Commissioner and individuals should be able to enforce their rights under the *Privacy Act* and obtain redress in appropriate cases by way of court action. S.41 of the *Act* should be expanded to cover all rights, not just access to information rights.

While better than no enforcement at all, enforcement exclusively via the Federal Court has proven to be of limited effectiveness given the high cost of litigation and difficulty quantifying damages caused by privacy invasions. **A more effective approach would give the Privacy Commissioner order-making powers, as a number of provinces have done.** This would not only give the Commissioner more clout, but would break down barriers to individual enforcement of the *Act*. Individuals could still be required to go to court for damages.

With respect to damages, we recommend consideration of the U.S. model, under which individuals are entitled to a minimum of $1,000 in damages, as well as legal fees, for intentional or willful government violations.[5] This approach provides individuals with meaningful redress in the case of egregious violations, thus creating a stronger incentive for individual enforcement and a correspondingly stronger incentive for government compliance.

4. Limit collection of personal data to that necessary for purposes

We strongly support the Privacy Commissioner's call for a legislated "necessity" test, requiring government institutions to demonstrate the need for all personal information that they collect. The current test of "relating directly to an operating program or activity" is a remarkably low standard - Treasury Board policy implicitly acknowledges this by applying a "necessity" criterion to government data collection. But this is too basic a requirement to leave to policy. Federal government agencies should be subject to the same standard regarding data collection as are private organizations and most provincial governments.

Amend s.4 of the *Act* to require that "No personal information shall be collected by a government institution unless it relates directly to *and is necessary for* an operating program or activity of the institution".

5. Protect unrecorded personal information

We also support the call to amend the definition of "personal information" so that it covers DNA and other biological samples, as well as video surveillance that does not involve recording. Public and private video surveillance for purposes of crime prevention/detection, border control, and employee monitoring is becoming increasingly common in Canada, and raises serious privacy issues. Such practices should be covered

[5] *Privacy Act of 1974*, Public law No. 93-579, 88 Stat.1897, 5 U.S.C. § 552a (g).

by the *Privacy Act*, as they are by other private sector and public sector privacy legislation in Canada. Given the potential for undesirable state surveillance using unrecorded data, the *Privacy Act* should cover all personal information, not just that which is "recorded".

Amend the definition of "personal information" in s.3 of the Act to delete the phrase "*that is recorded in any form*".

6. Require Privacy Impact Assessments

The need for privacy impact assessments of proposals for government programs or services is well-recognized and reflected in Treasury Board policy. Private sector data protection relies (in part) on individual consent. In contrast, public sector data protection, relies primarily upon institutional analysis of privacy impacts and decision-making in the public interest, backed up by an effective regime of transparency and accountability. In a context in which individuals have no choice but to provide their data to the government, PIAs are thus a critical component of privacy protection. They should be at the heart of the legislative regime, not left to unlegislated policy.

Indeed, reports from the Privacy Commissioner indicate that despite Treasury Board policy, many privacy impact assessments are completed only after the program has been implemented, if at all. Legislating a requirement for PIAs (and the public reporting of such) would give this essential feature of public sector privacy protection some teeth, presumably leading to greater compliance.

Adopt a new provision requiring Privacy Impact Assessments of new programs and services prior to implementation.

7. Security standards and breach notification

A number of serious data security breaches have made the news in recent months. Many of these involved government agencies that failed to take appropriate precautions to protect sensitive personal data from unauthorized access.

In contrast to PIPEDA and provincial privacy laws, the *Privacy Act* places no explicit obligation on the government to ensure that personal data is protected by reasonable security measures. Nor does the Act require government agencies to notify individuals of security breaches exposing their personal data to potential fraudulent use. Yet, this committee recommended that such a provision be added to PIPEDA, and Industry Canada is currently working with stakeholders in the private sector to develop such a legislative amendment.

As with so many features of the current regime, these key features of data protection are left to Treasury Board policy. While the specific implementation of legislative

requirements is an appropriate subject for policy guidelines, we submit that **basic obligations such as maintaining reasonable security of personal data and notifying individuals of breaches affecting them should be legislated** (as is done in other jurisdictions) both to give them added weight and authority, and to provide the basis for individual redress.

> **A new provision should be enacted requiring that government bodies:**
> **(a) take reasonable security measures to protect personal data from unauthorized access, use or disclosure; and**
> **(b) notify affected individuals of security breaches exposing their data to potentially harmful uses.**

8. Limit online disclosure of personal information

CIPPIC has received complaints about federal government agencies and administrative tribunals posting personal contact information and other sensitive information about individuals online, where the individuals participated in a public proceeding, or lodged formal complaints or appeals with the tribunal. The agencies in question posted the information in the interests of transparency and accountability, and in accordance with pre-internet policies of making such information publicly available. However, posting information on the world wide web amounts to a completely different level of public availability – one in which personal privacy is sacrificed to an unnecessary degree.

Subsection 69(2) of the Act allows for use and disclosure of "publicly available" information. Yet the term "publicly available" is not defined. We agree with the Privacy Commissioner that this exception "should not be interpreted so broadly as to throw all privacy considerations out the window merely because someone somewhere might be [entitled] to access the material".[6] Similarly, "consistent uses" should not permit the online publication of personal data without consideration of alternative, less privacy invasive means of achieving policy goals. The Act should allow for public disclosure of personal information in public registries, tribunal proceedings and decisions only in ways that accomplish the goals of openness and accountability without unduly violating individual privacy.

END OF DOCUMENT

[6] June 2006 report, Part V (F).