HOUSE OF COMMONS
CANADA

THE *PRIVACY ACT:* FIRST STEPS TOWARDS RENEWAL

Report of the Standing Committee on Access to Information, Privacy and Ethics

Paul Szabo, MP
Chair

JUNE 2009

40th PARLIAMENT, 2nd SESSION

Also available on the Parliament of Canada Web Site: http://www.parl.gc.ca

Additional copies may be obtained from Publishing and Depository Services
Public Works and Government Services Canada
Ottawa, Ontario K1A 0S5
Telephone: 613-941-5995 or 1-800-635-7943
Fax: 613-954-5779 or 1-800-565-7757
publications@tpsgc-pwgsc.gc.ca
http://publications.gc.ca

THE *PRIVACY ACT:*
FIRST STEPS TOWARDS RENEWAL

Report of the Standing Committee on Access to Information, Privacy and Ethics

Paul Szabo, MP
Chair

JUNE 2009

40th PARLIAMENT, 2nd SESSION

STANDING COMMITTEE ON
ACCESS TO INFORMATION, PRIVACY AND ETHICS

Russ Hiebert
Conservative
Vice-Chair

Paul Szabo
Liberal
Chair

Bill Siksay
New Democratic Party
Vice-Chair

Kelly Block
Conservative

Bob Dechert
Conservative

Earl Dreeshen
Conservative

Carole Freeman
Bloc Québécois

Pierre Poilievre
Conservative

Michelle Simson
Liberal

Ève-Marie Thaï Thi Lac
Bloc Québécois

Borys Wrzesnewskyj
Liberal

STANDING COMMITTEE ON ACCESS TO INFORMATION, PRIVACY AND ETHICS

CHAIR

Paul Szabo

VICE-CHAIRS

Russ Hiebert

Bill Siksay

MEMBERS

Kelly Block

Earl Dreeshen

Pierre Poilievre

Ève-Mary Thaï Thi Lac

Bob Dechert

Carole Freeman

Michelle Simson

Borys Wrzesnewskyj

OTHER MEMBERS OF PARLIAMENT WHO PARTICIPATED

Dave Batters

Charles Hubbard

Pat Martin

Glen Douglas Pearson

Mike Wallace

Sukh Dhaliwal

Carole Lavallée

Richard Nadeau

Dave Van Kesteren

CLERK OF THE COMMITTEE

Jacques Maziade

LIBRARY OF PARLIAMENT

Parliamentary Information and Research Service

Élise Hurtubise-Loranger

Alysia Davies

THE STANDING COMMITTEE ON ACCESS TO INFORMATION, PRIVACY AND ETHICS

has the honour to present its

TENTH REPORT

Pursuant to its mandate under Standing Order 108(2), the Committee has studied the subject of *Privacy Act* reform and has agreed to report the following:

CHAIR'S FOREWORD

As Chair of the Standing Committee on Access to Information, Privacy and Ethics, I want to thank the permanent members of the Committee and the other Members of Parliament who participated in the hearings for their support and efforts in discharging our collective responsibilities.

As well, no Parliamentary Committee can function properly without the experience, expertise and support of House of Commons and Library of Parliament personnel. Our clerk, research analysts, translators and other technical and support personnel were invaluable in helping us to organize our hearings. I am extremely grateful for their efforts related to this important study.

Respectfully submitted,

Paul Szabo, MP
Chair

INTRODUCTION

Classically understood as the "right to be left alone," privacy in this age of rapidly advancing informational technologies, globalization and heightened security concerns has come a long way since the federal *Privacy Act* (R.S.C. 1985, c. P-21) was enacted in 1983.

At that time, concerns about the protection of personal information essentially arose because computers had emerged as important tools for government and big business. In response to a federal government task force report on privacy and computers,[1] Canada enacted the first federal public sector privacy protection in Part IV of the *Canadian Human Rights Act* in 1977, which established the office of the Privacy Commissioner of Canada as a member of the Canadian Human Rights Commission, and provided it with a mandate to receive complaints from the general public, conduct investigations and make recommendations to Parliament. Arguably, the anti-discrimination provisions of the *Canadian Human Rights Act* were not the best fit for the right to privacy, and in 1983, the current *Privacy Act* came into force and has largely remained unaltered since then.

Thus, while privacy experts may now equate the right to privacy with a range of values such as the right to enjoy private space, to conduct private communications, to be free from surveillance and to have the sanctity of one's body respected, privacy protection in Canada essentially focuses on safeguarding personal information.

Much has changed since the *Privacy Act* first came into force. Indeed, having studied second generation privacy laws in its review of the *Personal Information Protection and Electronic Documents Act* (PIPEDA),[2] which was passed in 2000 to protect personal information held by the private sector, the House of Commons Standing Committee on Access to Information, Privacy and Ethics (the Committee) recognizes that the *Privacy Act* is a "first generation" approach to privacy protection. The Committee is also aware that calls for reform of the Act date as far back as 1987 when the House of Commons Standing Committee on Justice and the Solicitor General made more than 100 unanimous recommendations for improving the legislation in its report, *Open and Shut: Enhancing the Right to Know and the Right to Privacy*.[3] The House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities also recommended in 1997 that the *Privacy Act* be broadened and strengthened in relation to all issues of privacy within the federal sector.[4]

---

[1] Department of Communications and Department of Justice, *Privacy and Computers: A Report of a Task Force*, Information Canada, Ottawa, 1972.

[2] *Statutory Review of the Personal Information Protection and Electronic Documents Act* (PIPEDA), 4th Report of the Standing Committee on Access to Information, Privacy and Ethics, May 2007.

[3] House of Commons, Standing Committee on Justice and Solicitor General, *Open and Shut: Enhancing the Right to Know and the Right to Privacy: Report of the Standing Committee on Justice and Solicitor General on the Review of the Access to Information Act and the Privacy Act*, 1987.

[4] *Privacy: Where Do We Draw the Line?*, report of the House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities, April 1997.

With this background in mind, the Committee embarked on its own study of possible reforms to the *Privacy Act.* From April 17, 2008 to June 3, 2008, it heard from the Privacy Commissioner of Canada and from ten additional witnesses. The Privacy Commissioner, who was the first to appear, presented a series of 10 proposed reforms, or, as they came to be known by the Committee, 10 "quick fixes" for the *Privacy Act*. On May 11, 2009, the Commissioner appeared again before the Committee and updated the list of quick fixes by adding two more reform proposals, based on the testimony of some previous witnesses, for a final total of twelve.

While the majority of witnesses responded to the Commissioner's initiative and provided comments on the proposed reforms, not all of the witnesses addressed them. Officials from various federal government departments were given the opportunity to provide comments on the reform proposals, both before the Committee and afterwards, but only some of them have provided responses.

Accordingly, the Committee has gone ahead to consider the proposed reforms on the basis of the comments it does have. The Committee is aware that much work needs to be done, and a complete overhaul of the *Act* is in fact warranted. However, the Commissioner's proposed "quick fixes" present an opportunity for a strong first step in the process of reform.

OVERVIEW OF THE *PRIVACY ACT*

The *Privacy Act* came into force, on 1 July 1983, at the same time as the *Access to Information Act*. The *Privacy Act* is a data protection law, once described as an "information handler's code of ethics." Its basic premise is that individuals should, to greatest extent possible, be able to have control over what is known about them and by whom.

The *Act* has three basic components: (1) it grants individuals the legal right of access to personal information held about them by the federal government; (2) it imposes fair information obligations on the federal government in terms of how it collects, maintains, uses and discloses personal information under its control; and (3) it puts in place an independent ombudsman, the Privacy Commissioner,[5] to resolve problems and oversee compliance with the legislation. The *Privacy Act* applies only to those federal government departments and agencies set out in Schedule 1 to the Act, a list which was recently expanded under the *Federal Accountability Act* in 2006.

Personal information under the Act includes any information about an identifiable individual, recorded in any form (i.e., video or audiotape, or any electronic information medium), including information about one's age, education, medical or criminal or employment history (e.g., tax records, student loan applications).

[5] The Privacy Commissioner is an Officer of Parliament who is appointed by Governor in Council for a maximum of seven years.

The Act stipulates that no personal information shall be collected by a government institution unless it relates directly to an operating program or activity of the institution. As well, wherever possible, the information should be collected directly from the individual to whom it relates and the individual should be informed of the purpose for which it is being collected. In the interests of transparency and openness, government institutions are required to publish indexes indicating all of the personal information banks maintained by them, which are collected by the Treasury Board and published on-line in the form of four searchable reference tools known collectively as *Info Source*.[6] The Treasury Board Secretariat has the lead role in administering the legislation, a responsibility which is partially shared with the Department of Justice.

Everyone in Canada has the right to apply for access to personal information about themselves that is held by the federal government. If an individual is not satisfied with the accuracy of the information obtained, he or she may seek to have the inaccuracies corrected. If such a request is refused, the applicant may require that a notation be attached to the information describing any corrections requested but not made.

The Act provides a number of exemptions that may be used by a government institution to prevent an applicant from having access to part or all of his or her personal information held by the institution. If an applicant is not satisfied with the action of a government institution, a complaint can be made to the Privacy Commissioner. When this recourse is unsuccessful, an application can be made to the Federal Court.

In addition to investigating complaints about the operation of the *Privacy Act*, the Privacy Commissioner can conduct audits of the fair information practices of government institutions and carry out special studies referred to the Commissioner by the Minister of Justice.

THE QUICK FIXES

The Committee's study began with two appearances by the Privacy Commissioner, during which she presented her proposed "quick fixes" for the *Privacy Act*.[7] The Commissioner testified that she considered these to be the most important and necessary reforms to the *Act* that could be easily implemented in the short term, however, she emphasized that these proposed quick fixes in no way eliminated the need for a comprehensive review of the *Act*.

The Commissioner told the Committee that she believed these immediate changes would at least be a start in modernizing the *Act*:

> I'd like to remind the members that we have no pretensions that this is the definitive take on the Privacy Act, nor on the problems of Canadians' information

[6] http://www.tbs-sct.gc.ca/atip-aiprp/is/is-eng.asp

[7] Office of the Privacy Commissioner of Canada, *Proposed Immediate Changes to the Privacy Act: Appearance before the Standing Committee on Access to Information, Privacy and Ethics*, April 29, 2008, http://www.privcom.gc.ca/legislation/pa/pa_reform_e.asp

> rights. This is a very contextual document. It's meant to suggest some very needed and more easily made changes to a document that now dates from 1982. Throughout the world, it is one of the few information rights laws that has not been modified. So in the group of democratic nations--for example, the U.K., Australia, and so on--we find that our public Privacy Act is now very dated.[8]

The Privacy Commissioner listed several other reasons for seeking reform of the legislation as well, including the need to ensure that the responsibilities imposed on the public sector in the *Privacy Act* are at least as strong as those imposed on the private sector by the more recently enacted *Personal Information Protection and Electronic Documents Act* (PIPEDA):

> The government is not subjecting itself to the standards it imposes on Canadian corporations or the rights it gives Canadian consumers in relation to Canadian corporations or the rights it gives to complainants to our office, who do not like the way they've been treated by Canadian commercial organizations, to take their problems further…I think there's a real issue of equity. There's an issue of modernization. There's an issue, in a society that values something as important as this, of making sure the rights are defined in a way that makes them practically applicable today.[9]

Quick Fix # 1: Create a legislative "necessity test" which would require government institutions to demonstrate the need for the personal information they collect.

The Commissioner testified that it is now common in modern privacy legislation to require that the collection of information be reasonable and necessary for the relevant program and activity. The current wording of the *Act*, in section 4, contains only a broad statement that no information shall be collected by a federal institution unless "it relates directly to an operating program or activity of the institution."

The Commissioner referred to Treasury Board policies that make the stronger statement that there must be a demonstrable need for each piece of personal information collected. She also noted that the federal legislation governing the private sector, the *Personal Information Protection and Electronic Documents Act* (PIPEDA), and even the *Canadian Security Intelligence Service Act* which governs CSIS, contain more narrowly worded restrictions on collection.

The Commissioner noted as well that almost all provinces and the territories, which each have their own public sector legislation concerning privacy, have adopted a model which sets three conditions, including a necessity test:

(i) the collection is expressly authorized by statute;
(ii) the information is collected for the purpose of law enforcement; or
(iii) the information relates directly to and is necessary for an operating program or activity.

[8] Testimony of the Privacy Commissioner to the Committee, April 29, 2008 at 1615.
[9] Testimony of the Privacy Commissioner to the Committee, April 17, 2008 at 1640.

The Commissioner concluded that introducing a necessity test at the federal level would strengthen legislative controls around the collection of personal information and give effect to the fundamental right to privacy that has been recognized by the Supreme Court under the *Canadian Charter of Rights and Freedoms.*

The Canadian Internet Policy and Public Interest Clinic (CIPPIC), former Québec Access to Information Commission President Paul André Comeau, Professor Michael Geist, and the Canadian Bar Association all supported this proposed "quick fix". The Canadian Bar Association noted the importance of a necessity test in terms of the protection of personal information:

> An important additional maxim that's been developed with respect to best practices for the collection, use, and disclosure of personal information since 1982 is something called the "necessity test". Simply put, it's to collect only that information that is reasonably necessary, which safeguards against the natural tendency, or what appears to be a natural tendency, to collect more information than is required, which then of course requires that it be safeguarded. And if it's collected and is not necessary, it increases the likelihood that information can be misused.[10]

The Canadian Bar Association elaborated further on the need for a necessity test in the public sector context, which unlike the private sector context, does not use a consent model:

> On the philosophy or the difference…When you're dealing with a bank or dealing with your local video store, you have the opportunity to go elsewhere, so consent is really the bedrock of it. It's about informed consent, and that links to principle two and principle three within PIPEDA.
>
> A citizen does not have a voluntary relationship with the government. Perhaps when it comes to certain services and whether the individual chooses to take advantage of those particular services, there is a bit of the voluntary, but a citizen's relationship with Revenue Canada, the employment insurance commission, or other departments is not voluntary whatsoever. The individual has an obligation. One can't necessarily ask for consent.[11]

David Flaherty, a former Information and Privacy Commissioner of British Columbia, went further, and stated he saw no reason why a consent requirement for the public sector could not be implemented along the same lines as that used in the private sector. He placed this suggestion in the context of the general principles which inform most privacy

[10] Testimony of Gregory DelBigio and David Fraser, Canadian Bar Association, to the Committee, June 3, 2008 at 1605.
[11] Testimony of Gregory DelBigio and David Fraser, Canadian Bar Association, to the Committee, June 3, 2008 at 1620.

legislation models[12] – for example, openness about what is done with personal information; accountability for its handling; having a purpose for its collection; limiting its collection, use and disclosure; getting consent; having adequate security; and ensuring the right to see one's own personal information holdings and complain if necessary.

However, the Minister of Justice, in his appearance before the Committee, took the position that the current section 4 of the *Act*, as outlined above, already contains a necessity test. The RCMP also did not agree with a new test for collection being introduced into the legislation, expressing concerns that the Commissioner's proposed reforms would have a significant impact on the efficiency of its investigative work with respect to national security, transnational organized crime and sexual assaults against children.

CSIS testified that it already has its own necessity test under section 12 of the *Canadian Security Intelligence Service Act*. This test is applied in the context of what CSIS described as a broad mandate: "reason to suspect an activity". At one point during the testimony, a Member of the Committee made a statement to clarify this mandate, which elicited no disagreement from either of the relevant witnesses: while the RCMP investigates on the basis of evidence, it is the job of CSIS to investigate on the basis of suspicion.

Committee Response: *The Committee discussed whether section 4 of the Privacy Act is robust enough in its current form to give full effect to the rights underpinning the Act, but there were varying opinions on this issue. The Minister may wish to give it further study and consideration.*

Quick Fix #2: Broaden the grounds for which an application for Federal Court review under section 41 of the *Privacy Act* may be made to include the full array of privacy rights and protections under the *Privacy Act* and give the Federal Court the power to award damages against offending institutions.

Under the current *Act*, the grounds of review by the Federal Court, as set out in sections 41 and 42, are limited to complaints concerning denial of access to one's own personal information. While the Commissioner can investigate any other matter under the *Act*, these types of investigations can result in recommendations only, and further remedies cannot be sought by way of the courts.[13] Section 41 of the current *Act*, the key provision concerning access to the courts, reads as follows:

[12] In Canada, these are encapsulated in the *Model Code for the Protection of Personal Information* created by the Canadian Standards Association and based on other international models of this type. They were also used as a basis for the federal legislation governing the private sector, the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and incorporated into Schedule 1 of that legislation.
[13] The Federal Court confirmed this interpretation of the *Act* in *Murdoch v. Canada (Royal Canadian Mounted Police)*, [2005] 4 F.C.R. 340.

Review by Federal Court where access refused

41. Any individual who has been refused access to personal information requested under subsection 12(1) may, if a complaint has been made to the Privacy Commissioner in respect of the refusal, apply to the Court for a review of the matter within forty-five days after the time the results of an investigation of the complaint by the Privacy Commissioner are reported to the complainant under subsection 35(2) or within such further time as the Court may, either before or after the expiration of those forty-five days, fix or allow.[14]

The Commissioner proposes that all rights provided by the *Act* be supported by remedies, thus introducing enforceable accountability throughout the legislation. She submitted that this "quick fix" would also provide the added benefit of possible judicial interpretation of some aspects of the *Act* which have caused confusion in the past, such as when collection, use or disclosure of personal information is inappropriate. The Commissioner described the full rationale for this recommendation in her proposal as follows:

> **Giving Effect to the Fundamental and Quasi-Constitutional Status of Privacy Rights**
> Broadening Federal Court review would confirm that privacy rights in the public sector and the private sector are equally important, ensure that government institutions respect every Canadian's right to have their personal information collected, used and disclosed in accordance with the *Privacy Act* and give full weight to the privacy rights of individuals in a free and democratic society. The Supreme Court of Canada has confirmed that the purpose of the *Privacy Act* is to protect the privacy of individuals with respect to personal information about themselves held by a government institution, this purpose being of such importance to warrant characterizing the *Privacy Act* as "quasi-constitutional" because of the role privacy plays in the preservation of a free and democratic society.
>
> **Keeping Government Accountability Through a Meaningful Review Mechanism**
> Implementing our recommendation would give Canadians the same rights regarding their personal information collected, used or disclosed by their own government institutions that they hold vis-à-vis private-sector organizations exercising commercial activities under *PIPEDA*. Government institutions should be even more open and accountable with respect to their personal information handling practices, and increasing government accountability clearly requires strengthened privacy rights when it comes to how government handles the personal information of Canadians. Our recommendation is essential to achieving meaningful government accountability and transparency.
>
> **Directly Protecting Privacy Rights Through the Intended Legislation**
> The Supreme Court of Canada has held that a third-party to an access to information request made under the *ATI Act* can apply to the Federal Court for a hearing in respect of a government institution's disclosure of personal information.[4] Given that the Supreme Court of Canada has held that the right to privacy is paramount over the right of access to information, how can it be that a third-party can appear before the Federal Court with respect to the disclosure of another person's personal information under the *ATI Act*, but that an individual cannot even seek enforcement and a remedy for a violation of the

[14] *Privacy Act*, R.S., 1985, c. P-21, s. 41.

fundamental right of privacy under the *Privacy Act* vis-à-vis his or her own personal information? Broadening Federal Court review under the *Privacy Act* would address this unintended consequence.

There is No Right Without a Remedy
Every right needs a remedy in order to have meaning. This is especially so with respect to a fundamental right such as privacy. Implementing our recommendation would ensure that the Federal Court can review the full array of fundamental rights and protections under the *Privacy Act*, including inappropriate collection, use or disclosure of personal information, failure to maintain up-to-date and accurate data, improper retention or disposal, and denials of access or correction by government institutions. It would also ensure that the Federal Court may award damages in cases where, for example, the inappropriate use or disclosure of personal information causes embarrassment or other harms to the individual concerned.

The Need for Court Guidance
Implementing our recommendation would allow the Federal Court to provide needed guidance on what constitutes inappropriate collection, use or disclosure of personal information.[15]

This recommendation was supported by CIPPIC, David Flaherty, Paul André Comeau, Professor Michael Geist, and the Canadian Bar Association (CBA). The CBA in particular testified that widening remedial access to the courts under the *Act* to relate to all matters it deals with, rather than just denial of access, would augment government accountability in matters for which there is currently no enforceable recourse. The representatives of the CBA described accountability as the "touchstone" of the reform recommendations.

The RCMP indicated that while it did not directly oppose this second "quick fix", it had concerns that it would change the entire "spirit" of the *Act*.[16] As well, the Minister of Justice expressed concern about additional pressure on court resources, and speculated as to whether this proposal might conflict with another quick fix proposed by the Commissioner, providing her with the discretion to refuse to investigate repetitive or frivolous complaints (see number 6 below). The Minister stated:

> One of the suggestions would expand the role of the Federal Court to allow complaints under the Privacy Act. There would be an award of damages against offending institutions, presumably government. I'll be very interested to hear what you have to say about it, quite frankly, and I suppose you might want to have a look at that in conjunction with recommendation number 6, which would give power to the Privacy Commissioner to rule out some complaints that may not be in the public interest or that she thinks are vexatious or frivolous. To me, that is a bit of a challenge. You might have an issue that is of extreme importance to one

[15] Office of the Privacy Commissioner of Canada, *Proposed Immediate Changes to the Privacy Act: Appearance before the Standing Committee on Access to Information, Privacy and Ethics*, April 29, 2008, pp. 10-11, http://www.privcom.gc.ca/legislation/pa/pa_reform_e.asp
[16] Testimony of Chief Superintendent Bob Paulson, Acting Assistant Commissioner of the RCMP, to the Committee, May 13, 2008 at 1645.

particular individual, but it may have very few public policy ramifications. I'll be interested in hearing what you have to say on that one.

On the other hand, in recommendation number 2, you're giving a right to appeal to the Federal Court. It seems to me there has to be some squaring of that box. I don't know how you can dismiss some of them and then say there should always be a right to appeal to the Federal Court. Again, I'm very interested in what has been recommended, but I'll be very interested to hear what you have to say.[17]

[…]

If there is an automatic right of appeal to the Federal Court, there will certainly be court costs involved. And it depends on whether you expand the role and to what extent you recommend expanding the role of the Privacy Commissioner. Most of these things cost money. Any time you expand the role of any individual, it requires resources. I'll see when the recommendations are made.

What I indicated to you in my opening remarks was to just keep that in mind. These things aren't without costs, and our courts are very busy, for instance. There would be a cost, of course. But it may be your recommendation to allow these appeals to the Federal Court.[18]

[…]

I did have some questions with respect to a possible conflict, but I would be very interested to hear what you have to say between recommendations 2 and 6. On the one hand, if the Privacy Commissioner can dismiss or not pursue one, and then at the same time we're also giving them a right to appeal to the Federal Court, there may be a conflict there. Maybe not, but again I would be very interested.[19]

[…]

I was hoping to see, and in the first round of questions I pointed out that I'd like to see, more analysis of the relationship between recommendations number 2 and number 6. That's my own opinion. You may conclude that there's no problem, that they can both coexist, but it seemed to me, when I had a look at these initially—and I've thought about it since—there might be some challenges. I'll be interested to hear what you have to say.[20]

---

[17] Testimony of the Honourable Rob Nicholson, Minister of Justice and Attorney General, to the Committee, May 27, 2008 at 1545.
[18] Testimony of the Honourable Rob Nicholson, Minister of Justice and Attorney General, to the Committee, May 27, 2008 at 1545.
[19] Testimony of the Honourable Rob Nicholson, Minister of Justice and Attorney General, to the Committee, May 27, 2008 at 1600.
[20] Testimony of the Honourable Rob Nicholson, Minister of Justice and Attorney General, to the Committee, May 27, 2008 at 1615.

Committee Response: *The Committee discussed section 41 and whether access to the courts under it should be broadened by means of proposing amendments. It also discussed the relationship between this recommendation and recommendation #6, the proposal to give the Commissioner the discretion to refuse to investigate frivolous or vexatious complaints. The Committee recognizes the varying viewpoints of all who testified on this issue, and would suggest that the Minister give it further study and consideration. Discussion between the Minister and the Commissioner may help to determine whether these proposals should move forward, or be modified.*

Quick Fix #3: Enshrine a requirement for heads of government institutions subject to the *Privacy Act* to assess the privacy impact of programs or systems prior to their implementation and to publicly report assessment results.

The Privacy Commissioner testified that the Treasury Board introduced a policy in May 2002 requiring privacy impact assessments (PIAs) to be performed on any federal government proposals for programs and services that may raise privacy issues. The Treasury Board confirmed to this Committee that this policy was part of a suite of policies related to privacy and security, which are currently being consolidated and updated.

The Commissioner submitted that the implementation of the PIA policy across all federal government institutions had been "uneven", and she therefore proposed that this requirement be enshrined in law through the *Act.* The Commissioner's view was that making the PIAs mandatory would ensure that they were completed for all programs and services on a consistent and timely basis, and would promote transparency within government.

This proposal was supported by CIPPIC, David Flaherty, Paul André Comeau, Professor Michael Geist, and the Canadian Bar Association. The Director of CIPPIC noted that PIAs can help to ensure that, in the absence of a consent rule for the collection and use of personal information in the public sector, an equivalent standard is applied:

> We don't have the consent rule in the public sector. Instead we rely on the federal government to undertake analysis of privacy impacts in the public interest and to ultimately make decisions in the public interest. Of course, we rely on transparency and accountability mechanisms as well to back that up. But privacy impact assessments are critical; they are, in effect, replacing the consent requirement we have in the private sphere and they should be legislated. They should not be left to a matter of policy.[21]

David Flaherty testified that he believes government institutions should be consulting with the Privacy Commissioner on matters such as PIAs earlier in the process of their development than is currently occurring. He stated that he thinks a "privacy risk management" approach similar to the one used in the private sector should be taken,

[21] Testimony of Philippa Lawson, Director of CIPPIC, to the Committee, May 6, 2008 at 1540.

which would include the appointment of chief privacy officers, mandatory PIAs, and improved privacy training for public servants. He also testified in favour of having strengthened rules for the destruction of personal information once it is no longer required. He added that the assessment of privacy risk cannot be done in a vacuum:

> I want the financial risk management, labour relations risk management, and even resources risk management to put on their risk management hats when they think about privacy. And there *[sic]* the risks are that data goes missing, that data is used for unintended purposes that it's not supposed to be used for, that it's used to harm individuals, or it's stolen, or it's used to invade their privacy by people who are browsing databases, or it's sold to criminal elements.[22]

Mr. Flaherty summed up the nature of a PIA this way:

> The PIA is the story of a database. Why does it exist? What are its purposes? Why do you need this in the first place? Is it rational? What personal information do you collect? What personal information do you disclose? Do you get consent? What security provisions do you have in place?[23]

Paul André Comeau stated that Treasury Board has in many instances provided detailed guidelines for privacy procedures and technological security standards, and that making some of these practices mandatory would be easier because those procedures already exist and are developed. He noted that departments which have followed these guidelines from the beginning may be in a better position, and cited the example of a Quebec department whose upgrade to retroactively engineer increased privacy into its information technology systems ended up costing more than the original system implementation. He also noted that making PIAs mandatory would ensure that they are completed properly and that the necessary amount of resources are allocated to them in all institutions.

The Minister of Justice did not testify specifically about this recommendation, but indicated that Treasury Board policies are already in place to ensure PIAs are carried out throughout the government. The Minister also noted in his general testimony that there might be considerable cost implications to implementing the Privacy Commissioner's recommendations, and that many of them already exist in the form of policies, which in his view have the advantage of being more flexible than law.

The Commissioner's proposed "fix" was not supported by the RCMP, which testified that it already completes PIAs under all the existing policies and therefore feels including them in the law is unnecessary.

Committee Response: *The Committee discussed this recommendation and while it is sympathetic to the concerns raised by the Commissioner, does not consider this proposal to be a top priority for reform at this time.*

---

[22] Testimony of David Flaherty to the Committee, May 8, 2008 at 1710.
[23] Testimony of David Flaherty to the Committee, May 8, 2008 at 1615.

Quick Fix #4: **Amend the *Privacy Act* to provide the Office of the Privacy Commissioner of Canada with a clear public education mandate.**

The Commissioner noted that PIPEDA, the private sector privacy legislation, provides the Commissioner with a mandate to raise public awareness about privacy issues relating to this sector. However, there is no comparable mandate provided in the *Privacy Act* for the public sector. The Commissioner stated to the Committee:

> When this act was drafted and implemented, no one ever thought that one of the Privacy Commissioner of Canada's most important roles—some would say the most important—was to provide the public with information on a broad scale concerning threats to their privacy, how to preserve their privacy and, increasingly, navigating in this technological world that is beyond the understanding of many.[24]

The Commissioner proposed that her Office be given clear legislative direction to engage in research, communication and public education on privacy rights with respect to federal institutions. The Commissioner was of the view that this would enable her to communicate more frequently and in a greater variety of ways with the public.

The Commissioner indicated that in addition to putting out her current annual reports under the *Act*, she would like to create a compendium of significant privacy cases for the public to consult, to issue periodic assessments of the privacy performance of selected federal government departments, to provide information to ATIP professionals within the government to supplement their training programs, and to raise awareness amongst the public in general about the *Act* in ways that would help ensure greater compliance and best practices. The Commissioner stated that her office would also like to expand its current Research Contributions Program, which provides funding to selected studies on privacy issues.

The Commissioner described the rationale for her recommendation as follows:

> **Rationale:**
> While the OPC's central function under the *Privacy Act* is the investigation and resolution of complaints, the OPC also needs to advance privacy rights by other means – through research, communication and public education. The Commissioner lacks the legislative mandate under the *Privacy Act* to educate the public about their informational privacy rights with respect to information held by federal government institutions. The Commissioner should be equally empowered to sensitize business, government and the public under the *Privacy Act*.
>
> **Case Summaries on Public Sector Personal Information Management**
> Currently, the main vehicle for reporting on cases is the Annual Report under the *Privacy Act*. However, with a more explicit public education mandate and more flexible means for public reporting, the OPC could publish a compendium of

[24] Testimony of the Privacy Commissioner to the Committee, April 29, 2008 at 1545.

significant cases that fall under the *Privacy Act*, notably in the areas of national security, law enforcement, and health. Several civil society groups with an interest in privacy promotion have urged the OPC to make more timely public reports on the state of governmental surveillance activities and how these activities may impact on privacy.

Periodic Assessments of Departmental Privacy Performance

The OPC wishes to foster a more informed public debate of the federal government's role in areas involving the sharing of personal information between agencies and jurisdictions. A clear public education authority would allow the OPC to publish public advisories and education material on significant policy and legislative measures with "personal information" components.

Support the Learning Objectives of Informational Rights Professionals

Surveys carried out by Treasury Board Canada indicate there are significant learning needs on the part of Access to Information and Privacy (ATIP) professionals, pointing to the increased number and complexity of cases, as well as to the number of new organizations being covered by the *Privacy Act* as a result of the adoption of the *Federal Accountability Act*. The surveys also reveal—corroborated by the OPC's own audit and review work—that learning needs are not being addressed by the current learning infrastructure. By making more information available in a more timely way, the OPC will become a valuable source of information on the need for a more consistent approach to privacy management across the federal government.

Broader Parameters for the OPC's Research Program

Better research into public sector personal information management is needed to inform public policy. Section 24 of *PIPEDA* allows the OPC to undertake and publish research that is related to the protection of personal information in the private sector, with a specific funding envelope. Under this education mandate, the OPC has put in place a comprehensive Research Contributions Program which has allocated over $1,000,000 to more than 30 privacy research initiatives in Canada, resulting in extensive studies on key privacy issues. These research papers are publicly available on the OPC website. A similar mandate should exist under the *Privacy Act* for research relating to public sector matters.

Benefits the Citizens and Residents of Canada

A clearer public education mandate for the OPC would allow for more extensive and better informed public dialogue on federal privacy management in areas of critical importance to the right to privacy. It would also ensure a more consistent approach to privacy compliance by addressing the learning needs of informational rights professionals.[25]

[25] Office of the Privacy Commissioner of Canada, *Proposed Immediate Changes to the Privacy Act: Appearance before the Standing Committee on Access to Information, Privacy and Ethics*, April 29, 2008, pp. 15-16, http://www.privcom.gc.ca/legislation/pa/pa_reform_e.asp

This proposal was supported by David Flaherty, Paul André Comeau, Professor Michael Geist, and the Canadian Bar Association. Professor Geist testified that providing the Commissioner with a broad mandate to educate was particularly important in an era of 24-hour news:

> Moreover, the notion of limiting reporting to an annual report I think clearly reflects a bygone era. We're in a 24-hour news cycle, and any restrictions on the ability to disseminate information, particularly information that might touch on the privacy of millions of Canadians, such that it remains out of the public eye until an annual report can be tabled, need to be reformed so there's power to disclose the information in a timely manner.[26]

CSIS also indicated that it would have no objection to this proposed amendment to the *Act.*

The Minister of Justice took the position that the Commissioner already has these powers implied throughout the *Act*. He stated in his testimony:

> With respect to the ten I had a look at, I think some of them are possible right now within the existing legislation. One of them is that the Privacy Commissioner take more of an educative function. It seems to me she could expand and go forward on that.[27]
>
> […]
>
> I said, for example, on one of the recommendations--I forget which one right now, but she talked about the education component of that. It seems to me you could probably do that without legislation. That was my point.[28]

Committee Response: *The Committee supports this recommendation and suggests that the Minister consider amending the Act accordingly.*

Quick Fix #5: **Provide greater discretion for the Office of the Privacy Commissioner of Canada to report publicly on the privacy management practices of government institutions.**

This "quick fix" deals with a specific aspect of the Commissioner's proposals to be able to report more information publicly outside the framework of the annual reports from her Office. The Commissioner described the role played by her Office in her submissions to the Committee as follows:

---

[26] Testimony of Professor Michael Geist to the Committee, May 15, 2008 at 1640.
[27] Testimony of the Honourable Rob Nicholson, Minister of Justice and Attorney General, to the Committee, May 27, 2008 at 1600.
[28] Testimony of the Honourable Rob Nicholson, Minister of Justice and Attorney General, to the Committee, May 27, 2008 at 1630.

> There is a public expectation that the OPC will investigate and report on matters of public interest. This is particularly so where the privacy issue is already in the public domain. The OPC has been hampered in its ability to speak with the press, with the public, and even with Members of Parliament, due to the existing confidentiality constraints in the *Privacy Act*. Furthermore, a public interest disclosure discretion would allow for more timely and relevant disclosure rather than having to wait until the end of the reporting year when the information may have become moot, stale or largely irrelevant.[29]

The Commissioner noted that she believes such a power would assist in educating the public about privacy issues, and helping to uphold public confidence in her Office. She also stated that it would be an important factor in encouraging compliance:

> For example, if I find a huge privacy problem in a department or an institution that runs a service that affects most Canadians, I would think it might be appropriate, in some circumstances, to inform Canadians about this right away, rather than to wait 18 months. It might also provide a greater incentive for the department to be privacy proactive.[30]

This proposal was supported by CIPPIC, David Flaherty, Paul André Comeau, Professor Michael Geist, and the Canadian Bar Association. CSIS also indicated that it would have no objection to this proposed amendment.

Committee Response: *The Committee would support the proposal that more frequent latitude be given to the Commissioner to report to Parliament, subsequent to which her findings could be discussed publicly. To the extent that the proposal would require legislative amendment to allow disclosure other than provided for under the Officer of Parliament model where reports must be tabled in Parliament first, the Committee would have concerns. The Committee also expressed concern about what would constitute a "matter of public interest" and how this would be determined.*

Quick Fix #6: **Provide discretion for the Privacy Commissioner to refuse and/or discontinue complaints the investigation of which would serve little or no useful purpose, and would not be in the public interest to pursue.**

The Commissioner stated that under section 29 of the current *Act*, she must receive and investigate all complaints without being able to distinguish or prioritize those which are serious, or to separate them from those that may be repetitive or initiated by complainants for frivolous reasons.

---

[29] Office of the Privacy Commissioner of Canada, *Proposed Immediate Changes to the Privacy Act: Appearance before the Standing Committee on Access to Information, Privacy and Ethics,* April 29, 2008, p. 17, http://www.privcom.gc.ca/legislation/pa/pa_reform_e.asp

[30] Testimony of the Privacy Commissioner to the Committee, April 29, 2008 at 1650.

The Commissioner testified that this first-come-first-served approach has resulted in a persistent backlog of complaint cases in her Office, which cannot be solved by additional resources alone. It has also taken time away from the Office's ability to focus on what she described as the "more systemic and pervasive threats to privacy" that are currently developing.

The Commissioner described five areas where she might use the discretion to refuse to investigate a complaint if it were granted to her:

1. repetitive issues that come up and have already been clearly decided in past cases (e.g. legitimate collection and use of Social Insurance Numbers);
2. moot time complaints where the individual has since received the information requested (e.g. where access was already provided, though technically out of time and at no disadvantage to the individual);
3. frequent complaints brought forward by the same individual who has an obvious "axe to grind" against a government institution (e.g. where contentious labour or employment issues constitute the real dispute between the parties which could be more effectively dealt with through other, more appropriate procedures);
4. multiple complaints brought by many individuals in respect of the same incident (e.g. a data breach involving personal information of many individuals which is already well documented and need not be re-investigated only to confirm what is already known);
5. issues that have already been recognized and addressed by the government institution (e.g. effective remedial action has already been taken).

The Commissioner noted that this power is given to Commissioners in provinces such as Alberta and British Columbia, and that in her view it would help her Office to make more effective use of its resources.

This proposal was supported by David Flaherty, himself a former provincial commissioner, and the Canadian Bar Association. CIPPIC did not support this proposal, citing concerns about equal access rights for all comers. Paul André Comeau, another former head of a provincial commission, gave the alternative proposal of providing the Commissioner with special powers to expedite certain kinds of complaints in the above categories instead.

This "quick fix" was questioned by the Minister of Justice as being in possible conflict with the proposal to broaden the Federal Court's powers with respect to the *Privacy Act* (see recommendation #2 above).

Committee Response: *The Committee discussed this recommendation, and noted that the Minister's testimony had linked it with the second recommendation above concerning broadening the Court's powers with respect to the Privacy Act. The Committee recognizes the varying viewpoints of all who testified on this issue, and would suggest that the Minister give it further study and consideration. Discussion between the Minister*

and the Commissioner may help to determine whether these proposals should move forward, or be modified.

Quick Fix #7: **Amend the *Privacy Act* to align it with the *Personal Information Protection and Electronic Documents Act* (PIPEDA) by eliminating the restriction that the *Privacy Act* applies to recorded information only.**

The Commissioner explained to the Committee that section 3 of the current *Privacy Act* restricts its application to any information collected by the federal government in "recorded" form. The Commissioner pointed out that many forms of new information collection that have been facilitated by developing technologies do not meet this description, including live feeds of surveillance footage from cameras and DNA swab information collected from individuals, for example. The Commissioner proposed amending the *Act* to eliminate the restriction.

This "quick fix" was supported by David Flaherty, Paul André Comeau, Professor Michael Geist, and the Canadian Bar Association. Professor Geist noted the effect of developing technologies in creating a situation where all institutions are collecting more data, and different kinds of data, than they were previously able to collect, and noted that it is important to keep the law current in a situation where potential collection and future uses cannot be fully anticipated.

The Canadian Bar Association observed during its general testimony that the current *Act* was put in place before the development of technologies for data matching, biometrics, genetic information, the decoding of the human genome, portable electronics, surveillance, video surveillance, and GPS.

The RCMP did not support this proposed quick fix. It stated that this would be "unnecessary" and "a complete departure from the spirit of the existing act."[31] The RCMP added that it had concerns with respect to the legitimate criminal video surveillance and physical surveillance of subjects, and believed that the existing DNA legislative framework was capable of balancing privacy concerns.

Committee Response: *The Committee supports this recommendation and suggests that the Minister consider amending the Act accordingly.*

Quick Fix #8: **Strengthen the annual reporting requirements of government departments and agencies under section 72 of the *Privacy Act,* by requiring these institutions to report to Parliament on a broader spectrum of privacy-related activities.**

[31] Testimony of Chief Superintendent Bob Paulson, Acting Assistant Commissioner of the RCMP, to the Committee, May 13, 2008 at 1645.

Under section 72 of the *Privacy Act*, the heads of federal government institutions are each required to submit an annual report to Parliament on their administration of the *Act*, provided their institution falls under it. The Treasury Board introduced privacy reporting guidelines for these institutions in 2005, which additionally require deputy heads to report on matters related to privacy protection and promotion within their institutions. These guidelines were updated in 2008.

The Commissioner testified that the information actually provided under section 72 is not particularly comprehensive, and generally consists of statistics pertaining to the number of requests received under the *Privacy Act*, the dispositions taken on completed requests, the exemptions invoked or exclusions cited, and completion times.

The Commissioner proposed that section 72 of the *Act* be amended to incorporate the updated Treasury Board guidelines and to make them mandatory for all federal institutions. This would enshrine the following reporting requirements in the law:

- a description of each PIA completed during the reporting period;
- an indication of the number of new data matching and data sharing activities undertaken;
- a description of privacy-related education and training activities initiated;
- a summary of significant changes to organizational structure, programs, operations, or policies that may impact on privacy;
- an overview of new and/or revised privacy related policies and procedures implemented;
- a description of major changes implemented as a result of concerns or issues raised by the OPC or the Auditor General;
- an indication of privacy complaints or investigations processed and a summary of related key issues, and;
- an indication of the number of applications or appeals submitted to the Federal Court or Federal Court of Appeal on *Privacy Act* matters.

This "fix" was supported by CIPPIC, David Flaherty, Paul André Comeau, and the Canadian Bar Association.

Committee Response: *The Committee supports this recommendation and suggests that the Minister consider amending the Act accordingly.*

Quick Fix #9: **Introduction of a provision requiring an ongoing five year Parliamentary review of the *Privacy Act.***

The current *Act* contains a requirement that it be reviewed by Parliament on a "permanent basis" in section 75, but it does not set any time intervals at which this review must be

regularly performed. The Commissioner testified that this is in contrast to PIPEDA, which requires that Parliament review the legislation every five years. The only complete statutory review that has been performed on the *Privacy Act* so far is the *Open and Shut* report of the House of Commons Standing Committee on Justice and the Solicitor General in 1987. That report contained more than 100 recommendations for improving both privacy and access legislation, but they were never implemented.

The Commissioner recommended that the *Privacy Act* be amended to contain the same five-year review requirement as PIPEDA, in order to ensure that it receives regular attention and updating from legislators.

This "fix" was supported by David Flaherty, Paul André Comeau, and the Canadian Bar Association. The Canadian Bar Association in particular noted that this is an important tool for ensuring that the act stays up-to-date:

> While we're not purporting to say that a full comprehensive review needs to be done every five years, at the minimum there needs to be a bit of a reality check to make sure that this important piece of legislation that's been identified by the Supreme Court of Canada as being quasi-constitutional actually does keep up with the requirements of modern society. And it's our view that it hasn't. The world has changed significantly. The government information practices have changed very significantly since 1982, and it's very difficult to say what the next five years, ten years, fifteen years are going to look like.[32]

Committee Response: *The Committee supports this recommendation and suggests that the Minister consider amending the Act accordingly.*

Quick Fix #10: **Strengthen the provisions governing the disclosure of personal information by the Canadian government to foreign states.**

The current *Act* allows the Canadian government to share personal information about its citizens with foreign governments under any agreement to do so, written or otherwise, provided it is for the purposes of administering a law or conducting an investigation. The Commissioner proposes amending paragraph 8(2)(f) of the *Act* to add the phrase "which has a reasonable and direct connection to the original purpose for which the information was obtained."

She also proposes either amending the legislation or promulgating new regulations to provide specific guidance as to how this type of information should be handled, and suggests that the changes be based on the current Treasury Board guidelines for what information-sharing agreements with foreign governments should contain. Finally, she proposes that the government consider adding specific provisions to the *Act* to define the

[32] Testimony of Gregory DelBigio and David Fraser, Canadian Bar Association, to the Committee, June 3, 2008 at 1640.

responsibilities of those who transfer personal information to other jurisdictions and to address the issue of the adequacy of protection for the information in those jurisdictions.

This tenth "fix" was the subject of the most discussion among the various witnesses who appeared before the Committee.

CIPPIC agreed with the Commissioner's proposal but suggested adding a requirement that Canadians be notified by the government when their personal information is being shared with foreign states. CIPPIC particularly recommended that Canada adopt requirements used in Europe and Quebec that personal information held by governments only be shared with countries that have protective standards at an equivalent level to their own, or that contract arrangements be used to hold foreign governments to Canadian standards of protection. CIPPIC also cited concerns about the treatment of personal information obtained by the Federal Bureau of Investigation (FBI) in the United States, and recommended that the exemption in the *Act* to allow the government to provide personal information to comply with a Court subpoena or warrant be amended to apply only to subpoenas or warrants issued by Canadian courts.

Other witnesses who supported the Commissioner's proposal were David Flaherty, Paul André Comeau, Professor Michael Geist, and the Canadian Bar Association. Professor Geist stated that while his expertise mostly involved cross-border sharing of data in the private sector through outsourcing contracts and similar arrangements, he was of the view that the risks of cross-border sharing in any context could not be fully controlled by legislation. He stated that he believes the law to be an essential tool in managing those risks, but noted that it is difficult to impose Canadian standards on foreign jurisdictions even by way of contracts holding them to those standards – many jurisdictions cannot provide assurances of meeting them. He noted that the European approach of forbidding data transfer across borders except to countries with equivalent standards has proven difficult to implement and enforce in practice.

The Canadian Bar Association provided details reasons as to why it believes greater legislative oversight of cross-border data sharing is needed:

> The reasons for this oversight include the following: that an individual will have no opportunity to know when a law enforcement agency has collected data about the individual; if the data has been collected, the individual will have no opportunity to learn what the data is or whether it's accurate; an individual will have no opportunity to know if data has been shared with a foreign government or institution, and if so, what foreign government or institution the data's been shared with; an individual will have no opportunity to know the uses for which the data will be used by a foreign government or institution; an individual will have no opportunity to know if the foreign government or institution will have shared the data with other governments or institutions; an individual will have no way of knowing whether the foreign government or institution that has received data will comply with any terms or arrangement under which the data was transferred by the Government of Canada; and the data may be used by a foreign government or

institution in a manner or for a purpose that significantly jeopardizes the individual, the individual's family, or friends.[33]

CSIS did not agree with this proposed "fix". It indicated that it does not have written information-sharing agreements with all countries because many of them will not agree to written versions. CSIS further testified that whether or not information-sharing agreements with foreign countries are themselves in writing, they are all subject to pre-screening and agreement by the Minister of Public Safety and the Minister of Foreign Affairs under section 17 of the *Canadian Security Intelligence Service Act*, so a written description of them from that initial consultation already exists for each one. According to the official from CSIS who appeared before the Committee, the Security Intelligence Review Committee (SIRC) is also required to do an annual review of all of these arrangements under paragraph 38(a)(iii) of the *Canadian Security Intelligence Service Act*, even though this is not made public. As of the 2007 annual report, there were 271 foreign arrangements with agencies in 147 countries, and SIRC found that CSIS had duly considered the human rights situation and proceeded cautiously in each country with which it had an arrangement. CSIS also stated that in the field, when information is about to be shared, there is scrutiny of the foreign agency's past history and reliability in its dealings with Canada, and a sign-off by a director-general in each instance. CSIS testified that questions will usually be asked about why the information is being requested, although there are rare instances where this is not the case.

The RCMP also did not support this proposed "fix". It noted that Interpol has requested information from Canada approximately 4,000 times in the preceding year, and that the RCMP's liaison officers shared information with foreign agencies approximately 3,000 times that year, so a large volume of information is covered by the current exemption. The RCMP indicated that when sharing information with foreign governments, it follows the recommendations of Justice O'Connor, the author of the Arar Report,[34] by focusing on the "accuracy, reliability and origin of information" as the main concerns. The RCMP testified that it conducts a qualitative assessment of requests for information, with regard to the nature of the information, its intended use, and the human rights record of the country requesting it. It believes this "principled approach" is the best way to handle such information-sharing, since not all of the circumstances under which information might need to be shared can be anticipated and legislated for in advance. The RCMP indicated that generally all of its information-sharing agreements with other countries are in writing, and that some are quite flexible, such as a Memorandum of Understanding (MOU) with the United States governing joint investigations.

The Canada Border Services Agency (CBSA) did not testify directly about this proposal, but mentioned some related matters such as the "no fly" list that concerns the security history of passengers on airlines flights. It noted that the United States has a different no-fly list from Canada's and sometimes relies on its own interpretation of information in the

[33] Testimony of Gregory DelBigio and David Fraser, Canadian Bar Association, to the Committee, June 3, 2008 at 1610.

[34] Justice O'Connor, Report on the Factual Inquiry with respect to the *Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar*.

Canadian Police Information Centre (CPIC) system about past criminal convictions. It also testified that there is an agreement between the countries with respect to handling such issues when they involve third party nationals who are not American or Canadian citizens.

The CBSA was questioned about whether its collection of personal information from people crossing the border was being properly documented, or whether it was taking place primarily through verbal exchanges. The Members of the Committee referred to the Privacy Commissioner's findings that the CBSA's policy of written documentation was not being followed, and the witnesses indicated that work was being done to address that issue.

Committee Response: *The Committee is generally supportive of the Commissioner's recommendation, but there are some differing views on whether an exemption would need to be added to such an amendment for law enforcement purposes. The Committee suggests that the Minister consider an amendment and the form it would take.*

Quick Fix #11: Introduce a provision for proper security safeguards requiring the protection of personal information.

The Privacy Commissioner recommended this additional "quick fix" during her concluding appearance before the Committee on May 11, 2009. She testified to the Committee that it would involve enacting an existing Treasury Board directive on security into law:

> There is a Treasury Board directive on security and the protection of personal information. But in my experience and that of my predecessors, a Treasury Board directive does not seem to get the attention it requires from the department, certainly much less so than if were in an act. I do not wish to imply that there are no security safeguards. The government is presently developing a cyber security policy, and that is very important. I am very pleased that they are moving forward, but we are talking about day-to-day administrators of the act. I think that Parliament sends a much stronger message if it puts some minimum requirements into legislation, if it enshrines in legislation the basics of what needs to be done. [35]

This "quick fix" is similar to a recommendation made by the Canadian Bar Association (CBA) during its testimony to the Committee that the *Act* include a "duty to protect", i.e. to securely store the personal information under its control. The underlying rationale for the CBA proposal was as follows:

> Currently there's no statutory requirement that government safeguard that information, and there's currently no obligation that government notify affected individuals if their information is lost or disclosed. And it's not just a matter of individuals wanting to know what's happening with their information, which may

[35] Testimony of the Privacy Commissioner to the Committee, May 11, 2009 at 1640.

> in fact be their right or should be their right, but it's a matter of giving individuals the opportunity to take steps to mitigate any harm that might happen with respect to the misuse of that personal information.[36]

The CBA additionally proposed that requirements to monitor the amount and kind of data sharing that goes on between federal government departments be included in the *Act* as well, but the Commissioner did not include this element in her proposed fix.

Committee Response: *The Committee supports the Commissioner's recommendation and suggests that the Minister consider amending the Act accordingly.*

Quick Fix #12: Enshrine Treasury Board's breach notification guidelines into legislation.

The Privacy Commissioner recommended this additional "quick fix" during her concluding appearance before the Committee on May 11, 2009. She testified to the Committee that it would involve enacting existing Treasury Board guidelines on notification in the case of breaches of personal information by a government department into law[37]:

> Obviously the Government of Canada has a security policy and Treasury Board has breach notification guidelines, but again we don't hear much about problems of data being lost or misused in the public sector. But we know there are some. We know them often from the media. Occasionally we'll hear something from the government itself, but again it's kind of a momentum like what I was describing with when you go before a federal court. If you put this into a law and you say there's breach notification guidelines and you have to inform the Privacy Commissioner when there's a breach notification, I am banking on the hope that this will mean that these issues are taken more seriously and there are fewer stolen laptops with citizen's information found under bridges as we reported on a couple years ago.[38]

This "quick fix" is similar to a recommendation made by the Canadian Bar Association (CBA) that a duty to notify of breaches be added to both the public and private sector legislation on privacy:

> The Canadian Bar Association is advocating on both sides—within PIPEDA, the private sector legislation, and in the Privacy Act, the public sector legislation—

[36] Testimony of Gregory DelBigio and David Fraser, Canadian Bar Association, to the Committee, June 3, 2008 at 1605.
[37] The Commissioner did not specify the particular guidelines to which she was referring. The Treasury Board of Canada Secretariat has issued *Guidelines for Privacy Breaches*, available on-line at http://www.tbs-sct.gc.ca/atip-aiprp/in-ai/in-ai2007/breach-atteint-eng.asp and last modified March 23, 2007. All of the Treasury Board policies in the area of access and privacy are currently undergoing an update and revision process.
[38] Testimony of the Privacy Commissioner to the Committee, May 11, 2009, at 1615.

> that there be breach notification guidelines. We have not taken a specific position on the specifics of them in terms of what information would have to be disclosed in order for the individual to be notified, because it is a matter of balance. You don't want people to be bombarded by notifications about trivial breaches, but you do want to make sure that individuals whose information is compromised in a way that could actually have a significant impact on them are notified. So we're advocating in both pieces of legislation that there should be balanced notification.[39]

Committee Response: *The Committee takes no position on this recommendation at the current time and agrees that it requires further study.*

Other Possible Areas of Reform:

Training and Resources

The Commissioner made general comments in her testimony about the need to increase and improve training across the federal public service with respect to the handling of personal information. She also referred to the ongoing resource challenges faced by both federal institutions and her own Office in handling the large workload generated by the current legislation, and emphasized the importance of staffing to the level needed to ensure the objectives of the *Act* are carried out in full.

Other witnesses referred to the need to improve training and staffing across the federal government, most notably David Flaherty:

> In term *[sic]* of privacy training, there are more than 200,000 public servants, most of whom have not had privacy training in a long time. They don't understand the ten privacy principles and wouldn't know a privacy issue if it hit them in the head. Some do, of course, but that kind of knowledge is transitory. The name of the game today is a 20-minute quiz, 30-minute test, taken once a year, with certification to your HR record that you've actually had privacy training. As I said to you before, you'll recognize that one of the basic privacy principles is involved.[40]

Order-Making Powers

Several of the witnesses who testified proposed that the Privacy Commissioner be granted order-making powers, like her counterparts in some of the provinces.[41]

---

[39] Testimony of Gregory DelBigio and David Fraser, Canadian Bar Association, to the Committee, June 3, 2008 at 1615.
[40] Testimony of David Flaherty to the Committee, May 8, 2008 at 1540.
[41] The provinces that grant some form of order-making powers to its commissioners in this area are Quebec, Ontario, Alberta, British Columbia and Prince Edward Island.

The question of whether to give the Privacy Commissioner order-making powers has been previously studied by this Committee in its statutory review of PIPEDA, the private sector legislation,[42] but the Committee did not endorse this recommendation at the time, citing the need to let the Commissioner adjust to the new powers under PIPEDA before making further changes to the ombudsperson model on which her Office is currently based. The matter has also been studied by Justice Laforest in a study commissioned by the Minister of Justice in 2005,[43] and he also rejected the idea. The ombudsman model used by the Privacy Commissioner is similar to that used for the seven other officers of Parliament, and changes to it would have wide-ranging implications.

However, the proposal continues to be raised by many observers and privacy advocates, and recently the Information Commissioner came before the Committee as part of an unrelated study on the access to information legislation, and proposed that he be given a limited version of order-making powers, with respect to administrative complaints only.[44]

The Privacy Commissioner herself has not proposed this change, and has in the past indicated that she does not seek these powers. However, this idea was endorsed during the Committee's study of the *Privacy Act* by CIPPIC, David Flaherty, Paul André Comeau, and Professor Geist. The Canadian Bar Association indicated that while it had not studied this particular proposal, an alternative route might be to grant greater powers to the Federal Court instead, allowing it to award remedies on all matters covered by the *Act*, instead of just restricting it to denial of access issues.

The witnesses who supported this proposal all emphasized the need to give the Privacy Commissioner powers with "teeth" to enable her to make decisions and orders that deal with ongoing privacy challenges as they evolve in the context of her investigations.

New Exemptions

The RCMP suggested during its testimony to the Committee that there may be a need for even a more extensive national security exemption than the one that already exists in the *Act* for law enforcement investigations. It also suggested that there may be a growing need to obtain names and addresses of users from Internet Service Providers (ISPs).

Committee Response: *The Committee recommends that these additional proposals for reform be considered for study at a later date, when an in-depth comprehensive review of further reforms to the Privacy Act is commenced.*

---

[42] *Statutory Review of the Personal Information Protection and Electronic Documents Act* (PIPEDA), 4th Report of the Standing Committee on Access to Information, Privacy and Ethics, May 2007.
[43] The Honourable Gérard V. Laforest, *The Offices of the Information and Privacy Commissioners: The Merger and Related Issues* - Report of the Special Advisor to the Minister of Justice**,** November 15, 2005.
[44] Testimony of Robert Marleau, Information Commissioner of Canada, to the Committee, March 9, 2009.

SUMMARY:

Below are the twelve "quick fixes" to the *Privacy Act* recommended by the Privacy Commissioner of Canada, and the response of the House of Commons Standing Committee on Access to Information, Privacy and Ethics to each of them.

Quick Fix # 1: Create a legislative "necessity test" which would require government institutions to demonstrate the need for the personal information they collect.

Committee Response: *The Committee discussed whether section 4 of the Privacy Act is robust enough in its current form to give full effect to the rights underpinning the Act, but there were varying opinions on this issue. The Minister may wish to give it further study and consideration.*

Quick Fix #2: Broaden the grounds for which an application for Federal Court review under section 41 of the *Privacy Act* may be made to include the full array of privacy rights and protections under the *Privacy Act* and give the Federal Court the power to award damages against offending institutions.

Committee Response: *The Committee discussed section 41 and whether access to the courts under it should be broadened by means of proposing amendments. It also discussed the relationship between this recommendation and recommendation #6, the proposal to give the Commissioner the discretion to refuse to investigate frivolous or vexatious complaints. The Committee recognizes the varying viewpoints of all who testified on this issue, and would suggest that the Minister give it further study and consideration. Discussion between the Minister and the Commissioner may help to determine whether these proposals should move forward, or be modified.*

Quick Fix #3: Enshrine a requirement for heads of government institutions subject to the *Privacy Act* to assess the privacy impact of programs or systems prior to their implementation and to publicly report assessment results.

Committee Response: *The Committee discussed this recommendation and while it is sympathetic to the concerns raised by the Commissioner, does not consider this proposal to be a top priority for reform at this time.*

Quick Fix #4: **Amend the *Privacy Act* to provide the Office of the Privacy Commissioner of Canada with a clear public education mandate.**

Committee Response: *The Committee supports this recommendation and suggests that the Minister consider amending the Act accordingly.*

Quick Fix #5: **Provide greater discretion for the Office of the Privacy Commissioner of Canada to report publicly on the privacy management practices of government institutions.**

Committee Response: *The Committee would support the proposal that more frequent latitude be given to the Commissioner to report to Parliament, subsequent to which her findings could be discussed publicly. To the extent that the proposal would require legislative amendment to allow disclosure other than provided for under the Officer of Parliament model where reports must be tabled in Parliament first, the Committee would have concerns. The Committee also expressed concern about what would constitute a "matter of public interest" and how this would be determined.*

Quick Fix #6: **Provide discretion for the Privacy Commissioner to refuse and/or discontinue complaints the investigation of which would serve little or no useful purpose, and would not be in the public interest to pursue.**

Committee Response: *The Committee discussed this recommendation, and noted that the Minister's testimony had linked it with the second recommendation above concerning broadening the Court's powers with respect to the Privacy Act. The Committee recognizes the varying viewpoints of all who testified on this issue, and would suggest that the Minister give it further study and consideration. Discussion between the Minister and the Commissioner may help to determine whether these proposals should move forward, or be modified.*

Quick Fix #7: **Amend the *Privacy Act* to align it with the *Personal Information Protection and Electronic Documents Act* (PIPEDA) by eliminating the restriction that the *Privacy Act* applies to recorded information only.**

Committee Response: *The Committee supports this recommendation and suggests that the Minister consider amending the Act accordingly.*

Quick Fix #8: **Strengthen the annual reporting requirements of government departments and agencies under section 72 of the *Privacy Act,* by requiring these institutions to report to Parliament on a broader spectrum of privacy-related activities.**

Committee Response: *The Committee supports this recommendation and suggests that the Minister consider amending the Act accordingly.*

Quick Fix #9: **Introduction of a provision requiring an ongoing five year Parliamentary review of the *Privacy Act.***

Committee Response: *The Committee supports this recommendation and suggests that the Minister consider amending the Act accordingly.*

Quick Fix #10: **Strengthen the provisions governing the disclosure of personal information by the Canadian government to foreign states.**

Committee Response: *The Committee is generally supportive of the Commissioner's recommendation, but there are some differing views on whether an exemption would need to be added to such an amendment for law enforcement purposes. The Committee suggests that the Minister consider an amendment and the form it would take.*

Quick Fix #11: Introduce a provision for proper security safeguards requiring the protection of personal information.

Committee Response: *The Committee supports the Commissioner's recommendation and suggests that the Minister consider amending the Act accordingly.*

Quick Fix #12: Enshrine Treasury Board's breach notification guidelines into legislation.

Committee Response: *The Committee takes no position on this recommendation at the current time and agrees that it requires further study.*

Other Possible Areas of Reform

Committee Response: *The Committee recommends that these additional proposals for reform be considered for study at a later date, when an in-depth comprehensive review of further reforms to the Privacy Act is commenced.*

REQUEST FOR GOVERNMENT RESPONSE

Pursuant to Standing Order 109, the Committee requests that the government table a comprehensive response to this Report.

A copy of the relevant Minutes of Proceedings (Meetings Nos 28-36, 38, 39) of the 2nd Session of 39th Parliament and (Meetings Nos 10, 11, 17, 18, 20-23) of the 2nd Session of the 40th Parliament is tabled.

Respectfully submitted,

Paul Szabo, MP

Chair

APPENDIX A
LIST OF WITNESSES

Organizations and Individuals	Date	Meeting
Thirty-ninth Parliament, second Session		
As an individual	2008/04/15	28
Heather H. Black		
Office of the Privacy Commissioner of Canada	2008/04/17	29
Raymond D'Aoust, Assistant Privacy Commissioner		
Elizabeth Denham, Assistant Privacy Commissioner		
Patricia Kosseim, General Counsel		
Tom Pulcine, Director General and Chief Financial Officer, Corporate Services Branch		
Jennifer Stoddart, Privacy Commissioner		
Office of the Privacy Commissioner of Canada	2008/04/29	30
Raymond D'Aoust, Assistant Privacy Commissioner		
Patricia Kosseim, General Counsel		
Maureen Munhall, Director, Human Ressources Services		
Jennifer Stoddart, Privacy Commissioner		
Treasury Board Secretariat	2008/05/01	31
Ken Cochrane, Chief Information Officer		
Donald Lemieux, Executive Director, Information, Privacy and Security Policy		
Canada Border Services Agency	2008/05/06	32
Paul Colpitts, Director, Access to Information, Privacy and Disclosure Policy Division		
Caroline Melis, Director General, Intelligence Directorate, Enforcement Branch		
Janet Rumball, Director of Outreach and Consultation, Western Hemisphere Travel Initiative and Innovation, Science and Technology Branch		
Canadian Internet Policy and Public Interest Clinic		
Philippa Lawson, Director		
As an individual	2008/05/08	33
David Flaherty, Professor Emeritus, University of Western Ontario		

Organizations and Individuals	Date	Meeting
Canadian Security Intelligence Service (CSIS)	2008/05/13	34
Geoffrey O'Brian, Advisor, Operations and Legislation		
Royal Canadian Mounted Police		
Bob Paulson, Chief Superintendent and Acting Assistant Commissioner, National Security Criminal Investigations		
As an individual	2008/05/15	35
Paul-André Comeau, Director, Laboratoire d'étude sur les politiques publiques et la mondialisation (ÉNAP)		
Michael Geist, Canada Research Chair, Internet and E-commerce Law, University of Ottawa		
Department of Justice	2008/05/27	36
Carolyn Kobernick, Assistant Deputy Minister, Public Law Sector		
Denis Kratchanov, Director and General Counsel, Information Law and Privacy Section		
Hon. Rob Nicholson, Minister of Justice and Attorney General of Canada		
Joan Remsu, General Counsel, Public Law Policy Section		
Canadian Bar Association	2008/06/03	38
Gregory DelBigio, Chair, National Criminal Justice Section		
David Fraser, Treasurer, National Privacy and Access Law Section		
Correctional Service Canada	2008/06/05	39
Ian McCowan, Assistant Commissioner, Policy and Research		
Anne Rooke, Director, Access to Information and Privacy		
Fortieth Parliament, second Session		
Office of the Privacy Commissioner of Canada	2009/05/11	20
Chantal Bernier, Assistant Privacy Commissioner		
Hedy Kirkby, Acting Senior Counsel		
Jennifer Stoddart, Privacy Commissioner		

APPENDIX B
LIST OF BRIEFS

Organizations and Individuals

Canadian Bar Association

Canadian Resource Centre for Victims of Crime

Flaherty, David

Royal Canadian Mounted Police

Supplementary Report from Bill Siksay MP (Burnaby-Douglas) for the New Democratic Party

New Democrats strongly support all 12 “quick fix” recommendations made by Privacy Commissioner of Canada. New Democrats urge the government to introduce legislative amendments to the Privacy Act based on these proposed immediate changes without further delay. We concur in the rationale provided by the Commissioner for her recommendations.

Our support is based on the crucial importance of up-to-date and effective legislation to protect the privacy of Canadians when it comes to the operations of the federal government. It is also based in the fact that the Privacy Act has been deemed to have quasi-constitutional status in recognition of its fundamental importance to Canadians.

At one time Canada was a leader in protecting the privacy of its citizens. However, the Privacy Act has not kept up with the times or with developments in privacy protection. In fact, this legislation has not been significantly amended since its introduction.

New Democrats also appreciate the need to move from policy to legislation with regard to privacy protection. As the Commissioner noted in her testimony to the Standing Committee, “…it is far easier to ignore a policy as opposed to a legislated requirement.” Privacy protections must be applied rigorously and consistently across government, and up-to-date and effective legislation is central to this goal.

The government must also fully address the findings related to privacy issues of the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar by The Honourable Dennis O'Connor and the Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmed Abou-Elmaati and Muayyed Nureddin by The Honourable Frank Iacobucci in any legislative or regulatory proposals it brings forward.

New Democrats call on the government to introduce, without further delay, a comprehensive package of reforms to the Privacy Act which at a minimum incorporates all of the quick fix recommendations from the Privacy Commissioner of Canada.

Privacy Act Reform Recommendations

Recommendation Number 1: Create a legislative "necessity test" which would require government institutions to demonstrate the need for the personal information they collect.

Recommendation Number 2: Broaden the grounds for which an application for Court review under section 41 of the *Privacy Act* may be made to include the full array of privacy rights and protections under the *Privacy Act* and give the Federal Court the power to award damages against offending institutions.

Recommendation Number 3: Enshrine a requirement for heads of government institutions subject to the *Privacy Act* to assess the privacy impact of programs or systems prior to their implementation and to publicly report assessment results.

Recommendation Number 4: Amend the *Privacy Act* to provide the Office of the Privacy Commissioner of Canada with a clear public education mandate.

Recommendation Number 5: Provide greater discretion for the Office of the Privacy Commissioner of Canada to report publicly on the privacy management practices of government institutions.

Recommendation Number 6: Provide discretion for the Privacy Commissioner to refuse and/or discontinue complaints the investigation of which would serve little or no useful purpose, and would not be in the public interest to pursue.

Recommendation Number 7: Amend the *Privacy Act* to align it with the *Personal Information Protection and Electronic Documents Act* by eliminating the restriction that the *Privacy Act* applies to recorded information only.

Recommendation Number 8: Strengthen the annual reporting requirements of government departments and agencies under section 72 of the *Privacy Act*, by requiring these institutions to report to Parliament on a broader spectrum of privacy-related activities.

Recommendation Number 9: Introduction of a provision requiring an ongoing five year Parliamentary review of the *Privacy Act*.

Recommendation Number 10: Strengthen the provisions governing the disclosure of personal information by the Canadian government to foreign states.

Recommendation Number 11: Introduce a provision for proper security safeguard requiring the protection of personal information.

Recommendation Number 12: Enshrine Treasury Board's breach notification guidelines into legislation.

Office of the
Privacy
Commissioner
of Canada

Commissariat
à la protection de
la vie privée du Canada

Proposed Immediate Changes to the *Privacy Act*

Appearance before the Standing Committee on Access to Information, Privacy and Ethics

April 29, 2008

Canada

Table of Contents

Statement

Proposed Immediate Changes to the *Privacy Act*

Appearance before the Standing Committee on Access to Information, Privacy and Ethics

April 29, 2008

Statement by
Jennifer Stoddart
Privacy Commissioner of Canada

(Check against delivery)

Introduction

Thank you, Mr. Chairman and members of the Committee, for inviting me to address you once again on the issue of *Privacy Act* reform. I'm joined by Raymond D'Aoust, Assistant Commissioner for the *Privacy Act*, and Patricia Kosseim, our General Counsel.

In 2006, as you may recall, my Office tabled with the Committee a comprehensive document entitled *Government Accountability for Personal Information: Reforming the Privacy Act*. More recently, for the purposes of our April 17 appearance, we prepared an Addendum to that document, discussing how events of the past two years illustrate the ongoing need for reform of the Act. At that time, I provided you with a list of ten recommended changes to the *Privacy Act*. These changes were outlined in my opening statement to the Committee.

Further to a request from the Committee, my Office has now prepared a third document, which provides greater detail on the rationale supporting our ten "quick fix" recommendations.

I would like to make it clear that the changes we are currently proposing are not meant to be the definitive statement on *Privacy Act* reform. This is most emphatically not the case – the *Privacy Act* is in desperate need of a full Parliamentary review and complete overhaul.

I realize, however, that a full Parliamentary review of the Act may not happen for some time. While we wait for a comprehensive modernization initiative, there are some relatively simple changes we could make which would be of significant benefit to Canadians.

Some of the changes we are suggesting would simply incorporate into law existing Treasury Board Secretariat policies and practices. Other recommendations correspond to privacy requirements found in *PIPEDA* – Canada's private sector privacy law.

"Quick Fix" Recommendations

I'd like to provide a quick overview of the ten recommendations:

1. Parliament should create a requirement in the *Privacy Act* for government departments to demonstrate the need for collecting personal information. This "necessity test" is already included in Treasury Board policies as well as *PIPEDA*. It is an internationally recognized privacy principle found in modern privacy legislation around the world.

2. The role of the Federal Court should be broadened to allow it to review all grounds under the *Privacy Act*, not just denial of access.

3. Parliament should enshrine into law the obligation of Deputy Heads to carry out a Privacy Impact Assessment – or PIA – before a new program or policy is implemented.

4. The *Privacy Act* should be amended to provide my Office with a clear public education mandate. *PIPEDA* contains such a mandate and it is only logical that the *Privacy Act* contain a similar mandate for the public sector.

5. The Act should be further amended to provide my Office with increased flexibility to publicly report on the privacy management practices of the federal government. As it now stands, we are limited to reporting to Parliament and Canadians through annual or special reports.

6. My Office should have greater discretion to refuse or discontinue complaints if an investigation would serve no useful purpose or is not in the public interest. This would allow us to focus investigative resources on privacy complaints which are of broad systemic interest and affect the interests of a significant number of Canadians.

7. The Act should be aligned with *PIPEDA* by eliminating the restriction that the *Privacy Act* applies only to "recorded" information. At the moment, for example, personal information contained in DNA and other biological samples is not explicitly covered.

8. Annual reporting requirements of government departments and agencies under section 72 of the Act could be strengthened by requiring these institutions to report to Parliament on a wider spectrum of privacy-related activities.

9. The Act should include a provision requiring an ongoing five-year Parliamentary review of the *Privacy Act*, as is the case with *PIPEDA*.

10. The Act should be strengthened with respect to the provisions governing the disclosure of personal information by the Canadian government to foreign states. Treasury Board Secretariat (TBS) has taken some important steps by providing guidance on information sharing agreements and outsourcing of personal data processing. However, we need privacy protections related to cross-border information sharing enshrined into law.

Privacy Education in the Public Service

Our Office also believes more needs to be done to ensure that program managers in the public services are aware of their responsibilities under the *Privacy Act* and related TBS guidelines.

I urge the Government to carry out a comprehensive assessment of the privacy training provided to public servants. It is critical that privacy issues are thoroughly addressed in leadership, professional development and management courses aimed at all levels of the public service.

Conclusion

In closing I would like to re-emphasize that although we are proposing ten “quick fix” changes, the *Privacy Act* is still very much in need of a major review and overhaul. There are many other problems with the Act that require attention, including the need for proper security safeguards for personal information and mandatory breach notification. This said, however, making the adjustments to the Act that we are suggesting would certainly help to enhance the level of personal information protection in the federal public sector.

Thank you for inviting me to share some further thoughts on this important subject. We would be pleased to answer any questions.

Recommendations

Recommendation Number 1: Create a legislative “necessity test” which would require government institutions to demonstrate the need for the personal information they collect.

Recommendation Number 2: Broaden the grounds for which an application for Court review under section 41 of the *Privacy Act* may be made to include the full array of privacy rights and protections under the *Privacy Act* and give the Federal Court the power to award damages against offending institutions.

Recommendation Number 3: Enshrine a requirement for heads of government institutions subject to the *Privacy Act* to assess the privacy impact of programs or systems prior to their implementation and to publicly report assessment results.

Recommendation Number 4: Amend the *Privacy Act* to provide the Office of the Privacy Commissioner of Canada with a clear public education mandate.

Recommendation Number 5: Provide greater discretion for the Office of the Privacy Commissioner of Canada to report publicly on the privacy management practices of government institutions.

Recommendation Number 6: Provide discretion for the Privacy Commissioner to refuse and/or discontinue complaints the investigation of which would serve little or no useful purpose, and would not be in the public interest to pursue.

Recommendation Number 7: Amend the *Privacy Act* to align it with the *Personal Information Protection and Electronic Documents Act* by eliminating the restriction that the *Privacy Act* applies to recorded information only.

Recommendation Number 8: Strengthen the annual reporting requirements of government departments and agencies under section 72 of the *Privacy Act*, by requiring these institutions to report to Parliament on a broader spectrum of privacy-related activities.

Recommendation Number 9: Introduction of a provision requiring an ongoing five year Parliamentary review of the *Privacy Act*.

Recommendation Number 10: Strengthen the provisions governing the disclosure of personal information by the Canadian government to foreign states.

Recommendation Number 1:

Create a legislative "necessity test" which would require government institutions to demonstrate the need for the personal information they collect.

Relevant Section(s) of the *Privacy Act*:

Section 4. *No personal information shall be collected by a government institution unless it relates directly to an operating program or activity of the institution*

Background:

A far more effective expression of privacy rights, typical of modern data protection laws, is to require that the collection of information be reasonable and necessary for the program or activity. This standard has been adopted in other legislation both in Canada and abroad. Treasury Board policy states that there must be a demonstrable need for each piece of personal information collected in order to carry out the program or activity. Principle 4.4 of the *Personal Information Protection and Electronic Documents Act* ("*PIPEDA*") requires the collection to be limited to that which is necessary for the purposes identified. The standard set in section 12 of the *CSIS Act* limits information collection "to the extent that it is strictly necessary" to that institution's mandate.

Almost all provinces and the territories have adopted a model in the public sector legislation that requires that one of three conditions be met: (i) the collection is expressly authorized by statute; (ii) the information is collected for the purpose of law enforcement; or (iii) the information relates directly to and is necessary for an operating program or activity.

Consideration should also be given to including a requirement that the government institution must collect personal information in the least intrusive and most transparent manner possible, to address technologies which are inherently privacy-invasive such as video surveillance, GPS, biometrics, etc.

Rationale:

Giving Effect to the Fundamental Right to Privacy

The Supreme Court of Canada has recognized on numerous occasions that privacy interests are worthy of protection under the Charter[1] and that the *Privacy Act* has quasi-constitutional status.[2] The current wording of section 4 of the *Privacy Act* sets a

[1] See for example, *Dagg v. Canada (Minister of Finance)*, [1997] 2 S.C.R. 403.
[2] *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 [*Heinz*].

disproportionately low standard for the fundamental rights at the heart of the *Privacy Act*. By building in better controls at the collection point, there is less potential for misusing and disclosing personal information.

Providing Stronger Legislative Controls around the Collection of Personal Information

The public reaction to HRDC's Longitudinal Labour Force File provides a graphic reminder of the need to provide better legislative controls around the collection of personal information. The Office of the Privacy Commissioner (the "OPC") reported on this matter in its 1999-2000 Annual Report. The department had assembled an extensive database for research purposes containing personal information on millions of individuals. While the department argued that it was in compliance with the literal collection standard set by the *Privacy Act*, the OPC did not accept that all of the information contained in that database was directly relevant and necessary to HRDC's operating programs and policy activities. Since then, the database has been dismantled and the department has been steadily improving in its privacy management practices.

In another of its recommendations, the OPC urges that the *Privacy Act* be broadened to permit an individual to seek court review for all aspects of personal information collection, use and disclosure. An appropriate collection standard, combined with a right of court review, would be an important first step in creating a more meaningful legal framework.

Recommendation Number 2:

Broaden the grounds for which an application for Court review under section 41 of the *Privacy Act* may be made to include the full array of privacy rights and protections under the *Privacy Act* and give the Federal Court the power to award damages against offending institutions.

Relevant Section(s) of the *Privacy Act*:

41. *Any individual who has been refused access to personal information requested under subsection 12(1) may, if a complaint has been made to the Privacy Commissioner in respect of the refusal, apply to the Court for a review of the matter within forty-five days after the time the results of an investigation of the complaint by the Privacy Commissioner are reported to the complainant under subsection 35(2) or within such further time as the Court may, either before or after the expiration of those forty-five days, fix or allow.*

42. *The Privacy Commissioner may*
(a) apply to the Court, within the time limits prescribed by section 41, for a review of any refusal to disclose personal information requested under subsection 12(1) in respect of which an investigation has been carried out by the Privacy Commissioner, if the Commissioner has the consent of the individual who requested access to the information;
(b) appear before the Court on behalf of any individual who has applied for a review under section 41; or
(c) with leave of the Court, appear as a party to any review applied for under section 41.

Background:

Under section 41 of the *Privacy Act*, the Federal Court may only review a refusal by a government institution to grant access to personal information requested by an individual under section 12 of the *Privacy Act*. Although the Commissioner can investigate complaints concerning the full array of rights and protections under the *Privacy Act* and make recommendations to the government institution, if the response of the institution is not satisfactory, neither the individual nor the Privacy Commissioner has the possibility to apply to the Federal Court for enforcement and remedy.

The inability of the *Privacy Act* to provide effective remedies for violations of privacy rights was confirmed by the Federal Court in *Murdoch v. Canada (Royal Canadian Mounted Police)*, [2005] 4 F.C.R. 340. In that case, the RCMP wrongfully disclosed

personal information regarding Mr. Murdoch to his employer. The OPC concluded that Mr. Murdoch's complaint was well-founded, and he tried to seek a Court remedy. However, the Court concluded that, as it is currently structured, the *Privacy Act* did not give Mr. Murdoch the right to seek a remedy for the breach of his privacy. Furthermore, the Court noted that the power of the Federal Court to grant a remedy is effectively restricted to granting access to personal information.

Rationale:

Giving Effect to the Fundamental and Quasi-Constitutional Status of Privacy Rights

Broadening Federal Court review would confirm that privacy rights in the public sector and the private sector are equally important, ensure that government institutions respect every Canadian's right to have their personal information collected, used and disclosed in accordance with the *Privacy Act* and give full weight to the privacy rights of individuals in a free and democratic society. The Supreme Court of Canada has confirmed that the purpose of the *Privacy Act* is to protect the privacy of individuals with respect to personal information about themselves held by a government institution, this purpose being of such importance to warrant characterizing the *Privacy Act* as "quasi-constitutional" because of the role privacy plays in the preservation of a free and democratic society. [3]

Keeping Government Accountability Through a Meaningful Review Mechanism

Implementing our recommendation would give Canadians the same rights regarding their personal information collected, used or disclosed by their own government institutions that they hold vis-à-vis private-sector organizations exercising commercial activities under *PIPEDA*. Government institutions should be even more open and accountable with respect to their personal information handling practices, and increasing government accountability clearly requires strengthened privacy rights when it comes to how government handles the personal information of Canadians. Our recommendation is essential to achieving meaningful government accountability and transparency.

Directly Protecting Privacy Rights Through the Intended Legislation

The Supreme Court of Canada has held that a third-party to an access to information request made under the *ATI Act* can apply to the Federal Court for a hearing in respect of a government institution's disclosure of personal information.[4] Given that the Supreme Court of Canada has held that the right to privacy is paramount over the right of access to information, how can it be that a third-party can appear before the Federal Court with respect to the disclosure of another person's personal information under the *ATI Act*, but that an individual cannot even seek enforcement and a remedy for a violation of the fundamental right of privacy under the *Privacy Act* vis-à-vis his or her

[3] *Heinz,* supra note 2.
[4] *Ibid.*

own personal information? Broadening Federal Court review under the *Privacy Act* would address this unintended consequence.

There is No Right Without a Remedy

Every right needs a remedy in order to have meaning. This is especially so with respect to a fundamental right such as privacy. Implementing our recommendation would ensure that the Federal Court can review the full array of fundamental rights and protections under the *Privacy Act*, including inappropriate collection, use or disclosure of personal information, failure to maintain up-to-date and accurate data, improper retention or disposal, and denials of access or correction by government institutions. It would also ensure that the Federal Court may award damages in cases where, for example, the inappropriate use or disclosure of personal information causes embarrassment or other harms to the individual concerned.

The Need for Court Guidance

Implementing our recommendation would allow the Federal Court to provide needed guidance on what constitutes inappropriate collection, use or disclosure of personal information.

Recommendation Number 3:

Enshrine a requirement for heads of government institutions subject to the *Privacy Act* to assess the privacy impact of programs or systems prior to their implementation and to publicly report assessment results.

Relevant Section(s) of the *Privacy Act*:

There is no specific section requiring Privacy Impact Assessments as part of a sound privacy regime that should be in place for ensuring compliance with the *Privacy Act* and fair information principles.

Background:

In May 2002, the Treasury Board Secretariat (the "TBS") introduced an administrative policy on Privacy Impact Assessments. The policy was adopted to assure Canadians that privacy principles would be taken into account when there are proposals for programs and services that raise privacy issues, throughout the design, implementation and evolution of those initiatives. This represents a core component of a privacy compliant regime since the policy requires that institutions demonstrate that their collection, use and disclosure of personal information respect the *Privacy Act.*

Rationale:

Given the unevenness with which government institutions are implementing the Privacy Impact Assessment policy, there should be a legal requirement for Privacy Impact Assessments to ensure that they are done on a consistent and timely basis.

Ensuring Compliance with the Privacy Impact Assessment Policy

In the OPC's 2007 audit of government compliance with the Privacy Impact Assessment policy, it was ascertained that institutions are not fully meeting their commitments under the policy. Privacy Impact Assessments are not always conducted when they should be. They are frequently completed well after program implementation, or not at all. Present PIA reporting and notification standards provide little assurance or information to Canadians seeking to understand the privacy implications of government services or programs.

Furthermore, the Policy in and of itself does not provide assurance that privacy impacts are being assessed for pervasive and strategic government-wide initiatives. Knowing the potential privacy impacts of proposed policies and plans would provide government (TBS and/or Cabinet) with an early opportunity to modify programs or systems to protect the personal information of individuals in Canada, and perhaps reduce future costs associated with program or system changes.

Strengthening Accountability

Privacy Impact Assessments should be submitted to the OPC for review prior to program implementation. Review by the OPC provides independent and objective recommendations as to how privacy could be better protected while meeting program objectives in less intrusive ways.

Ensuring the Transparency of Government Programs

Privacy Impact Assessments are vitally important and should be a key element of a privacy management framework enshrined in legislation. Canadians should be assured in law that privacy risks will be identified and mitigated as an integral part of administering federal government programs. To this end, institutions should be required to publicly report assessment results. In making the privacy implications of programs more transparent, Canadians will have an opportunity to voice their concerns and will have assurance that privacy risks are being addressed.

Recommendation Number 4:

Amend the *Privacy Act* to provide the OPC with a clear public education mandate.

Relevant Section(s) of the *Privacy Act*:

There is no specific section providing the OPC with an explicit public education mandate.

Background:

While *PIPEDA* provides the OPC with a public education mandate, the *Privacy Act* does not do so explicitly. Section 24 of *PIPEDA* states that "the Commissioner shall: (a) develop and conduct information programs to foster public understanding…; (b) undertake and publish research that is related to the protection of personal information, including any such research that is requested by the Minister of Industry; (c) encourage organizations to develop detailed policies and practices, including organizational codes of practice…; and (d) promote, by any means that the Commissioner considers appropriate, the purposes of this Part."

Rationale:

While the OPC's central function under the *Privacy Act* is the investigation and resolution of complaints, the OPC also needs to advance privacy rights by other means – through research, communication and public education. The Commissioner lacks the legislative mandate under the *Privacy Act* to educate the public about their informational privacy rights with respect to information held by federal government institutions. The Commissioner should be equally empowered to sensitize business, government and the public under the *Privacy Act*.

Case Summaries on Public Sector Personal Information Management

Currently, the main vehicle for reporting on cases is the Annual Report under the *Privacy Act*. However, with a more explicit public education mandate and more flexible means for public reporting, the OPC could publish a compendium of significant cases that fall under the *Privacy Act*, notably in the areas of national security, law enforcement, and health. Several civil society groups with an interest in privacy promotion have urged the OPC to make more timely public reports on the state of governmental surveillance activities and how these activities may impact on privacy.

Periodic Assessments of Departmental Privacy Performance

The OPC wishes to foster a more informed public debate of the federal government's role in areas involving the sharing of personal information between agencies and jurisdictions. A clear public education authority would allow the OPC to publish public

advisories and education material on significant policy and legislative measures with "personal information" components.

Support the Learning Objectives of Informational Rights Professionals

Surveys carried out by Treasury Board Canada indicate there are significant learning needs on the part of Access to Information and Privacy (ATIP) professionals, pointing to the increased number and complexity of cases, as well as to the number of new organizations being covered by the *Privacy Act* as a result of the adoption of the *Federal Accountability Act*. The surveys also reveal—corroborated by the OPC's own audit and review work—that learning needs are not being addressed by the current learning infrastructure. By making more information available in a more timely way, the OPC will become a valuable source of information on the need for a more consistent approach to privacy management across the federal government.

Broader Parameters for the OPC's Research Program

Better research into public sector personal information management is needed to inform public policy. Section 24 of *PIPEDA* allows the OPC to undertake and publish research that is related to the protection of personal information in the private sector, with a specific funding envelope. Under this education mandate, the OPC has put in place a comprehensive Research Contributions Program which has allocated over $1,000,000 to more than 30 privacy research initiatives in Canada, resulting in extensive studies on key privacy issues. These research papers are publicly available on the OPC website. A similar mandate should exist under the *Privacy Act* for research relating to public sector matters.

Benefits the Citizens and Residents of Canada

A clearer public education mandate for the OPC would allow for more extensive and better informed public dialogue on federal privacy management in areas of critical importance to the right to privacy. It would also ensure a more consistent approach to privacy compliance by addressing the learning needs of informational rights professionals.

Recommendation Number 5:

Provide greater discretion for the OPC to disclose information in the public interest on the privacy management practices of government institutions.

Relevant Section(s) of the *Privacy Act*:

There is no specific section authorizing the Commissioner to make public interest disclosures under the *Privacy Act*

Background:

Pursuant to the *Federal Accountability Act*, the OPC is now subject to both the *ATI Act* and the *Privacy Act*. As a result, there is now a public right of access under the *ATI Act* to certain information contained in OPC investigation files, and an individual right of access to personal information in such files under the *Privacy Act*. The right of access arises only once the OPC has completed its investigation, thus respecting the need to maintain confidentiality of ongoing investigations.

No changes were made by the *Federal Accountability Act* to the provisions in the *Privacy Act* that govern the Commissioner's authority to initiate a public release of its investigation activities and findings. As a result, the only clear legislative vehicles available to the OPC for public reporting purposes are the annual and special reporting provisions.

Rationale:

Serving the Public Interest and Meeting Public Expectations

It would be consistent with the recent amendments to the *ATI Act* and *Privacy Act* granting a right of access to information in OPC investigation files, to permit the OPC to release information on its own initiative concerning the personal information management practices of a government institution where this serves the public interest.

There is a public expectation that the OPC will investigate and report on matters of public interest. This is particularly so where the privacy issue is already in the public domain. The OPC has been hampered in its ability to speak with the press, with the public, and even with Members of Parliament, due to the existing confidentiality constraints in the *Privacy Act*. Furthermore, a public interest disclosure discretion would allow for more timely and relevant disclosure rather than having to wait until the end of the reporting year when the information may have become moot, stale or largely irrelevant.

Educating Canadians

Strengthening the ability to report publicly is an integral component of a strong public education mandate. Under *PIPEDA*, the legislated public education mandate is accompanied by the discretion to disclose information concerning the personal information management practices of an organization if the Commissioner considers that it is in the public interest to do so.

Upholding Public Confidence

The discretion to report publicly under PIPEDA has been an invaluable tool for the OPC in advancing public understanding, providing public assurances, and restoring public confidence where required. The discretion to make a public interest disclosure has been used responsibly and judiciously by the OPC, after due consideration of the various interests at play.

Recommendation Number 6:

Provide discretion for the Privacy Commissioner to refuse and/or discontinue complaints the investigation of which would serve little or no useful purpose, and would not be in the public interest to pursue.

Relevant Section(s) of the *Privacy Act*:

Section 29(1). *Subject to this Act, the Privacy Commissioner shall receive and investigate complaints*…

Currently, subsection 29(1) of the *Privacy Act* requires the Privacy Commissioner to receive and investigate *all* complaints. The *Privacy Act* affords her with no discretion whatsoever to refuse to investigate complaints and/or discontinue investigations on any grounds.

Background:

At the time the OPC requested and received additional funding in 2006, it was the hope that the generous influx of new resources would enable the Office to reduce the lengthy and persistent delays associated with having to investigate all individual complaints that come in the door, while at the same time, focus efforts towards the more systemic and pervasive privacy threats facing modern society as a whole. Despite the progress the OPC has made to date, and notwithstanding plans to take these efforts to the next level, valuable Office resources are still being disproportionately consumed by having to open and investigate all individual complaints on a first-come first-serve basis. The waste of public resources is particularly taxing in cases where the complaints appear to have no merit, the central issue is clearly not privacy but some different dispute between the parties, the Office's intervention would serve no useful purpose and/or a full-scale investigation into the matter would not be in the public interest.

As concrete examples of some of the kinds of complaints the OPC receives, relatively little is gained by investigating and/or re-investigating:

1) repetitive issues that come up and have already been clearly decided in past cases (e.g. legitimate collection and use of Social Insurance Numbers);
2) moot time complaints where the individual has since received the information requested (e.g. where access was already provided, though technically out of time and at no disadvantage to the individual);
3) frequent complaints brought forward by the same individual who has an obvious "axe to grind" against an government institution (e.g. where contentious labour or employment issues constitute the real dispute between the parties which could be more effectively dealt with through other, more appropriate procedures);
4) multiple complaints brought by many individuals in respect of the same incident (e.g. a data breach involving personal information of many individuals which is already well documented and need not be re-investigated only to confirm what is already known);

5) issues that have already been recognized and addressed by the government institution (e.g. effective remedial action has already been taken).

Rationale:

More Effective Use of Limited Resources

Greater discretion at the front end of the intake function would enable the Commissioner to concentrate her limited available resources on complaints that raise systemic issues and have broader, more significant impact on the state of personal information management across the Federal Government.

Traditionally, privacy issues have come up through the individual complaint system as a result of discrete informational transactions between individuals and their governments. Today, major privacy issues arise from more systemic threats resulting from the encroachment of national security and law enforcement initiatives, multiple trans-border data flows, sophisticated data-mining and data-matching programs, and rapidly-advancing information technologies, particularly those enabled by the internet. Such new and emerging threats affect society as a whole, on such a daily and pervasive level, and in such complex and non-transparent fashion, that in most cases, the average person would not even know about them, let alone complain about them.

Data protection authorities around the world recognize that they must increasingly direct their efforts at curbing these massive threats at their source, as these emerge, rather than wait for an individual to bring a complaint about them and deal with them as they make their way up the long queue. Many data protection authorities in Canada and elsewhere face similar challenges in having to treat all complaints received indiscriminately, with no ability to dismiss or discontinue some of them early on where no public interest would be served by investigating or continuing to investigate them. We are all concerned about the cost of carrying out investigations that amount to no useful purpose and the corresponding *opportunity* cost of not dealing more effectively with the growing number of broad and systemic issues that are far more pervasive and pose much greater threat to privacy rights.

Focussing Investigative Resources on Privacy Issues that are of Broader Public Interest

The UK Commissioner recently asked the British Parliament for the right to investigate only when an issue is in the public interest. In like manner, the US Federal Trade Commission (the “FTC”) does not accept complaints from individuals but uses them to track systemic issues warranting FTC intervention. Here in Canada, the *Canadian Human Rights Act*, the *Public Servants Disclosure Protection Act* and the *Accountability Act* as well as the *Quebec Private Sector Act* allow those Commissioners to refuse or cease to examine a matter if the application is frivolous, made in bad faith, could be better dealt

with in another forum or where further investigation would clearly serve no purpose.[5] In November 2007, the Alberta Select Special Review Committee recommended that Alberta's *Personal Information Protection Act* be amended "to provide the Commissioner with explicit authority to discontinue an investigation or a review when the Commissioner believes the complaint or request for review is without merit or where there is not sufficient evidence to proceed."[6] More recently, the British Columbia Special Review Committee recommended an identical amendment to B.C.'s *Personal Information Protection Act*, as well as a further clarification "that the Commissioner has the discretion not to proceed with an inquiry in certain circumstances and the authority to reasonably determine his own process."[7]

The OPC requests that the Committee recommend granting similar discretion for the Commissioner: one which gives the Commissioner greater discretion at the front-end to refuse complaints and/or close complaints early if their investigation would serve no useful purpose, thereby allowing the Office to focus its investigative resources on privacy issues that are of broader public interest. The OPC has asked the government that it be given the same discretion under *PIPEDA* and it makes sense that both Acts should mirror each other in this respect.

[5] *An Act Respecting the Protection of Personal Information in the Private Sector,* R.S.Q., c.P-39, s. 52 states: "The Commission may refuse or cease to examine a matter if it has reasonable grounds to believe that the application is frivolous or made in bad faith or that its intervention would clearly serve no purpose." The *Canadian Human Rights Act,* R.S.C., 1985, c.H-6, s.41, the *Public Servants Disclosure Protection Act*, S.C. 2005, c.46, s.24, and the *Federal Accountability Act*, S.C. 2006,c.9, s. 52 all have similar sections.
[6] Select Special *Personal Information Protection Act* Review Committee, Final Report, November 2007, http://www.assembly.ab.ca/committees/reports/PIPA/finalpipawReport111407.pdf, Recommendation 32 at 34.
[7] *Streamlining British Columbia's Private Sector Privacy Law*: Report of the Special Committee to Review the *Personal Information Protection Act*, April 2008, Recommendations 27 and 29, at 33-35.

Recommendation Number 7:

Amend the *Privacy Act* to align it with *PIPEDA* by eliminating the restriction that the *Privacy Act* applies to recorded information only.

Relevant Section(s) of the *Privacy Act*:

Section 3 of the *Privacy Act* defines personal information for the purposes of the *Act* to mean "information about an identifiable individual that is recorded in any form…"

Background:

The definition of personal information under the *Privacy Act* is limited to information that exists in recorded form. At the moment, personal information contained in DNA and other biological samples is not explicitly covered. This is not the case in the *PIPEDA* legislation – in which the definition of personal information includes personal information in any form. New health sector privacy laws in Canada also define personal information to include unrecorded personal information. This broader, more modernized definition serves as a means to protect the privacy rights of Canadians in a changing, technology-driven world.

Rationale:

Having the *Privacy Act* Reflect Modern Realities

The *Privacy Act's* current definition of personal information is outdated. Unrecorded information, such as from surveillance cameras that monitor, but do not record, individuals at border crossings and the comings and goings of government workers is beyond the scope of the *Privacy Act*. In an ever-shrinking world, it is important that individuals are free to go about their daily activities anonymously. With the onset of rapid technological changes, governments are using increasingly sophisticated means to monitor Canadians in the work place and on the streets.

Likewise, personal information such as DNA and other human tissue samples are not covered. This use of unrecorded information can yield intelligible information about identifiable individuals. As such, it should have legal protection.

Harmonizing the Definition of Personal Information

Modern privacy laws such as *PIPEDA* and provincial private sector privacy laws apply to both recorded and unrecorded information. For example, a security company in the Northwest Territories mounted four security cameras on the roof of its building aimed at a main intersection in Yellowknife. For several days, 24 hours a day, staff monitored a

live feed and reported a number of incidents to local police. The monitoring was intended to demonstrate the service and generate business for the company.

Although a public outcry quickly ended the company's video surveillance demonstration, the OPC had the power to investigate under *PIPEDA* and issued findings that provided helpful guidance for other organizations. The OPC concluded that, while monitoring public places may be appropriate for public safety reasons, there must be a demonstrable need, the monitoring must be done by lawful public authorities and it must be carried out in ways that incorporate all legal privacy safeguards. The *Privacy Act* would not have permitted an investigation in this situation, since no video recordings were made. A reformed *Privacy Act* needs to be responsive to the digital imagery and biometric applications of contemporary law enforcement surveillance and monitoring activities.

Recommendation Number 8:

Strengthen the annual reporting requirements of government departments and agencies under section 72 of the *Privacy Act*, by requiring these institutions to report to Parliament on a broader spectrum of privacy-related activities.

Relevant Section(s) of the *Privacy Act*:

Section 72(1). *The head of every government institution shall prepare for submission to Parliament an annual report on the administration of this Act within the institution during each financial*

Background:

The Treasury Board Secretariat issued privacy reporting guidelines for government institutions in April 2005, and updated these in February 2008.[8] The guidelines buttress section 72 by requiring Deputy Heads to report comprehensively on a wide range of management matters related to privacy promotion and protection within federal institutions.

Rationale:

The Need for More Substantive Information

Our experience in reviewing section 72 reports over the years indicates that on the whole they have rarely contained substantive information. As such their use to Parliament, Canadians, and the OPC has been somewhat limited. Section 72 reports have tended to be a patchwork of statistics pertaining to the number of requests received under the *Privacy A*ct, the dispositions taken on completed requests, the exemptions invoked or exclusions cited, and completion times.

Integrating Into Law TBS Guidelines

The OPC is of the view that the *Privacy Act* should be amended by integrating into the legislation requirements already provided for under the Treasury Board guidelines. These guidelines are quite comprehensive, and among other things require government institutions to provide:

- a description of each PIA completed during the reporting period;

[8] The guidelines, titled *Annual Reports on the Access to Information Act and the Privacy Act - Implementation Report No. 109*, are available at: http://www.tbs-sct.gc.ca/atip-aiprp/impl-rep/2008/109-imp-mise_e.asp.

- an indication of the number of new data matching and data sharing activities undertaken;
- a description of privacy-related education and training activities initiated;
- a summary of significant changes to organizational structure, programs, operations, or policies that may impact on privacy;
- an overview of new and/or revised privacy related policies and procedures implemented;
- a description of major changes implemented as a result of concerns or issues raised by the OPC or the Auditor General;
- an indication of privacy complaints or investigations processed and a summary of related key issues, and;
- an indication of the number of applications or appeals submitted to the Federal Court or Federal Court of Appeal on *Privacy Act* matters.

Benefits to Parliament, the OPC and Canadians

The Treasury Board guidelines would have added weight and authority if their provisions were mandated by the *Privacy Act*. Parliamentary committees would be better positioned to discharge their responsibilities to review the personal information management practices of the federal government in the broader context of reviewing departmental performance. A more comprehensive coverage of privacy management issues would provide Parliamentarians with relevant information to evaluate the extent to which government institutions are addressing new and emerging privacy challenges, and whether programs or initiatives being undertaken may pose a threat to the privacy rights of citizens. Canadians too would be better informed on how their personal information is being handled by government departments and agencies, and the manner in which their information requests or complaints are being processed. The OPC could better carry out its mandate, for the benefit of Parliament and Canadians as a whole.

Recommendation Number 9:

Introduction of a provision requiring an ongoing five year Parliamentary review of the *Privacy Act*.

Relevant Section(s) of the *Privacy Act*:

Section 75(1). *The administration of this Act shall be reviewed on a permanent basis by such committee of the House of Commons, of the Senate or of both Houses of Parliament as may be designated or established by Parliament for that purpose.*

Section 75(2). *The committee designated or established by Parliament for the purpose of subsection (1) shall, not later than July 1, 1986, undertake a comprehensive review of the provisions and operation of this Act, and shall, within a year after the review is undertaken or within such further time as the House of Commons may authorize, submit a report to Parliament thereon including a statement of any changes the committee would recommend.*

Background:

Currently, there is no mandatory periodic review of the *Privacy Act* to ensure its ongoing evolution and adaptation to modern realities and challenges. By contrast, section 29 of *PIPEDA* requires that the first part of that act be reviewed ***every five years*** by the committee of the House of Commons, or of both Houses of Parliament, that may be designated or established by Parliament for that purpose. A number of provinces have a similar requirement for regular legislative review of their public sector privacy law.

While a statutory review of the *Privacy Act* took place in 1987, the recommendations in the report Open and Shut and in the testimony heard by the Justice standing committee were never enacted.[9] The OPC has repeatedly emphasized the need for informed public debate on privacy laws whether they apply to the operations of government or to the activities of the private sector. Discussion of privacy issues has been spotty and targeted since the review in 1987, with a very limited consultation on electronic commerce issues prior to PIPEDA implementation, and the sole Senate committee hearings on the proposed privacy charter under Senator Sheila Finestone in 1995-96.[10]

Rationale:

Harmonize the Data Protection Framework across Jurisdictions in Canada

[9] *Open and Shut: Enhancing the Right to Know and the Right to Privacy*, Report of the Standing Committee on Justice and Solicitor General on the Review of the Access to Information Act and the Privacy Act (March 1987).

[10] *Privacy: Where Do We Draw The Line?* Report of the Standing Committee on Human Rights and the Status of Persons with Disabilities (April 1997), available at http://www.privcom.gc.ca/information/02_06_03d_e.pdf (accessed April 22, 2008)

Harmonization between private sector and public sector laws at the federal level, and between federal and provincial legislation, is a laudable goal for the privacy protection regime in Canada wherever possible. Committing government officials to a regular review of the legislation would greatly assist in that regard, as developments at various levels of government could be more easily taken into account.

Ensure the *Privacy Act* Keeps Pace with Rapidly Evolving Technologies and International Trends

The *Privacy Act* serves as the information crux between Canadians and their government; but as with previous reviews, there is a real risk of this legislation fading into irrelevance as new programs, technologies and data practices go unmonitored. A serious, sustained national discussion is now needed to renew the *Privacy Act* for the networked, digital environment that now exists in Canada. Cyberspace was the stuff of science fiction when the *Privacy Act* came into force twenty-five years ago; today the Internet and digital devices shape our identities, professional lives and personal sphere in new ways every day.

In summary, the five-year review requirement would serve three ends. It would help synchronize the Canadian data protection framework across jurisdictions; keep the privacy practices of all organizations, both private and public sector, on the minds of Canadian decision-makers and industry; and it would ensure federal law keeps pace with rapidly evolving technologies and international trends.

Recommendation Number 10:

Strengthen the provisions governing the disclosure of personal information by the Canadian government to foreign states.

Relevant Section(s) of the *Privacy Act*:

Paragraph 8(2) *Subject to any other Act of Parliament, personal information under the control of a government institution may be disclosed . . . (f) under an agreement or arrangement between the Government of Canada or an institution thereof and . . . the government of a foreign state, an international organization of states or an international organization established by the governments of states, or any institution of any such government or organization, for the purpose of administering or enforcing any law or carrying out a lawful investigation.*

Background:

Technological advances over the past two decades have made it much easier and cheaper for governments to collect and retain personal information about their citizens. At the same time, information sharing between nations has increased dramatically as governments have adopted more coordinated approaches to regulating the movement of goods and people and to combating transnational crimes and international terrorism. In particular, enhanced information sharing has been a key strategy in improving intelligence analysis since September 2001.

To cite a few examples: the Canadian Border Services Agency shares customs information and information about travellers entering Canada; the Financial Transaction and Reports Analysis Centre ("FINTRAC") has over 40 agreements with other financial intelligence units to shares information about individuals suspected of engaging in money laundering or terrorist financing; Canada has negotiated Mutual Legal Assistance Treaties (MLATs) with several countries; and law enforcement and national security agencies regularly share information with international counterparts.

However, the *Privacy Act* does not reflect this increase in international information sharing. The *Privacy Act* places only two restrictions on disclosures to foreign governments: an agreement or arrangement must exist; and the personal information must be used for administering or enforcing a law or conducting an investigation. The *Privacy Act* does not even require that the agreement or arrangement be in writing. The *Privacy Act* does not impose any duty on the disclosing institution to identify the precise purpose for which the data will be disclosed and limit its subsequent use by the foreign government to that purpose, limit the amount of personal information disclosed and restrict further disclosure to third parties. Moreover, the *Privacy Act* even fails to impose any basic obligations on the Canadian government institution itself to adequately safeguard personal information.

As reported in the OPC'S 2002-2003 Annual Report, the Office conducted a preliminary review of 21 information-sharing agreements between Canada and the US. It concluded

that only about one-third were reasonably well drafted. To mention just two deficiencies: many of the agreements did not describe the personal information to be shared or include a third party caveat; that is, a statement indicating that the information received under the agreement will not be disclosed to a third party without the prior written consent of the party that provided the information.

Rationale:

Putting in Place Standards for the Sharing of Personal Information

The consequences of sharing personal information without adequate controls are clearly demonstrated in Justice O'Connor's Report on the Factual Inquiry with respect to the *Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar*. Justice O'Connor concluded that it was very likely that, in making the decisions to detain and remove Mr. Arar to Syria, the U.S. authorities relied on inaccurate information about Mr. Arar provided by the RCMP.

The lack of standards governing the sharing of personal information by Canadian officials was also addressed in a January 2008 public hearing as part of work currently being conducted by former Supreme Court of Canada Justice Iacobucci, in the *Internal inquiry into the actions of Canadian officials in relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin*.

Minimizing Risks to Canadians by Clearly Defining Responsibilities

In order to minimize the risks to Canadians resulting from this increased information sharing, the OPC believes that the Government of Canada and Parliament should consider specific provisions to define the responsibilities of those who transfer personal information to other jurisdictions and to address the issue of the adequacy of protection in those jurisdictions.

Prescribing the Form and Content of Information-Sharing Agreements

The Treasury Board Secretariat has developed guidelines setting out elements that a written agreement or arrangement should contain. These guidelines are a positive first step that should be formalized either in legislation or by amending section 77 of the *Privacy Act* to include a provision allowing the Governor-in-Council to make regulations prescribing the form and content of information-sharing agreements.

Limiting Disclosure of Personal information

In addition, paragraph 8(2)(f) should be amended to state that personal information may only be disclosed where the information is required for the purpose of administering or enforcing any law which has a reasonable and direct connection to the original purpose for which the information was obtained.

Reforming the *Privacy Act* – A Chronology of Recommendations

Theme	**Open and Shut: *Enhancing the Right to Know and the Right to Privacy* Report of the Standing Committee of Justice and Solicitor General on the Review of the *Access to Information Act* and the *Privacy Act* (March 1987)**	**The Steps Ahead: Government Response to *Open and Shut: Enhancing the Right to Know and the Right to Privacy* (1987)**	**Government Accountability for Personal Information - Reforming the *Privacy Act* (June 2006)**	**Addendum to Government Accountability for Personal Information: Reforming the Privacy Act (April 2008) & Opening Statement by Jennifer Stoddart, Privacy Commissioner of Canada on *Privacy Act* Reform (April 2008)**
1. Limiting Collection			Amend *Privacy Act* to include a "necessity test" for the collection of personal information. Amend *Privacy Act* to strengthen notice requirements to individuals.	**Amend Privacy Act to include a "necessity test" for the collection of personal information.**
2. Expanding Court Review	Simplify rules of court to allow individuals to seek court review in as simple a manner as possible and that Federal Court should award costs on solicitor-client basis to a successful applicant. Amendment to provide individuals with monetary damages for identifiable harm resulting from unauthorized collection, improper disclosure and denial of access.	No direct response with respect to simplifying rules of court. Creation of civil sanctions in *Privacy Act* not warranted at this time.	Amend the *Privacy Act* to permit Court review of innapropriate collection, use, disclosure of personal information. Amend Act to give Court the power to award damages.	**Amend the Privacy Act to permit Court review of innapropriate collection, use, disclosure of personal information.** **Amend Act to give Court the power to award damages.**
3. Privacy Impact Assessments	Privacy Impact statement requirement for all legislation before Parliament with privacy	Government will not move to require that a PIA accompany each piece of legislation.	Amend *Privacy Act* to require PIAs and public reporting on results of PIAs.	**Amend *Privacy Act* to require PIAs and public reporting on results of**

	implications.			**PIAs.**
4. Research and Public Education Mandate	Amend *Privacy Act* to include public education mandate for Treasury Board and Privacy Commissioner. Amend *Privacy Act* to enable Privacy Commissioner to undertake research studies.	Government will establish public awareness program. Government will amend *Privacy Act* to include public education mandate for Privacy Commissioner. No direct response with respect to research mandate. Government recognized Privacy Commissioner should have public education mandate.	Amend *Privacy Act* to give Privacy Commissioner research and education mandate.	**Amend *Privacy Act* to give Privacy Commissioner research and education mandate.**
5. Communication with Public			Amend the *Privacy Act* to enable the Privacy Commissioner to disclose information on the privacy management practices of government institutions outside the Annual Reporting vehicle.	**Amend the *Privacy Act* to enable the Privacy Commissioner to disclose information on the privacy management practices of government institutions outside the Annual Reporting vehicle.**
6. Discretion in Dealing with Complaints			Amend the *Privacy Act* to give the Privacy Commissioner the discretion to more efficiently and expeditiously deal with complaints which have less systemic and societal significance.	**Amend the *Privacy Act* to give the Privacy Commissioner the discretion to more efficiently and expeditiously deal with complaints which have less systemic and societal significance.**
7. Definition of "Personal Information"	Amend definition of "personal information" to include personal data in any form.	Maintain definition, monitor government surveillance and testing activities.	Amend definition of "personal information" to include unrecorded information.	**Amend definition of "personal information" to include unrecorded information.**

8. Annual Reporting Requirements	Establish hearings to review annual reports of institutions under section 72 of the *Privacy Act.* Amend section 72 of *Privacy Act* to require TBS to prepare a Consolidated Annual Report on annual reports received from government institutions.	No direct response. Government will prepare the consolidated annual report for 1987-1988 fiscal year.	Amend section 72 of the *Privacy Act* to strengthen annual reporting requirements for government institutions.	**Amend section 72 of the *Privacy Act* to strengthen annual reporting requirements for government institutions.**
9. Public Consultation/ Review of Act	Amend section 75(2) of the *Privacy Act* to provide for a second legislative review four years after tabling of Open and Shut.	Government supports ongoing parliamentary oversight, however, Committee should set its own agenda.	Need for broad based public consultation.	**Introduction of a provision in the *Privacy Act* requiring an ongoing five-year parliamentary review of the Act.**
10. Transborder Data Flows	No Amendment to *Privacy Act* recommended, but Government should conduct a review/study of TBDF.	Government agreed.	Amend paragraph 8(2)(f) of the *Privacy Act* to tighten control over information sharing with foreign states. Amend section 77 of the *Privacy Act* to add regulation making power regarding information sharing agreements.	**Amend paragraph 8(2)(f) of the *Privacy Act* to tighten control over information sharing with foreign states.** **Amend section 77 of the *Privacy Act* to add regulation making power regarding information sharing agreements.**