Privacy Commissioner
of Canada

Commissaire à la protection
de la vie privée du Canada

Addendum to *Government Accountability for Personal Information: Reforming the Privacy Act*

April 2008

Office of the Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3

Tel. 613-995-8210, 800-282-1376
Fax 613-947-6850
TDD 613-992-9190

This publication is also available on our Web site at www.privcom.gc.ca.

In June 2006 the Office of the Privacy Commissioner of Canada issued a comprehensive document summarizing the factors driving the need for reform of the federal *Privacy Act*, and setting out general proposals and recommendations for changes to the Act. This addendum provides further comment and substantiation for the position taken by the OPC in 2006 based on events of the past two years.

National Security Issues

Events over the past two years have kept national security issues dramatically at the centre of public attention, with numerous bodies calling for improved oversight of the government's public safety and national security programs. The OPC will continue to urge the government to act on the recommendations that have been made in this regard.

In December 2006 the *Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar* released its "policy report", *A New Review Mechanism for the RCMP's National Security Activities*. In his report, Justice O'Connor made a series of detailed recommendations with respect to the review of the RCMP's national security activities as well as those of other federal departments and agencies. He concluded that "increased information sharing, increased police powers of coercion and increased integration among Canadian and foreign national security actors" requires the creation of a new review agency to oversee the RCMP's national security activities, as well as a new review process for the other federal departments and agencies involved in national security.

Justice O'Connor observed that the case for giving an independent review body the mandate to conduct self-initiated reviews of the RCMP's national security activities is now overwhelming, given the inability of potential complainants to lay complaints, the threat that investigative activities may pose to individual liberties, the lack of judicial or other independent scrutiny, and the need for public confidence and trust in the agency being reviewed.

In his report, Justice O'Connor also observed that the national security environment is complex and multi-stakeholder by nature, with each player subject to its own policy requirements. From the OPC perspective, this reinforces the need to provide a complaint review mechanism that is more comprehensive and citizen-centric. The architecture of oversight (both internal and external) must be commensurate with the apparatus of surveillance. Otherwise, who is watching the watchers?

Similarly, in its main report dated February 2007, *Fundamental Justice in Extraordinary Times*, the Special Senate Committee on the *Anti-terrorism Act* recommended that the government implement more effective oversight of the RCMP. It also recommended the creation of a standing committee of the Senate, with dedicated staff and resources, to monitor, examine and periodically report on matters relating to Canada's anti-terrorism legislation and national security framework on an ongoing basis. The House of Commons Subcommittee on the review of the *Anti-terrorism Act* submitted its report in March 2007, recommending that the Government proceed with legislation to establish a National Security Committee of Parliamentarians responsible for the review of national security matters.

In its July 2007 response to the House of Commons Subcommittee, the government stated that it will propose an approach to national security review that will meet the basic objectives set out in the policy report of the *Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar* and is considering options for an enhanced role for Parliamentarians as a key part of these proposals for an improved national security review framework. There has been nothing further from the Government concerning its specific intentions in this regard.

As the OPC has stated on previous occasions, the Department of Public Safety and Emergency Preparedness (PSEP) should be subject to the highest standards of privacy protection and accountability, with a stronger leadership role assumed by the Minister. This is only appropriate given the extent of personal information collection and processing within that portfolio. It appears that separate parts of that bureaucracy continue to work in isolation from one another.

For example, when one takes a horizontal view of privacy impact assessments generated by the Public Safety portfolio, it is clear that a "whole-of-portfolio" view is not taken. In commenting on the PSEP enabling legislation, to both the department and the Parliamentary Committee, the OPC recommended that a Chief Privacy Officer be statutorily defined. The recommendation was ignored.

The right of individuals to know what information the Government has about them, and the right to insist that the information be appropriate and accurate, is a basic element of the right of privacy. The national security imperatives of the government have been contrary to the principles of fundamental justice by unduly and unnecessarily shielding critical information from the affected individual. The opacity of many National Security initiatives denies the very core of privacy: namely, the right of individuals to control and validate the information that is collected about them by both private and public organizations.

In a February 2007 decision, *Charkaoui v. Canada (Citizenship and Immigration)*, the Supreme Court of Canada found that the security certificate scheme and the detention review procedures under the *Immigration and Refugee Protection Act* infringed the right to life, liberty and security of the person under section 7 of the *Charter*. The secrecy required by the scheme denied the named person the opportunity to know the case against them, and hence to challenge the government's case. The SCC observed that less intrusive alternatives were available, notably the use of special counsel to act on behalf of the named individual. Bill C-3 was tabled by the government in direct response to the Supreme Court decision, providing for a special advocate to perform the challenge function as to the confidentiality, relevance, reliability, sufficiency and weight of evidence. This is a welcome development, and corresponds to recommendations made by the OPC in the context of the review of the *Anti-terrorism Act*.

In November 2007, the Privacy Commissioner of Canada appeared before the *Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182* to comment on the privacy implications of various government programs relating to aviation security, most recently the Passenger Protect Program (the "no-fly list"). The OPC submission to that Inquiry canvassed in depth the circumstances leading to the creation of the PPP, observing that neither the public nor Parliament had a meaningful opportunity to question or challenge the legislation authorizing the Program.

Consistent with the resolution signed by Canada's privacy commissioners and ombudsmen in June 2007, the OPC concluded in its submission that Parliament should review the justification for the program, the operation of the program, the impact on fundamental rights and freedoms and the adequacy of the current legal framework. The submission cited a number of ways in which the *Privacy Act* could be strengthened to provide the public with greater protection and remedies to meet the privacy risks resulting from this type of initiative, including stronger provisions for sharing of personal information with foreign governments, enhanced court review, and a comprehensive accountability framework for national security agencies.

The *Privacy Act* is at the hub of the informational relationship between state agencies and individuals. If the legislative framework that governs this relationship is weak, the entire edifice of accountability is undermined. Privacy is too important to be left to the vagaries of internal policy and management.

In a separate submission to the Air India Inquiry regarding the financial monitoring regime in Canada, the OPC commented that it was encouraged that the need for greater oversight over the operations of FINTRAC has been recognized. The *Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar* called for increased oversight of FINTRAC, as did the Senate Committee which conducted the five-year review of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*. Parliament gave the issue enough weight to amend that Act in December 2006, requiring the OPC to conduct a review every two years of FINTRAC and to report to Parliament.

In February 2008 the OPC tabled its first special report to Parliament, documenting the results of the Office's audit of the RCMP's exempt data banks. These are data banks containing national security and criminal operational intelligence files which are sheltered from public access, depriving individuals of the right to see their own information. The audit confirmed a lack of effective internal controls by the RCMP over these information holdings, finding that more than half of the files examined as part of our audit did not properly belong in the exempt banks. It was evident that greater care was required to ensure that personal information is concealed in an exempt bank only when absolutely necessary. The OPC made a number of recommendations which have been accepted by the RCMP to improve management and internal review procedures concerning these banks. This will ensure greater transparency in the management practices governing Exempt Banks.

The recommendations suggested by the OPC in 2006 for amendments to the *Privacy Act* revolve around creation of a robust privacy management regime, particularly for agencies with a national security mandate, governing all aspects of collection, use and disclosure of personal information. A proper framework requires a full articulation of the fair information principles, with a defined role and accountability structure to frame the privacy leadership responsibilities of the head of the institution, and more stringent reporting requirements to Parliament.

Absent voluntary progress on this front, there is an ever increasing imperative to amend the *Privacy Act* to ensure greater transparency, accountability and oversight over the activities of

national security agencies. Events over the course of the past two years strongly support this position.

Transborder Data Flows

The government's practices with respect to transfers of personal information outside the country have also received a good deal of public scrutiny over the course of the past two years, with active interest being shown by three separate Commissions of Inquiry – the O'Connor Inquiry, the Air India Inquiry, and the Iacobucci Inquiry.

Enhanced information sharing has been a key strategy in improving intelligence analysis since September 2001. Within government departments, between government organizations, from one level or government to another, or from one national government to another, there has been enormous emphasis placed on exchanging more information to enrich the work of analysts and policy makers. Unfortunately, privacy and data security safeguards have lagged behind as sharing of data has quickened.

In September 2006, the *Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar* released its report on the Factual Inquiry. 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 information about Mr. Arar provided by the RCMP, and that the RCMP had provided American authorities with information about Mr. Arar which was inaccurate. Justice O'Connor noted that this inaccurate information had the potential to create serious consequences for Mr. Arar in light of American attitudes and practices at the time.

Numerous recommendations were made in that report addressing the RCMP's national security activities and the information sharing practices of other government agencies. Of particular interest in the context of *Privacy Act* reform were the following:

- The RCMP should establish internal controls to ensure that it stays within its law enforcement mandate when conducting investigations and collecting information, and that it respects the distinct role of CSIS relating to threats to the security of Canada;

- The RCMP's agreements or arrangements with other entities in regard to intergrated national security operations should be reduced to writing;

- Training for national security investigators should include a specific focus on practices for information sharing with the wide range of agencies and countries that may become involved in national security investigations;

- The Minister responsible for the RCMP should continue to issue ministerial directives to provide policy guidance to the RCMP in national security investigations, given the potential implications of such investigations;

- A centralized unit with expertise in national security investigations (such as the Criminal Intelligence Directorate) should have responsibility for oversight of

information sharing related to national security with other domestic and foreign departments and agencies;

- The RCMP should ensure that when sharing information with foreign and domestic agencies it does so in accordance with clearly established policies respecting screening for relevance, reliability and accuracy;

- The RCMP should never share information in a national security investigation without attaching written caveats in accordance with existing policy, specifying precisely which institution may have access to the information and what use may be made of the information; and

- Other Canadian agencies that share information relating to national security should ensure that their information-sharing policies conform to the appropriate extent with the recommendations made to the RCMP.

Of equal interest is the 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*. In January 2008 the Inquiry held a public hearing about the standards that ought to have governed the sharing of information by Canadian officials with foreign entities at the relevant time. The *Privacy Act* was not identified by any of the parties as a legal standard that governed the international sharing of information by CSIS and the RCMP. The fact that the *Privacy Act*, despite its direct application to matters pertaining to accuracy and sharing of information in this case, received no meaningful attention is evidence of the compelling need for legislative reform. Simply put, the antiquated nature of the *Privacy Act* renders it of little significance to the public debate on security and privacy in Canada. This puts privacy at a considerable disadvantage.

In June 2006 the OPC reported on significant risks to privacy stemming from the information sharing practices of the Canada Border Services Agency. The OPC found that the CBSA did have systems and procedures in place for managing and sharing personal information with other countries. However, significant opportunities exist to better manage privacy risks and achieve greater accountability, transparency and control over the trans-border flow of data. For example, many of the information exchanges are verbal, and are not based on written requests, contrary to CBSA policy and the terms of the relevant Canada–US agreement. The Agency could also not with a reasonable degree of certainty, report either on the extent to which it shares personal information with the United States, or how much and how often it shares this information. Overall, the OPC concluded that the CBSA requires a comprehensive privacy-management framework to guide improvements to privacy related policies, systems, procedures and practices, including strengthening the monitoring of the day-to-day information handling practices.

Another instance of cross-border data exchange has been the Government's recent support for provincial Enhanced Driver's License (EDL) programs. These new forms of identification are designed to speed processing of travellers at Canada-US border points. Provincial licensing authorities issue the licenses but provide CBSA with the data of program participants; this data can then be accessed by US Customs and Border Protection personnel from CBSA servers whenever an EDL holder approaches a US border point. The OPC has urged the government to take privacy protections more seriously, asserting that verbal requests and administrative

agreements are simply not rigorous safeguards to meaningfully protect personal information in a networked, digital world.

A long list of recent data breaches in government departments across the US, UK and Canada make one point painfully clear: privacy protection cannot be left to chance, casual exchanges, vague policy memoranda and sloppy management practices. Strong, clear legislation is needed to set rules and boundaries. It is evident that the *Privacy Act* does not currently provide any assistance at all to government departments in managing their information sharing practices and agreements with foreign partners. While there has been cogent response from the Treasury Board Secretariat in the form of guidance on information sharing, privacy breach guidelines and a privacy risk assessment process for government outsourcing, more work is still needed. Until the Act is amended to provide an articulated control framework, it can be anticipated that results will continue to be uneven between departments, and that errors will continue to be made at potentially great cost to the affected individual.

Breach notification

As outlined above, it has been forcefully argued that government should hold itself to standards similar to those it sets for industry. This speaks to credibility, policy coherence and good governance. Data protection and privacy compliance is no exception. How government institutions handle, protect and share personal information should set a clear example to other organizations in other areas of the economy.

An emerging example of this harmonization is the area of data breaches. Currently, federally regulated public sector and private sector organizations are subject to *guidelines* which detail how they should deal with data breaches. However, these instruments are voluntary, non-binding, without basis in legislation and with no demonstrable sanctions for non-compliance. Enshrining these provisions into law would greatly strengthen privacy protections for individuals in Canada. In fact, Industry Canada has begun a consultative process to do precisely this for Canadian private sector organizations. In the not too distant future *Personal Information Protection and Electronic Documents Act* (PIPEDA), Canada's private sector privacy legislation, will in all likelihood carry requirements for the notification of individuals by organizations experiencing a data breach.

Similarly, the Treasury Board Secretariat (TBS) last year published its *Guidelines for Privacy Breaches*, covering the improper or unauthorized access to or disclosure of personal information as defined in the *Privacy Act*. While many of the process details run parallel to the breach guidelines in place for the private sector, they remain provisional and administrative. The President of the Treasury Board, as the designated Minister under the *Privacy Act*, is responsible for such guidelines. This means, while they are general requirements under the *Privacy Act*, they do not carry the full weight and onus of the law. It is the view of the OPC that these requirements should be incorporated into the Act itself.

Privacy Act Coverage

Following passage of the *Federal Accountability Act* in December 2006, the coverage of the *Privacy Act* was greatly extended, resulting in current coverage of about 250 federal departments, foundations, agents of Parliament and Crown Corporations. This has added significant complexity and serious challenges to the OPC role in assessing privacy impacts within government, while at the same time necessitating more staffing and training for departmental staff responsible for *Privacy Act* compliance.

Privacy can be an extremely challenging file – the legal, technological and operational implications for programs can be profound. The OPC is currently engaged in discussions with Treasury Board Secretariat (TBS) and the Canada School of Public Service (CSPS) on a curriculum to support better privacy management across the Public Service of Canada. It is the view of the OPC that this curriculum should be mandatory for all government employees, from senior officials to line employees and managers.

All managers and executives are now required to have financial and human resource management training. Personal information management training should also be mandatory. The OPC believes that this learning curriculum should be integrated within a broader framework to include access to information and information management. The OPC is willing to work cooperatively with TBS and CSPS and lend its expertise to inform the development of this program.

Changes of Immediate Benefit to the *Privacy Act*

Clearly a comprehensive review and re-write of the *Privacy Act* is required. There are however a number of immediate changes that could be made to the Act that would be relatively straightforward and would be of great benefit. Some of these changes would merely incorporate into the law existing Treasury Board policies. In other cases, some of the changes would correspond either to existing provisions in the PIPEDA or to changes anticipated in the context of PIPEDA Review.

These include:

1. Creating a legislative requirement for government departments to demonstrate the necessity for collecting personal information. This necessity test already exists in Treasury Board policy, as well as in PIPEDA and is recognized internationally. For example, the European Union requires that personal data be collected for specified, explicit and legitimate purposes and that it cannot be excessive in relation to the purposes of collection. The collection must be reasonable and there must be a demonstrable need for each piece of personal information collected.

2. Broadening the Federal Court review to all grounds under the *Privacy Act*, rather than being limited to denial of access as is currently the case. This would correspond to the current approach in PIPEDA.

3. Enshrining into law the obligation of Deputy Heads to carry out Privacy Impact Assessments prior to implementing new programs and policies, including a requirement to submit the PIA for review by the OPC, and requiring public disclosure of PIA results, subject to national security constraints.

4. Enunciating a clear public education mandate. This would be consistent with the current provisions in PIPEDA. Canadians need to know what their government is doing with respect to their personal information. The OPC can actively contribute to informed public debate if a clear public education mandate is enshrined in legislation.

5. Providing greater flexibility for the OPC to publicly report on the government's privacy management practices, rather than being limited to the current mechanisms of annual and special reports. PIPEDA enables the OPC to disclose information about an organization's personal information management practices where this is in the public interest.

6. Providing discretion for the OPC to more efficiently and expeditiously deal with complaints which have less systemic and societal significance, enabling the OPC to invest more resources in complaints that will have a significant impact on improving the state of personal information management across the federal government.

7. Aligning the *Privacy Act* with PIPEDA by eliminating the restriction that the *Privacy Act* applies only to recorded information, thereby excluding from the Act unrecorded information such as the collection, use and disclosure of biological samples (including DNA).

8. Strengthening the annual reporting requirements under section 72 of the *Privacy Act*, to require government institutions to report to Parliament on a broader spectrum of privacy management responsibilities, including those under Treasury Board policies on Privacy Impact Assessments and Data Matching.

Conclusion

The entire framework of the *Privacy Act* needs to be revisited in accordance with our June 2006 proposals. On a more immediate basis, there are a number of relatively straightforward changes that could be made to the Act that would greatly advance the cause of privacy in Canada. These changes would bring the standards of the *Privacy Act* into alignment with more modern data protection legislation.

It is inarguable, based on events of the past two years, that a stronger, updated *Privacy Act* could have been instrumental in guiding government institutions and potentially even preventing many lapses which occurred. Instead, we have received no reaction or interest from Government in the two years since we issued our June 2006 proposals for reform.

We commend the House of Commons Standing Committee on Access to Information, Privacy and Ethics for its leadership in opening this important discussion.