THE CANADIAN BAR ASSOCIATION
L'ASSOCIATION DU BARREAU CANADIEN

Privacy Act Reform

CANADIAN BAR ASSOCIATION

June 2008

500-865 Carling, Ottawa, Ontario, Canada K1S 5S8
tel/tél. : 613.237.2925 **toll free/sans frais :** 1.800.267.8860 **fax/téléc. :** 613.237.0185 **info@cba.org** **www.cba.org**

TABLE OF CONTENTS

PREFACE

The Canadian Bar Association is a national association representing 37,000 jurists, including lawyers, notaries, law teachers and students across Canada. The Association's primary objectives include improvement in the law and in the administration of justice.

This submission was prepared by the Canadian Bar Association, with assistance from the Legislation and Law Reform Directorate at the National Office. The submission has been reviewed by the Legislation and Law Reform Committee and approved as a public statement of the Canadian Bar Association.

Privacy Act Reform

I. INTRODUCTION

The Canadian Bar Association (CBA) is pleased to contribute to the Standing Committee on Access to Information, Privacy and Ethics study on reform of the *Privacy Act*. The *Privacy Act* was passed in 1982 and is showing its age. Technological and societal changes since its enactment have significantly diminished its effectiveness in affording privacy protection to Canadians. The CBA believes that comprehensive reform of the *Act* is warranted, and important changes are required to ensure that the *Privacy Act* will fulfill its objectives into the future.

The *Privacy Act* is the primary legislation dealing with personal information held by federal public sector institutions. However, the *Act* lags behind other privacy legislation, including that governing information in the private sector. This is a serious concern given the nature and extent of personal information held by federal institutions. In 2004, the CBA's National Council urged the federal government to strengthen its privacy legislation, practices and policies by establishing strict safeguards and mechanisms for accountability and public oversight, to balance privacy and individual liberties with a demonstrated need for the information and to limit state intrusion into the lives of people in Canada to the greatest extent possible. In 2006, CBA's National Council urged the federal government to initiate a comprehensive consultation and review process to modernize the *Privacy Act* to increase the privacy protection it affords to Canadians.[1] We commented that the collection, use and disclosure of personal information by federal institutions should be balanced and well-considered to minimize the infringement of personal privacy and civil rights in a free and democratic society. We noted several deficiencies in the *Privacy Act*, including limitations in its scope, limitations of the right of access, the extent of permitted disclosures by federal institutions, limited enforcement powers for the Privacy Commissioner of Canada (federal Privacy Commissioner) and limited available remedies.

---

1 Canadian Bar Association, Resolutions 04-05-A, 04-06-A, and 06-03-A.

The Standing Committee has framed its review of the *Privacy Act* around ten recommendations from the federal Privacy Commissioner. While this targeted review of certain key issues is not the comprehensive review that the CBA urged, we believe it is an important step. Given the abbreviated time for the study, we have not addressed all ten suggested issues in great detail. We begin with two additional points that also warrant the Standing Committee's consideration.

II. GENERAL DUTY TO PROTECT PERSONAL INFORMATION

The CBA believes that the *Privacy Act* should impose a general duty on federal institutions to protect personal information in their possession or under their control.[2] The duty to safeguard personal information is one of ten fair information practices that serve as the basis for privacy laws in Canada: "Personal information shall be protected by security safeguards appropriate to the sensitivity of the information."[3] The *Privacy Act* should explicitly impose a fundamental responsibility on federal institutions to safeguard the personal information entrusted to them.

RECOMMENDATION:

The Canadian Bar Association recommends that the *Privacy Act* impose a general duty on federal institutions to protect personal information that they hold, with safeguards appropriate to the sensitivity of the information.

III. DATA MATCHING AND SHARED SERVICES

Data matching has potential to pose a significant privacy risk to personal information held by institutions bound by the *Privacy Act*. Data matching typically involves cross referencing discrete information databases to identify individuals who might be of interest for some reason distinct from that governing the original collection of the information.

Calls for more effective controls on data matching began soon after the introduction of the *Privacy Act*. Just four years after it came into force, a House of Commons Committee recommended that the *Act* be amended to ensure that personal records could be linked only when demonstrably

---

2 Section 6(2) of the *Privacy Act* requires a government institution to take "…all reasonable steps" to ensure that personal information is accurate, current and complete. Clause 71(1)(a) requires the Minister to ensure personal information banks are maintained and managed to ensure compliance with right of access by individuals. These provisions do not convey the responsibility federal institutions should be under to protect personal information.

3 *Personal Information Protection and Electronic Documents Act*, 2000, c. 5, Schedule 1, Principle 7.

necessary and under oversight of the federal Privacy Commissioner.[4] As the Privacy Commissioner noted in the 2004-05 Annual Report to Parliament:

> Although government use of data matching (or "computer-matching") arguably poses the greatest threat to individuals' privacy, the *Privacy Act* is silent on the practice. Privacy Commissioners (bolstered by Parliamentary Committees) have all recognized the dangers inherent in excessive and unrelated data collection. All have recommended amending the *Privacy Act* to ensure that government institutions link personal records in discrete systems only when demonstrably necessary, and under the continued vigilant oversight of the Privacy Commissioner of Canada. The recommendations have not been followed through. The same report noted that the federal Treasury Board had issued guidelines in 1989 outlining the steps departments should take before matching data, including submitting a detailed proposal for the Privacy Commissioner's review. However, the Office of the Privacy Commissioner reported that it had received few notices, despite the likely frequency of the practice.[5]

In the public sector, rules that limit the use of personal information to the purpose for which it was obtained or for a "consistent purpose"[6] arguably also limit data matching. Most provincial and territorial public sector privacy statutes deal with data linkage or data matching in the context of disclosures of personal information without consent for research purposes. These statutes typically include a condition that disclosure may only occur if the linkage would not likely harm the individuals to whom the personal information pertains, and the benefit to be derived from the linkage and research would be in the public interest.

Some Canadian jurisdictions require prospective matches to first be assessed to ensure compliance with legislative requirements for privacy protection, mainly in the area of health-related information. Alberta's *Health Information Act* defines data matching as "the creation of individually identifying health information by combining individually identifying or non-identifying health information or other information from two or more electronic databases, without the consent of the individuals who are the subject of the information."[7] That *Act* requires a privacy impact assessment (PIA) to be completed and the province's Privacy Commissioner to be notified of any proposed data matching.

---

4 As cited in a 1995 speech by Privacy Commissioner, Jennifer Stoddart, "Privacy and Technology: More Action Needed", a speech delivered at Sixth Annual Access to Information and Privacy Conference: Technology - Enhancing or Undermining Democracy? (Ottawa: April 20, 2005).

5 Office of the Privacy Commissioner of Canada, "Identity, Privacy and the Need of Others to Know Who You Are: A Discussion Paper on Identity Issues" (Ottawa: Sept., 2007) at 36-37. http://www.privcom.gc.ca/information/pub/id_paper_e.pdf

6 See, for example, Ontario's PIPA, s. 41(1)(b).

7 Section 1(1)(g).

In Québec, *An Act respecting access to documents held by public bodies and the protection of personal information* requires either a "favourable" opinion from the provincial Commissioner or government approval of the proposed data matching.[8] Ontario's *Personal Health Information Protection Act* requires the Minister of Health to submit a proposal to the province's Privacy Commissioner before matching de-identified personal information by a health data institute and allows the Commissioner to review and comment on the proposal.[9]

We see no apparent reason for this level of protection to be confined to personal health information. In our view, the *Privacy Act* should be amended to allow federal institutions to engage in data matching only where demonstrably necessary, and under the ongoing oversight of the federal Privacy Commissioner. The amendment should be broad enough to include shared services within government and the trend toward merging government databases, which is a form of data matching.

RECOMMENDATION:

The Canadian Bar Association recommends that the *Privacy Act* be amended to permit federal institutions to link personal records in computer systems only if the linkage would not reasonably be expected to harm individuals whose information is being disclosed and if the benefits to be derived from the linkage/research are in the public interest or where demonstrably necessary, and under the ongoing oversight of the federal Privacy Commissioner.

The details of an assessment regarding data matching may already be part of a PIA process, depending on whether the data matching activity is seen to fall within the proposed requirement for a PIA. Given evolving technologies, particular circumstances that should trigger a data matching review may be difficult to articulate. We suggest that considerations for an assessment, including the authority for the data match, notification to affected persons, data retention and security would be best contained in regulations to the *Privacy Act*. The federal Privacy Commissioner should review such assessments, and similar to PIAs, they should be publicly available in summary form.

---

8 R.S.Q., A-2.1.

9 See section 47 of *Personal Health Information Protection Act*, S.O. 2004, c. 3.

IV. ISSUES IDENTIFIED BY FEDERAL PRIVACY COMMISSIONER

A. Necessity Test (Recommendation 1)

Under the *Privacy Act*, the only restriction on collecting personal information is that it be "directly relevant" to the operating programs of the public body collecting the information. Our experience is that this offers weak protection, as information can often be described to appear relevant to the goals of a program.

RECOMMENDATION:

The Canadian Bar Association recommends that the *Privacy Act* be amended to require federal institutions to identify the specific purpose for collecting personal information and to ensure that the information is necessary for the articulated purpose or is authorized by law.

Simply put, the federal government should not compile personal information about Canadians unless it has been shown to be necessary or authorized by law. The ideal should be the Canadian Standards Association *Model Code for the Protection of Personal Information* which is already used as the standard in PIPEDA, and requires that organizations limit collection, use and disclosure of personal information to that which is reasonably necessary. Privacy laws developed or substantially amended since the introduction the *Privacy Act* generally include such a requirement. For example, the *Freedom of Information and Protection of Privacy Act* (Alberta) states:

> 33. No personal information may be collected by or for a public body unless:
>
> (a) the collection of that information is expressly authorized by an enactment of Alberta or Canada,
>
> (b) that information is collected for the purposes of law enforcement, or
>
> (c) that information relates directly to and is necessary for an operating program or activity of the public body.

Similarly, the *Freedom of Information and Protection of Privacy Act* (Ontario) provides:

> 38(2) No person shall collect personal information on behalf of an institution unless the collection is expressly authorized by statute, used for the purposes of law enforcement or necessary to the proper administration of a lawfully authorized activity.

This recommended amendment would require the government institution to inquire first whether the desired information is in fact necessary for its programs. If not, common sense and general respect for privacy principles suggest that the information should not be collected at all.

B. Role of the Federal Court (Recommendation 2)

The *Privacy Act* provides limited judicial oversight. Under section 41 of the *Privacy Act*, the Federal Court may only review a refusal by a federal institution to grant access to personal information requested by an individual under section 12 of the *Act*. Other legal restrictions on what a government institution can collect, how it can be used and when it can be disclosed are provided as citizens' legal rights in their dealings with government, but these rights are of significantly reduced value without a clear remedy. The federal Privacy Commissioner has an ombudsperson role, so no actual mechanism is available for an individual to require a federal institution to follow the law. The possible embarrassment of being named by the federal Privacy Commissioner in a public report provides insufficient redress.

RECOMMENDATION:

The Canadian Bar Association recommends that the Privacy Act be amended to provide Federal Court oversight and a remedy for individuals with grievances under the Act.

Federal Court oversight would provide interpretations of the legislation to guide the federal government in meeting its lawful requirements.

C. Privacy Impact Assessment (Recommendation 3)

The federal Privacy Commissioner suggests that:

> Parliament could enshrine into law the obligation of Deputy Heads to carry out *Privacy Act* Assessments (PIA) 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.[10]

The CBA supports this recommendation which would address the need to specifically develop PIAs under the *Privacy Act*. Further details, for example when PIAs should be conducted, the timing of the PIA, the scope, form and substance of the PIA and material elements of the federal

---

[10] Privacy Commissioner of Canada, "Proposed Immediate Changes to the *Privacy Act*"- Appearance before the Standing Committee on Access to Information, Privacy and Ethics on the *Privacy Act* Reform: Recommendations, April 29, 2008, online: http://www.privcom.gc.ca/parl/2008/parl_080429_02_e.asp [Commissioner Recommendations].

Privacy Commissioner's review process, could be included in regulations to the *Act*. Regulations would facilitate future amendment as required, and could be further supplemented by guidelines from the federal Privacy Commissioner. For confidentiality and security reasons, we recommend that only a summary of the PIA be made publicly available.

RECOMMENDATION:

The Canadian Bar Association recommends that the *Privacy Act* be amended to require public bodies to conduct PIAs prior to the development of any new programs and policies which involve the collection, use or disclosure of personal information.

PIAs should be initiated as early as possible in the design phase of any system involving personal information, and completed well in advance of the target for implementing the system. Although this requirement is arguably already in place under the Treasury Board's "Guidelines for Privacy Breaches" [11](Treasury Board Guidelines), we believe that it merits the heightened attention of specific inclusion in the *Privacy Act*.[12] Consideration should also be given to enforcement of this duty, either through the Federal Court or through audit review.

D. Public Education (Recommendation 4)

The CBA supports the recommendation of the federal Privacy Commissioner that the *Privacy Act* be amended to give the Commissioner a clear public education mandate. Many public sector privacy statutes authorize commissioners to engage in public education.

E. Reporting by Federal Privacy Commissioner and Government Bodies (Recommendations 5 and 8)

The federal Privacy Commissioner made two related recommendations pertaining to the obligations of federal institutions (including the Commissioner) to report upon personal information handling practices.[13] Recommendation 5 would give the federal Privacy Commissioner greater discretion to make public reports on the privacy management practices of

---

[11] Treasury Board of Canada Secretariat, "Guidelines for Privacy Breaches", online: http://www.tbs-sct.gc.ca/atip-aiprp/in-ai/in-ai2007/breach-atteint_e.asp; see also e.g. Ontario Information and Privacy Commissioner, "What to do if a privacy breach occurs: Guidelines for government organizations", online: www.ipc.on.ca/images/Resources/up-prbreach.pdf

[12] Reference can also be made to the Alberta Commissioner's experience with mandatory PIAs under the *Health Information Act*.

[13] *Supra*, note 9 - Commissioner Recommendations.

federal institutions, and recommendation 8 would strengthen the annual reporting requirements of federal institutions by requiring them to report to Parliament on a broad spectrum of privacy-related activities.

In regard to recommendation 5, the federal Privacy Commissioner observed that there is no specific section authorizing her to make public interest disclosures under the *Privacy Act*:

> 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.[14]

The CBA supports the intent underlying these two recommendations, but cautions that they are likely to have limited impact. The current reporting obligations for federal institutions leave much to be desired, particularly where a federal institution has experienced a privacy breach and personal information has been inadvertently or improperly disclosed. There is simply no "real time" obligation upon federal institutions or the Commissioner to advise individuals affected by a breach so they may take appropriate steps to mitigate possible adverse consequences.[15]

For example, under sections 38 and 39 the federal Privacy Commissioner may issue an annual report or special report about matters relating to the *Privacy Act*. However, the reports must first be tabled in the Senate and House of Commons, which limits their timeliness. Also, section 63 prevents the Commissioner from disclosing any information arising from the performance of her duties and functions under the *Privacy Act*, which may limit the Commissioner's ability to facilitate notification of individuals affected by a government institution's privacy breach.

Section 72 obliges federal institutions to prepare an annual report "on the administration of this *Act* within the institution." Only a strained interpretation would suggest this obliges a government institution to notify individuals affected by a privacy breach. Because reports are laid before

---

[14] *Ibid.*

[15] The Commissioner has published a number of guidance documents on how to prevent identity theft, as well as what can be done if an individual is an identity theft victim - See Privacy Commissioner of Canada, "Key Issues: Identity Theft," online: http://www.privcom.gc.ca/keyIssues/ki-qc/mc-ki-idt_e.asp

Parliament while sitting, notification may well be too late to assist an affected individual wishing to mitigate possible consequences. In any event, the recently updated privacy reporting guidelines for federal institutions[16] do not include any explicit requirement to describe privacy breach occurrences in their annual report, or to set out what notification steps were taken by the institution.

The inadequacies of the reporting mechanisms of the *Privacy Act* are clearly a matter of concern for an inadvertent privacy breach involving personal information. Unfortunately, examples of privacy breaches by government entities are not hard to find.[17]

Currently, the *Privacy Act* places no obligation for a federal government institution to notify affected individuals of a privacy breach. The Treasury Board Guidelines lack the force of legislation and obligations toward an affected individual can easily be overlooked. Indeed, in the Treasury Board's recently published Policy on Privacy Protection[18], the documents listed under "Related policies and guidelines" include no reference to the Treasury Board Guidelines, nor is there any indication in the Policy on Privacy Protection that the government institution should consider obligations towards affected individuals in the event of a privacy breach.

A statutory breach notification requirement for private sector companies has been subject to vigorous debate recently in the statutory review of the *Personal Information Protection and Electronic Documents Act* (PIPEDA).[19] However, the Commissioner's recommendations for changes to the *Privacy Act* do not contain an explicit recommendation for a parallel statutory breach notification requirement upon a government institution that suffers a privacy breach.

---

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

17 See e.g. Kenyon Wallace, "Passport applicant finds massive privacy breach", *The Globe and Mail* (04/12/07), online: http://www.theglobeandmail.com/servlet/Page/document/v5/content/subscribe?user_URL=http://www.theglobeandmail.com%2Fservlet%2Fstory%2FRTGAM.20071204.wpassport1204%2FBNStory%2FNational%2Fhome&ord=21746931&brand=theglobeandmail&force_login=true; see also Jonathan Fowlie, "Privacy breach 'a wake-up call': Sale of tapes by the provincial government exposes personal information and health records", *Vancouver Sun* (04/03/06), online: http://www.canada.com/vancouversun/news/story.html?id=ee7c35fb-1ae4-4140-9a82-bab28269ef2d

18 Online: http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/CHAP1_1-1_e.asp - published on April 24, 2008 by Information Notice 2008-09 (http://www.tbs-sct.gc.ca/atip-aiprp/in-ai/in-ai2008/2008-09-in-ai_e.asp)

19 See Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics (May 2007), online: http://cmte.parl.gc.ca/cmte/CommitteePublication.aspx?COM=10473&Lang=1&SourceId=204322, as well as the Government Response that was presented to the House of Commons on October 17, 2007 (Government Response), online: http://cmte.parl.gc.ca/cmte/CommitteePublication.aspx?COM=10473&Lang=1&SourceId=215982

The debate around a possible breach notification amendment to PIPEDA has shown that drafting an amendment would not be easy. Some important considerations are: (i) the number of individuals impacted, (ii) the sensitivity of the information involved, and (iii) the probability that information was improperly accessed. In addition to the criteria for notification or reporting, other considerations for a notification model include (a) the content of reports to the Commissioner, (b) penalties for failure to notify, (c) the ability of the Commissioner to make information public, and (d) the timing and notification of credit reporting agencies.[20] An amendment that appropriately balances all the necessary considerations and is workable in practice will require careful drafting.

The Government's Response to the Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics in regard to PIPEDA acknowledged that the details of a breach notification model will be critical and that "[r]esearch, analysis and consultation will be required to arrive at the best model for Canada." The Response stated:

> An important part of consultations will pertain to specifics for the purpose of developing effective and practical notification parameters as well as for the purpose of determining whether specific offences are appropriate. The issues considered will include the timing, form, content and mode of notification to individuals, and in addition, identification of which organizations, such as credit bureaus, should be notified in addition to the Privacy Commissioner. Clearly defined, industry-wide guidelines and standards would be particularly useful to SMEs that may lack the internal resources necessary to make notification assessments.[21]

The CBA is aware that Industry Canada has been consulting about a breach notification model for PIPEDA, and amendments to that legislation are anticipated in the near future. The federal Privacy Commissioner has also commented that:

> [I]t 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

---

[20] See CBA's Privacy and Access Law Section submission on *Five Year Review of the Personal Information Protection and Electronic Documents Act* (Ottawa: CBA, 2006).

[21] *Supra*, note 18, Government Response.

> demonstrable sanctions for non-compliance. Enshrining these provisions into law would greatly strengthen privacy protections for individuals in Canada. […]
>
> [T]he 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.[22]

The CBA believes that a breach notification regime is required for federal institutions under the *Privacy Act*. Such a regime should adopt a balanced approach taking into account all relevant factors at play,[23] and be at least as stringent as any regime adopted under PIPEDA. Private businesses, including small or medium sized enterprises, should not be held to a higher standard than the federal government.

RECOMMENDATION:

The Canadian Bar Association recommends that the *Privacy Act* be amended to contain a breach notification requirement requiring federal institutions to notify individuals if their personal information has been improperly disclosed. Such a requirement should adopt a balanced approach, and be at least as stringent as any breach notification regime imposed on private businesses under PIPEDA.

F. Discretion to Refuse or Discontinue Privacy Complaints (Recommendation 6)

The CBA supports the federal Privacy Commissioner's recommendation to give her Office discretion to refuse or discontinue complaints. A provision comparable to section 13(2) of PIPEDA could be added to the *Privacy Act* to authorize the Commissioner *not* to prepare a report in specified circumstances.

---

22 Privacy Commissioner of Canada, "Addendum to Government Accountability for Personal Information: Reforming the *Privacy Act*" (April 2008) (online: http://www.privcom.gc.ca/information/pub/pa_ref_add_080417_e.asp)

23 This balanced approach is discussed in detail by the CBA's National Privacy and Access Law Section in its 2006 submission on PIPEDA. S*upra*, note 20.

RECOMMENDATION:

The CBA recommends that a section comparable to section 13(2) of PIPEDA be added to the *Privacy Act* so the federal Privacy Commissioner may use discretion not to prepare a report in specific circumstances.

G. Recorded and Unrecorded Information (Recommendation 7)

The *Privacy Act* protects "personal information", defined as information "…about an identifiable individual that is recorded in any form…".[24] The limitation that information be recorded should be reconsidered.

Information about identifiable individuals can be collected, used or disclosed without being recorded. An example would be a biological sample. We see no reason to exclude unrecorded information from the protection of the *Act*. Where federal institutions collect, use or disclose information about an identifiable individual, the privacy of that individual should be protected, whether or not the information is recorded. We note that the French text of law does not appear to be limited to "recorded" information.

RECOMMENDATION:

The CBA recommends that the definition of "personal information" be amended to remove the requirement that personal information be recorded to be protected under the *Privacy Act*.

H. Five Year Statutory Review (Recommendation 9)

The CBA supports the federal Privacy Commissioner's recommendation that the *Privacy Act* be reviewed by a Committee of the House of Commons every five years, as in section 29 of PIPEDA.

I. Information Sharing with Foreign Governments (Recommendation 10)

The CBA believes that the *Privacy Act* should be significantly strengthened to ensure better governance and more effective oversight when personal information is disclosed by the Canadian government to foreign states.[25]

---

[24] Section 3.

Existing Statutory Framework under the *Privacy Act*

Section 3 limits "personal information" to information "that is recorded in any form." The definition otherwise refers to a broad range of personal data including (b) "information relating to the…criminal…history of the individual or information relating to financial transactions in which the individual has been involved."

Section 8 (2) sets out conditions or circumstances when personal information may be disclosed, including:

> (a) for the purpose for which the information was obtained or compiled by the institution or for any use consistent with that purpose,…
>
> (f) under an agreement or arrangement between the Government of Canada or an institution thereof…the government of a foreign state…or any institution of any such government or organization, for the purpose of administering or enforcing any law or carrying out a lawful investigation, …
>
> (m) for any purpose where, in the opinion of the institution
>
> (i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure.

Section 12 (1) – Right of Access

Section 12 (2)(a) Right to request a correction of personal information where the Individual believes there has been an error or omission therein.

Section 12 (2)(c) Right to require that a notation be attached to information where a correction was requested but not made.

Section 22 - Law Enforcement and Investigation

> **22 (1)** The head of a government institution may refuse to disclose any personal information requested under subsection 12(1)
>
> (a) that was obtained or prepared by any government institution, or part of any government institution, that is an investigative body specified in the regulations in the course of lawful investigations pertaining to
>
> (i) the detection, prevention or suppression of crime,
>
> (ii) the enforcement of any law of Canada or a province, or

---

[25] See CBA Resolution 04-06-A, s*upra*, note 1.

(iii) activities suspected of constituting threats to the security of Canada within the meaning of the *Canadian Security Intelligence Service Act*, if the information came into existence less than twenty years prior to the request;

(b) the disclosure of which could reasonably be expected to be injurious to the enforcement of any law of Canada or a province or the conduct of lawful investigations, including, without restricting the generality of the foregoing, any such information

(i) relating to the existence or nature of a particular investigation,

(ii) that would reveal the identity of a confidential source of information, or

(iii) that was obtained or prepared in the course of an investigation; or

(c) the disclosure of which could reasonably be expected to be injurious to the security of penal institutions.

22 (2) - Policing services for provinces or municipalities

The head of a government institution shall refuse to disclose any personal information requested under subsection 12(1) that was obtained or prepared by the Royal Canadian Mounted Police while performing policing services for a province or municipality pursuant to an arrangement made under section 20 of the *Royal Canadian Mounted Police Act*, where the Government of Canada has, on the request of the province or municipality, agreed not to disclose such information.

Definition of "investigation"

(3) For the purposes of paragraph (1)(b), "investigation" means an investigation that

(a) pertains to the administration or enforcement of an Act of Parliament;

(b) is authorized by or pursuant to an Act of Parliament; or

(c) is within a class of investigations specified in the regulations.[26]

Operation of the Act in Relation to Personal Information, Law Enforcement, and Trans-Border Data Sharing

The above provisions show that individuals have no right to access their personal information held by a federal institution obtained for law enforcement and investigation purposes. Without that right, the individual cannot review the information for accuracy or seek to have inaccuracies or

---

[26] 1980-81-82-83, c. 111, Sch. II "22"; 1984, c. 21, s. 90, c. 40, s. 79.

omissions corrected. A federal institution may disclose the information to a foreign government or an institution of a foreign government on the basis of mere "arrangements", for example, between a policing agency and a foreign government.

The Arar Commission Report

The case of Maher Arar illustrates the risks and complexities associated with intelligence gathering by law enforcement agencies, sharing data between different agencies within Canada and abroad, and the great harm that can arise when systems fail. As the findings and recommendations of Commissioner Dennis O'Connor[27] are relevant to this review of the *Privacy Act*, we reference them in some detail.

What is now referred to as "intelligence-led" policing[28] has the potential to result in a vast amount of information being collected, not all of which is verified or even verifiable as to its accuracy. Commissioner O'Connor wrote:

> From the RCMP's standpoint, intelligence can be understood as information developed to direct police action...it is strategic, tactical and background information that any large organization requires in order to direct its actions and limited resources in an intelligent and focused manner.[29]

Further:

> The gathering of information must not, however, be used to justify the reliance upon information that is inaccurate. "Inaccurate analysis of information and unwarranted assumptions must be avoided, as they may trigger unforeseen chains of events and cause grave damage.[30]

And,

---

27 Commissioner Dennis O'Connor, Commission of Inquiry into the Actions of Canadian Officials in the Case of Maher Arar, "A New Review Mechanism for the RCMP's National Security Activities" (Ottawa: Arar Commission, 2006).

28 *Ibid*. Commissioner O'Connor relied on the RCMP's definition of "intelligence-led policing" at 43:

> ...At its most fundamental, intelligence-led policing involves the collection and analysis of information to produce an intelligence end product designed to inform policy decision-making at both the tactical and strategic levels. It is a model of policing in which intelligence serves as a guide to operations, rather than the reverse. It is innovative and, by some standards, even radical, but it is predicated on the notion that a principal task of the police is to prevent and detect crime rather than simply to react to it.

29 *Ibid.* at 315.

30 *Ibid*. at 325.

> Sharing unreliable or inaccurate information does not provide a sound foundation for identifying or thwarting real and dangerous threats to national security and can cause irreparable harm to individuals.[31]

Commissioner O'Connor observed that the RCMP distinguishes between information (defined as "unprocessed data") and "intelligence".[32] The risks of inaccurate analysis and unwarranted assumptions and the consequent harms are greatest when decisions are based upon information, rather than intelligence.

We suggest consideration be given to how Canada's laws might prohibit, or at least limit the sharing of information which has unknown or unverifiable reliability. Certainly, police forces must rely on their experience and expertise to develop practices and techniques that make policing more effective. At the same time, intelligence-led policing must be conducted within the mandate of the policing agencies – it does not change that mandate. Commissioner O'Connor concluded: "Controls designed to ensure that RCMP activities are properly within its law enforcement mandate are necessary to guarantee respect for the rule of law...".[33]

The combination of increasingly sophisticated police forces, increased vigilance by Canada's law enforcement agencies and increased coordination and widespread sharing of information between those agencies has resulted in an unprecedented volume of personal information being collected by Canadian federal institutions. Commissioner O'Connor wrote:

> Since 9/11, there has been increasing integration of different parts of government involved in national security affairs, both in Canada and elsewhere. The RCMP's integration initiatives with respect to national security matters are not limited to other police forces, but extend to a wide range of other federal departments and agencies. For example, INSET's include representatives of agencies such as the Canada Border Services Agency (CBSA), CSIS, Citizenship and Immigration Canada (CIC) and the Canada Revenue Agency. Moreover, there has been an increased amount of information sharing among a broad range of federal departments and agencies in relation to these types of investigations.[34]

The CBA recognizes the challenge that trans-national crime presents to Canada's law enforcement agencies, but that challenge does not justify unrestricted or unregulated powers. On this point,

---

31 *Ibid.* at 335.

32 *Ibid.* at 325.

33 *Ibid*. at 316.

34 *Ibid*. at 319-320.

Commissioner O'Connor commented that "While police agencies must concern themselves with law enforcement, these agencies should also respect "constraints on their powers and expect that the legality of their actions will be reviewed"". [35] Further, "the increased level of integrated activity makes it essential that there be a clearly articulated framework within which the activity is carried out." [36]

The Arar Commission also addressed the issue of oversight:

> …national security investigations have several features that are different from other criminal investigations. There is a greater need for integration with other agencies, both domestic and foreign; there is more information sharing, often involving sensitive material; there is a greater need for centralized oversight with the RCMP; and there are concerns about individual liberties. Ministerial directives are a useful tool in ensuring that the way the RCMP manages its national security investigations is consistent with ministerial accountability… I also believe that ministerial directives should be readily accessible to the public, subject to valid national security and confidentiality concerns.[37]

The Commission addressed the enforcement of Canada's arrangements with foreign jurisdictions. Though the issue of enforcement is complex, the need for an enforcement mechanism is clear.

> Once information is in foreign hands, it will be used in accordance with the laws of the foreign jurisdiction, which may not be the same as Canadian law. Reducing arrangements to writing, even if only in an exchange of letters, greatly assists in ensuring accountability in decision making and in reviewing integrated activities including information sharing.[38]

Commissioner O'Connor recommended that arrangements with foreign jurisdictions be subject to review and clarified if there are problems. He noted that "respect for human rights cannot always be taken for granted". [39]

Concerns in Relation to Personal Information, Law Enforcement, and Trans-Border Data Sharing

The existing statutory framework under the *Privacy Act* lacks a mechanism for effective and ongoing oversight of the Canadian government and its institutions in relation to trans-border data sharing. The existing statutory framework also does not provide an adequate mechanism for

---

35 *Ibid.* at 314.

36 *Ibid.* at 320.

37 *Ibid.* at 330.

38 *Ibid.* at 321.

39 *Ibid.*

ensuring compliance and accountability. In our view, effective ongoing oversight should be mandatory given the enormous trust placed in and power accorded to the government and its institutions in relation to law enforcement and data sharing. Reasons for this oversight include:

1. an individual will have no opportunity to know when a law enforcement agency has collected data about that individual;
2. if data has been collected, an individual will have no opportunity to learn what that data is, or if it is accurate;
3. 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 it has been shared with;
4. an individual will have no opportunity to know the uses for which the data will be used by a foreign government or institution;
5. an individual will have no opportunity to know if the foreign government or institution will have also shared the data with other foreign governments or institutions;
6. an individual will have no way to know whether the foreign government or institution that has received the data will comply the terms of any "arrangement" under which the data was transferred by the Government of Canada;
7. the data may be used by a foreign government or institution in a manner or for a purpose that significantly jeopardizes an individual and friends or family members;
8. even if an individual knows that a foreign government or institution has breached the terms of the "arrangement' under which the data was transferred, the individual will have no recourse or remedy.

RECOMMENDATIONS:

The Canadian Bar Association recommends that:

- **arrangements for disclosing personal information to a foreign government or institution be written, formal, detailed and public;**
- **arrangements with foreign governments or institutions that do not respect fundamental principles of democracy, human rights and the rule of law be very carefully considered;**
- **a full record be made of the personal information disclosed, the foreign government or institution to which it was disclosed, the arrangement under which it was disclosed and the specific purposes for which it was disclosed;**

- **arrangements under which personal information is disclosed clearly specify and limit the purposes for which the disclosure may be made, with consequences for breach of the terms or conditions of the arrangement;**

- **an independent oversight mechanism ensure effective and ongoing compliance by the Government of Canada and its institutions with the law. Because of the increased cooperation between and integration of operations between government agencies, a single oversight mechanism must have the power to review the disclosures by all federal institutions;**

- **the Government of Canada and its institutions be required by law to notify the independent oversight body of personal information disclosed in a way that does not comply with the law and instances where the foreign government or institution receiving personal information has used, or intends to use the information in a manner inconsistent with the arrangement under which it was disclosed; and**

- **an effective remedy exist for any individual whose personal information has been disclosed to a foreign government or institution in a manner inconsistent with applicable law.**

We believe these recommendations are consistent with an expanded jurisdiction of the Federal Court to both review alleged contraventions of the *Privacy Act* and to grant remedies where the Court finds that the *Act* has been contravened.

V. CONCLUSION

The CBA trusts that our comments will assist in improving the *Privacy Act*. We recognize that there are resource implications to implementing many of our recommendations. Careful consideration should be given to the cost implications of any initiatives to ensure that compliance would be realistic and achievable.

As we offer our comments for this targeted study, we repeat our view that the importance of the *Privacy Act* and its widely recognized deficiencies at present call for a thorough and comprehensive review.