A Matter of Trust:

Integrating Privacy and Public Safety in the 21st Century

A reference Document from the Office of the Privacy Commission of Canada

November 2010

Table of Contents

Executive Summary

This reference document presents a general approach for privacy analysis in relation to the wider policy goals of national security and public safety. The document outlines the analytical framework and basic steps used by the Office of Privacy Commissioner (OPC) when examining legislative initiatives, program proposals or undertaking compliance reviews through our audit and investigation functions. It stems from discussions held with senior federal public servants, practitioners, academics and civil society, and aims to provide guidance when integrating privacy protections with new public safety and national security objectives.

Understanding this framework, however, requires clarity on two legal concepts: first, what is 'personal information' and, secondly, what is a 'reasonable expectation of privacy.' Both key definitions are discussed. Details on four specific stages of consideration for privacy — conception, design, implementation and review — are then presented for the development and implementation of security programs and policies:

Stage one concerns the rationale and justification for collecting personal information when a policy or program is being conceived. This requires considering the 'four part test' used by courts and legal advisors to ascertain whether a law or program can justifiably supersede or intrude upon rights like privacy. The elements of this test: necessity, proportionality, effectiveness and minimization are set out in plain language.

Having established the basis for collection at the conception of a program, **stage two** concerns the proper security, use (such as linkages of data), disclosures and maintenance of information collected. This requires consideration of a second set of internationally recognized standards, the Fair Information Practices, which can guide both commercial and government organizations in program development where personal information is used.

Stage three elaborates on the need for ongoing governance and privacy practices as program operations continue. Concrete examples of these policies and practices are explained, alongside reference to the suite of federal policies and reporting established by the Treasury Board Secretariat (TBS) for privacy and data protection.

The document concludes with external controls — **stage four** — and a series of suggestions for longer-term review and oversight of organizations to ensure privacy and sound personal information handling practices are developed around public safety initiatives.

Introduction

The aim of this document is to present the analytical framework and basic steps used by the Office of Privacy Commissioner (OPC) when examining new public safety measures. The same lens is applied to legislative initiatives, program proposals or undertaking compliance reviews through our audit and investigation functions. It is intended to guide policy makers, practitioners, academics and citizens, when integrating privacy protections with new public safety and national security objectives.

As an independent Officer of Parliament, the OPC provides Parliamentarians with a privacy view on new legislation and program proposals. The Office also reviews the personal information handling practices of all federal government departments. Given that public safety issues have become a central focus by the Government of Canada in recent years, privacy considerations have come increasingly into play during legal and policy debates. Recent events and studies — including a wide-ranging government review of security policies, Canada's hosting of international events like the Winter Olympics and G-8/G-20 summits and the final report of the Major Inquiry into the bombing of Air India Flight 182 — continue to highlight issues around privacy and public safety.

In March 2009, the Office of the Auditor General treated the issues of intelligence and information sharing directly in her Annual Report. It stressed that "for Canadians to have confidence in their security and intelligence organizations, they need to know that government agencies and departments maintain a balance between protecting the privacy of citizens and ensuing national security." The aim of this document is to assist in that challenge.[1]

Given that public safety issues have become a central focus by the Government of Canada in recent years, privacy considerations have come increasingly into play during legal and policy debates.

In integrating privacy concerns within security initiatives, it is useful to consider the perspective articulated by the Australian Privacy Commissioner's, namely that "any lowering of privacy protections ... must be a necessary response to a clearly defined problem, proportionate to the risk posed and accompanied by adequate accountability and review mechanisms."[2] This is a view that the OPC shares. By providing an overarching view — as opposed to a reactive response to program specifics — this document charts broad positions and concerns that should be applicable to any new security initiative.

[1] Office of the Auditor General of Canada, 2009 March Report of the Auditor General of Canada – Chapter 1 — National Security: Intelligence and Information Sharing — URL: http://www.oag-bvg.gc.ca/internet/English/parl_oag_200903_01_e_32288.html#hd4a

[2] Office of the Privacy Commissioner (Australia), *Submission on the Inquiry into the Independent Reviewer of Terrorism Laws Bill* (September 2008), p.2. URL: http://www.aph.gov.au/senate/committee/legcon_ctte/terrorism/submissions/sub06.pdf

Preamble: Privacy and its social value to Canadians

Globally, there is general acceptance that the right to privacy is one of the precursors to sustaining freedom and democracy. This enabling relationship underpins the status of privacy as an international human right. In Canada, it is a recognized right protected under the *Canadian Charter of Rights and Freedoms*. For many countries, protecting this right was the rationale for passing privacy and data protection laws over the past half-century.

Since the establishment of democratic principles, societies have seen it as critically important to put limits on the ability of government to invade private property or an individual's personal space, impinge on their reputation or misuse personal information. Undue intrusion upon the intimate personal lives of citizens is the antithesis of a secure and confident state. Careful checks and balances were created specifically for the purpose of ensuring a wider social space where citizens could enjoy privacy and conduct their personal affairs freely.

Some observers contend that the world has changed — that we need to accept a new reality in which the threats of terrorism and transnational crime loom ever present. Others would argue terrorism, threatened violence and radicalism, are issues that democracies have been combating successfully since their advent. It is this Office's view that, rather than diminishing the centrality of privacy issues, threats of terrorism and organized crime amplify the need for their consideration. As the Chief Justice of Canada noted just a year ago,

> *One of the most destructive effects of terrorism is its ability to provoke responses that undermine the fundamental democratic values upon which democratic nations are built. The fear and anger that terrorism produces may cause leaders to make war on targets that may or may not be connected with the actual terrorist incident. Or perhaps it may lead governments to curtail civil liberties and seek recourse in tactics, like torture, which they might otherwise deplore — tactics that may not, in the clearer light of retrospect, be necessary or defensible.*[3]

The Chief Justice's warning highlights the need for effective oversight and regular reassessment of anti-terrorism and national security programs. Trust and social cohesion are perhaps the first casualties as people put aside either privacy or security in favour of the other. Trust between citizens and their neighbours, as well as citizens and the state, hinges on a mutual understanding or consensus about the need to provide security protection and the need to respect rights like privacy and to preserve the free and democratic society which we all cherish.[4]

Privacy is not simply an individual right or civil liberty; it is a vital component of the social contract between Canadians and their government. Without privacy, without protective boundaries between government and

[3] From "The Challenge of Fighting Terrorism While Maintaining our Civil Liberties" – Remarks of the Right Honourable Beverley McLachlin, P.C. Chief Justice of Canada – URL: http://www.scc-csc.gc.ca/court-cour/ju/spe-dis/bm2009-09-22-eng.asp

[4] Refer also to Daniel J. Solove, "Digital dossiers and the dissipation of Fourth Amendment privacy" in *Southern California Law Review*, 75 (2002), pp. 1083 – 1167. URL: http://ssrn.com/abstract=313301

citizens, trust begins to erode.[5] Good governance requires mutual trust between state and citizen. Otherwise, alienation and a sense of inequality begin to spread, circumstances under which no program for public security can be tenable or effective in the long term. Where citizen trust hits a low point, in fact, such security measures may be undermined, ignored, circumvented — or in the most egregious cases — passively or actively resisted.

A key challenge in the protection of privacy is the rapid development of new technologies. The online tools, devices and systems of the 21st century provide government organizations with enormous ability to acquire and analyse information. In a world where most electronic communication is logged, or transaction recorded, citizens and governments need to work harder to ensure that the rights and autonomy of individuals are not compromised. In the past decade, countries around the world have passed a succession of new security laws to acquire, analyse and exploit the information transiting these digital networks.[6] Technology is indeed evolving, as are the threats, but the manner in which we respond to these changes requires a proactive, protective framework to ensure that our fundamental values, such as privacy, are maintained.

Privacy is not simply an individual right or civil liberty; it is a vital component of the social contract between Canadians and their government. Without privacy, without protective boundaries between government and citizens, trust begins to erode.

[5] For discussion of the role of privacy in fostering trust, social cohesion and solidarity, as opposed to being cast simply as a individual right or civil liberty, see Priscilla M. Regan's 1995 work, *Legislating Privacy: Technology, Social Values and Public Policy*

[6] For overview of recent legislative changes, refer to OPC Backgrounder: Surveillance, Search or Seizure Powers Extended by Recent Legislation in Canada, Britain, France and the United States (Ottawa, 2009) – URL: https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2009/parl_bg_090507/

An analytical framework for privacy and security

Policy makers often point out that the ground around them continues to shift in the context of privacy and security and those new situations constantly call into question these established notions.[7] A series of normative frameworks, policy instruments, statutes and jurisprudence have been adopted to redefine the grounds of privacy:

- passage of the *Protection of Privacy Act* (1974) that created Part VI of the *Criminal Code* to govern wiretapping;
- passage of the Canadian Human Rights Act (1977) which first established privacy as a basic legal right in Canada and created the first Privacy Commissioner;
- adoption of the *Canadian Charter of Rights and Freedoms* (1982);
- debate and passage of the federal *Privacy Act* along with the administrative establishment of the Office of the Privacy Commissioner of Canada (1983);
- landmark privacy cases from *Oakes* (1986) to *Ruby* (2002) and *Tessling* (2004);
- the passage of Canada's private sector privacy law, the *Personal Information Protection and Electronic Documents Act*(2000), which reflects the OECD *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*;
- the broadened application of privacy governance to all Canadian federal organizations under the *Federal Accountability Act* (2006).

Each of these milestones in personal information treatment and regulation has shaped our understanding of what personal information is and when an individual has a reasonable expectation that personal information will remain private. These two basic concepts are discussed below, followed by an outline of how any new security proposal — be it legislation, government program or regulatory initiative — can be systematically reviewed for privacy implications.

What is 'personal information'?

Section 3 of the *Privacy Act* defines "personal information" as any "information about an identifiable individual that is recorded in any form," with the exception of that person's professional contact information (e.g. name, title, business address or telephone number of an employee within an organization). This definition is intentionally broad to allow for greater privacy protection, and Canadian courts have generally been hesitant to circumscribe it. For example, Canadian courts have ruled personal information to include Social Insurance Numbers, email addresses and messages; consumer purchases, service and transaction histories and customer membership and account information. Information can still be considered "personal information" even if it is publicly available. Circulation of personal information in the public domain for one purpose does not lift all privacy restrictions on its indiscriminate collection, use or disclosure for other purposes.

As new technologies emerge, the concept of personal information has expanded. By carrying and communicating through a new generation of connective devices, individuals produce constant data about themselves. This means that even biometric data (such as fingerprints and voiceprints), digital video footage (such as of a person's home or movements), Internet Protocol (IP) address information or geo-location data

[7] Public Policy Forum, The Federal Privacy Regime Roundtable Series – Outcomes Report (March 2008), p. 10-12

(e.g. place points collected from a radio frequency identification tag (RFID) or Global Positioning System (GPS)) could be considered personal information in certain circumstances. Though granular, ambient data points may not necessarily say much about an individual in pure isolation, a clear privacy issue arises when these data streams are generated constantly and/or combined with other data. Indeed, these data trails or emissions can be highly revealing if broadly collected, consolidated into personal profiles and analysed for patterns or behavioural insights.

When is there a reasonable expectation of privacy?

As new technologies emerge, the concept of personal information has expanded. By carrying and communicating through a new generation of connective devices, individuals product constant data about themselves.

Despite not containing the word "privacy", the *Canadian Charter of Rights and Freedoms* protects various privacy rights and interests.

For example, privacy interests have been found to form part of the right to life, liberty and security of the person protected by section 7 of the *Charter*, with respect to control over our bodies and our personal information.[8] The Supreme Court of Canada has suggested that the right to privacy might itself be a principle of fundamental justice,[9] and has recognized that the right to privacy and maintaining the privacy of information about ourselves is an essential aspect of liberty in a free and democratic society.

Some commentators have suggested that various privacy interests are protected under the *Charter*'*s* fundamental freedoms and mobility rights, right to counsel on arrest, right of a witness to keep silent and right to protection against self-incrimination.[10] In Canada, the notion of a "reasonable expectation of privacy" flows from judicial interpretation of section 8 of the *Charter*. Section 8 of the *Charter* protects individuals from unreasonable search and seizure when there is a "reasonable expectation of privacy." As Justice Lebel noted in *R. v. Kang-Brown*, "from the first days of its application, s. 8 evolved into a shield against unjustified state intrusions on personal privacy".

Whether an individual enjoys a reasonable expectation of privacy in any given case involves a contextual evaluation of the specific facts surrounding any particular search, and entails an assessment of subjective and objective elements. The case law has also repeatedly stressed that section 8 protects 'people, not places'. While privacy rights in Canada have historically focused on conceptions of protecting property,[11] Canadian jurisprudence interpreting section 8 of the *Charter* now recognizes that individuals in Canada can enjoy an expectation of privacy in the conduct of their lives in public as well.

As a result, it is the protection afforded by section 8 of the *Charter*, and its judicial treatment, that gives weight to individual privacy. This is particularly acute in the context of government security initiatives. In the

---

[8] See Stanley A. Cohen, "The Legal Basis of Privacy under the Charter," from *Privacy, Crime and Terror: Legal Rights and Security in a Time of Peril* (2005), pp. 14-19; also "Privacy protection under the Charter of Rights and Freedoms", from *The Law of Privacy in Canada* (2009), pp. 2.3 to 2.15.
[9] *R. v. Mills*, [1999] 3 S.C.R. 668 at 714.
[10] Alain-Robert Nadeau, Vie privée et droits fondamentaux: étude de la protection de la vie privée en droit constitutionnel canadien et américain et en droit international (Scarborough, Ont.: Carswell, 2000), 106.
[11] Eric H. Reiter, "Privacy and the Charter: Protection of People of Places?" (2009) 88 Can. Bar Rev. 119, at pg. 123.

context of searches by government bodies in particular, the Supreme Court of Canada has recognized that an individual's expectation of privacy may turn on location, the nature of the information and the relationship of the information to the individual.

On this element, one criterion the Supreme Court of Canada has adopted in weighing an individual's reasonable expectation of privacy is specifically if the personal information accessed by government involves "a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state".[12] As new technologies and social practices emerge and shape our conception of privacy, they can also raise new security concerns, and so that fundamental legal principles become all the more important. Finally, as noted above, context is vital as courts have weighed the question of what an individual truly expects to be reasonable with privacy in mind. How is personal information being collected, by whom, how is it being acquired and to what end?

All of these issues matter for the backdrop for considering privacy and create an underlying architecture for personal information that can be ruled as either protective or invasive. The *Tessling* case has come to stand for this necessity that government officials consider the 'totality of the circumstances'.[13] This means not only taking into account *subjective* expectations as security programs are designed (i.e. do individuals think their information or interactions are private in the proposed context?) but also objective elements including,

As new technologies and social practices emerge and shape our conception of privacy, they can also raise new security concerns, and so that fundamental legal principles become all the more important.

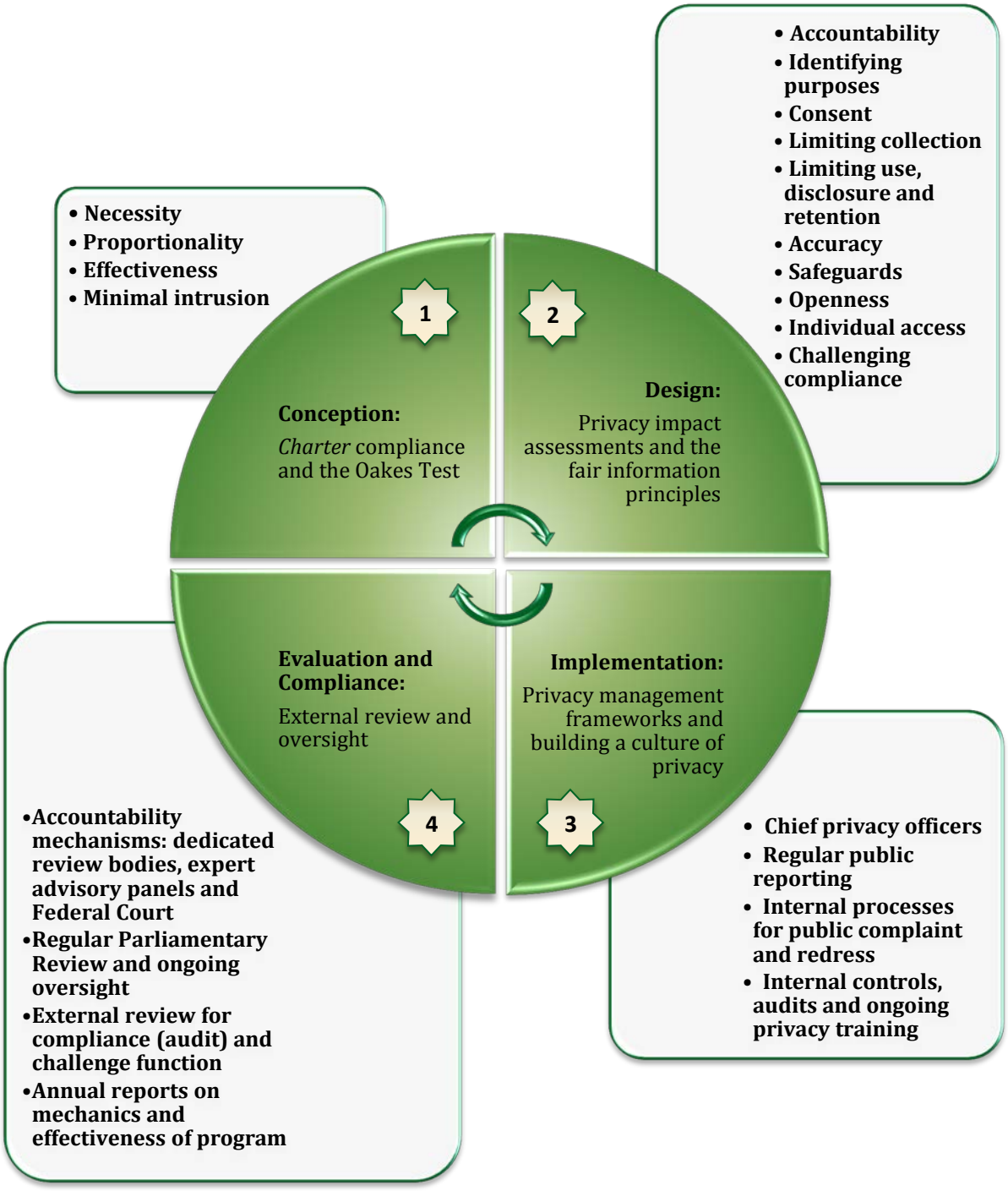
- does the information sought reveal individual lifestyle or 'biographical core' — things like their personal thoughts and reflections, political beliefs, mental state or medical condition,
- was the search open or covert — did the individual know their person or possessions were being scrutinized (as with a physical inspection or warranted search of premises) or were the citizen's actions or communications recorded in secret,
- the location the search is carried out — was the search undertaken in a completely public setting or somewhat protected from view, for example, in a vehicle or office,
- was the information on their person or discarded — for example stored on a personal device and password protected, or alternatively, simply on paper and thrown away,
- was the information in the hands of third parties and considered confidential — be that with a telecommunications company, government institution or legal representative,
- was an intrusive investigative technique deployed — such as a hidden camera, concealed microphone, location beacon, spyware or some other covert method, and,
- would the mode of surveillance be considered objectively reasonable under the circumstances?

[12] *R. v. Plant* (1990); refer also to Justice Lamer in *Schreiber v. Canada* (1998), "privacy is not a right tied to property, but rather a crucial element of individual freedom which requires the state to respect the dignity, autonomy and integrity of the individual."

13 *R. v. Tessling [2004] 3 S.C.R. 432*: "Few things are as important to our way of life as the amount of power allowed the police to invade the homes, privacy and even the bodily integrity of members of Canadian society without judicial authorization."

Privacy from the start: four stages for consideration

There are four general stages — conception, design, implementation and evaluation — in the development and implementation of security programs and policies. In each of these stages, there are certain factors that should be taken into account in order to ensure that privacy is respected and carefully documented (as within Privacy Impact Assessments). They are outlined below:



Stage 1: "Making the Case" — Charter compliance and R. v. Oakes

Following the enactment of the *Canadian Charter of Rights and Freedoms* in 1982, the Supreme Court of Canada formulated a methodological test to determine whether the violation of a *Charter* right is nonetheless justifiable in a free and democratic society. Stemming from the case *R. v. Oakes*, this became known widely as the *Oakes* test.[14] It requires:

- **Necessity:** there must be a clearly defined necessity for the use of the measure, in relation to a pressing societal concern (in other words, some substantial, imminent problem that the security measure seeks to treat),
- **Proportionality:** that the measure (or specific execution of an invasive power) be carefully targeted and suitably tailored, so as to be viewed as reasonably proportionate to the privacy (or any other rights) of the individual being curtailed,
- **Effectiveness:** that the measure be shown to be empirically effective at treating the issue, and so clearly connected to solving the problem, and finally,
- **Minimal intrusiveness:** that the measure be the least invasive alternative available (in other words, ensure that all other less intrusive avenues of investigation have been exhausted).

The importance of the objective, its underlying justification and a clear attempt to minimize the social effects of any intrusion are all inherent in this analysis. Although developed in the context of determining whether a *prima facie* violation of the *Charter* is justifiable under section 1 of the *Charter*, the *Oakes* test provides a useful framework to analyze the viability of a potential new security initiative.

Like the *Oakes* test, jurisprudence that specifically addresses the limits of police powers can assist with an assessment of the legitimacy of security initiatives that affect privacy interests.[15] In *R. v. Godoy*, for example, the Supreme Court ruled,

> *While residents have a recognized privacy interest within the sanctity of their home, the public interest in maintaining an effective emergency response system is obvious and significant enough to merit some intrusion ... however, the intrusion must be limited to the protection of life and safety; the police do not have further permission to search premises or otherwise intrude on a resident's privacy.*[16]

The Court determined that justification for the use of police powers and interference with individual's liberty turns on a number of factors, including the specific duty being performed by the police, the extent to which the interference with individual liberty is required to perform the duty, the importance of the duty in relation

---

[14] *R. v.* Oakes *[1986] 1 S.C.R. 103*
[15] See, for example, *R. v. Waterfield,* [1963] 3 All E.R. 659; *R. v. Stenning*, [1970], S.C.R. 631; *Knowlton v. The Queen*, [1974] S.C.R. 443; *Dedman v. The Queen*, [1985] 2 S.C.R. 2)
[16] *R v. Godoy*, [1999] 1 S.C.R. 311

to the public good, the nature of the liberty being interfered with and the nature and extent of that interference.[17]
Assessing security initiatives in relation to jurisprudence that assess the legitimacy of *prima facie* violations of individuals' interest can help ensure that a program's legal mandate is properly targeted, the powers appropriately tailored and that its impacts on established rights and freedoms are properly contained. It also establishes a test for determining whether any given infringement of a fundamental right can be reasonably justified. Without taking steps to discuss, document and demonstrate a balanced, reasoned approach in these aspects of information collection, government security agencies risk running afoul with review bodies, commercial stakeholders, political representatives and the wider Canadian public.

Without taking steps to discuss, document and demonstrate a balanced, reasoned approach in these aspects of information collection, government security agencies risk running afoul with review bodies, commercial stakeholders, political representatives and the wider Canadian public.

Stage 2: "Setting the Stage" — the Fair Information Principles

Once collection of personal information has been vetted, through the lens of the *Oakes* test or a similar analysis, a second set of operational questions can be applied to ensure that personal information is properly treated and protected. For the public sector, this is typically accomplished through the Privacy Impact Assessment (PIA), just as security issues are isolated by using Threat Risk Assessment (TRA). Both mechanisms assure Canadians that the privacy and security of their personal information are carefully considered in the design of any new federal program or service.

At this stage, the widely accepted *Fair Information Principles* can be brought to bear to ensure that the detailed architecture of a particular government program or technique is assessed and constructed with privacy in mind. These principles serve as the basic foundation for many countries' own data protection laws (including Canada's *Personal Information Protection and Electronic Documents Act*):

- **Accountability —** Ensure that someone is actively accountable for that information and puts appropriate policies and procedures in place;
- **Identifying purposes** — specify why the personal information is being collected;
- **Consent** — individuals must consent to use of their personal information beyond its original purpose or disclosures other than certain limited exemptions;;
- **Limiting collection** — collect only necessary, relevant information required to accomplish the security aim and use only lawful and fair means;
- **Limiting use, disclosure, and retention** — put logical and appropriate limits on the disclosure of sensitive information to other parties, limit use or disclosure to specified purposes and limit the timeframe for which information should be usefully maintained and fit for purpose.
- **Accuracy** — ensure the personal information is sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate decisions may be made about an individual;
- **Safeguards** –protect personal information by security safeguards appropriate to its sensitivity;

[17] *R v. Godoy*, [1999] 1 S.C.R. 311, par. 18

- **Openness** — be open about an agency's privacy policies and practices by making information available to citizens;
- **Individual access** — allow individuals to see and challenge the accuracy and completeness of their personal information and have it amended as appropriate;
- **Challenging compliance** — establish a complaint procedure.

These principles offer concrete privacy elements for planners or policy-makers to consider as they map out the broad strokes of any new public security initiative. The well-established fair information principles of privacy, as set out in many data protection laws, offer a filter that seeks to address the issue of over-collection.

These principles will help ensure that public security programs are well defined and properly structured. Examples can be found of government organizations involved in public security that have embraced these privacy practices and fair information principles for greater transparency and efficiency (see *Annex A: Three Privacy and Security Case Studies* for some specific controls and checks). It should be noted that many of these general principles of data protection have clear parallels or precedents in the intelligence-handling cycle or military classification.

Communication technologies have greatly expanded the speed, sophistication and sources by which governments acquire information ... the problem has become isolating what is necessary, significant and telling about security threats amid massive daily flows of data.

Throughout the 20th century, security and intelligence authorities around the world expended significant resources finding ways to collect more information, from widely disparate points, in a timely fashion. As with all government analysts and decision-makers, security bodies were often stymied by the technical requirements, staff capacity and communications problems of collecting and analysing information fast enough for its use in the national security context. More information was always viewed as advantageous.

However, impressive advances in information and communication technologies have greatly expanded the speed, sophistication and sources by which governments acquire information. Rather, the problem has become isolating what is necessary, significant and telling about security threats amid massive daily flows of data. Security forces have become very efficient at collecting dots. The challenge lies in connecting them.

Privacy principles should not be immediately viewed as a hurdle to the collection of information or its exchange. Rather they can be a powerful lens to focus its analysis. A minimalist approach — inherent to privacy protection — can be a useful model for focussed collection and use of information. In this way, investigations and intelligence are streamlined and tailored to those matters that are aligned with meeting public security objectives.

Stage 3: "Running the Program" — Embedding privacy into information management

Having incorporated the privacy protections described above into the basic architecture of a program, the organization must also develop internal mechanisms to ensure compliance. These mechanisms should represent the third element or stage of privacy protections within organizations, once a security program has oved from initial design to ongoing operations.[18] Internal mechanisms should be considered as possible levers to sustaining appreciation of privacy issues, such as,

- clear organizational roles and responsibilities for personal information handling, including regular review for accuracy and continued relevance of sensitive personal information,
- accessible, plain language documentation of privacy policies and practices,
- strong internal audit capacity for privacy issues, especially in the areas of access, security safeguards and information transfer,
- detailed agreements in cases of information sharing where ever personal information is involved,
- regular public reporting and publication of Privacy Impact Assessment (PIA) information,
- straight-forward internal processes for handling and reporting of potential complaints, problems or data breaches,
- ongoing privacy training for both frontline staff and management, and,
- Senior-level accountability for managing the privacy element of programs, including designation of Chief Privacy Officers

The Chief Information Officer Branch of the Treasury Board Secretariat administers a comprehensive suite of policies, guidelines and best practices in this area. Reference to them is obviously crucial for carefully engineering any system or program that will be handling personal information on behalf of the Government of Canada (see *Annex B: Treasury Board Policy, Directives and Guidance on Privacy).*

The Chief Information Officer Branch of the Treasury Board Secretariat administers a comprehensive suite of policies, guidelines and best practices.

[18] For additional discussion and recommendations see *Privacy Management Frameworks of Selected Federal Institutions – Audit Report of the Privacy Commissioner of Canada* (2009) – URL: https://www.priv.gc.ca/en/opc-actions-and-decisions/audits/pmf_20090212/

Stage 4: "Calibrating the System" — External review and oversight

Public security programs often enable significant collection and use of personal information. In a democratic society, these programs must be subject to independent, external review mechanisms that are proportional to the scope of the powers and potential invasion of privacy. A common thread runs through the many legislative reviews, inquiries and reports that have examined Canada's national security regimes: namely, poor information handling practices, patchwork accountability mechanisms and limited oversight can lead to tragic, costly mistakes in the realm of national security operations.[19] In an era of networked intelligence sharing, there is a need for networks of review and oversight.

In an era of networked intelligence sharing, there is a need for networks of review and oversight.

Review and oversight mechanisms include a systematic process for handling complaints and concerns from the public, ensuring a clearly articulated method for appeal and reconsideration where problems arise, as well as periodic external review by Parliamentarians and by specifically mandated oversight bodies. These are all important controls in ensuring consideration and integration of rights within protections for security. Public security programs cannot be exempted from these mechanisms of legitimacy. On the contrary, the powers they confer can be so broad and discretionary that they require commensurate oversight. Moreover, a clear mechanism for independent review and redress, one that is properly empowered and sensibly resourced, lends credence and credibility to any security program or initiative.

There are a variety of possible external review and oversight mechanisms that can be adopted. These include five-year parliamentary reviews of legislation and increased involvement of House and Senate Committees in the review of public safety agencies and programs; dedicated external review bodies; and enhanced transparency through greater use of annual reports and other reporting processes. Some of these mechanisms are already being used. For instance, the Security Intelligence Committee (SIRC) reviews in detail the operational activities of the Canadian Security and Intelligence Service (CSIS) and the Communications Security Establishment Commissioner reviews in detail the activities of the Communications Security Establishment (CSE), both with specific references to protecting privacy.

As a last resort, many organizations observe specific penalties for unauthorized access to sensitive systems or misuse of personal information. The RCMP and other police organizations across Canada, for example, have set clear rules and regulations allowing their agencies to fine, discipline or even suspend officers who mishandle secure sources and systems or access personal information in an unacceptable fashion. In a similar vein, and with even stricter prohibitions, the *Criminal Code* imposes terms of imprisonment up to five years for unauthorized interception of private communications.[20]

---

[19] Canada has conducted numerous Inquiries into security matters: from the Wells (1966) and Spence (1966) inquiries into the tactics of the RCMP hunt for suspected Communist infiltrators, to the Mackenzie Commission (1969) recommendation to detach state security operations from the RCMP, the Marin Commission into RCMP Complaints (1974), to the Keable and McDonald inquiries (1981) which focused on RCMP activities in Quebec to monitor and undermine separatists. More recently, we have seen the Inquiries of O'Connor (2006), Iacobucci (2008) and Major (2010), all focused on one facet of Canada's national security structure or another.

[20] *Criminal Code,* Part VI – Invasion of Privacy, section 184

Finally, public reporting (like annual *Privacy Act* reporting or *Departmental Performance Reports*) should not be overlooked as another mechanism that can protect privacy by demonstrating the measures and performance of privacy protections, identifying gaps, reviewing privacy incidents, analyzing trends and recommending enhancements to processes and systems. SIRC and the CSE Commissioner, for instance, submit annual reports to their respective ministers for tabling in Parliament. The report on CSIS even includes, among other things, an analysis of the CSIS warrant system and use of surveillance, just as Public Safety Canada tables a similar annual report on the use of electronic surveillance.

In Canada, as in most other countries, the security operations of government are conducted largely in secret. There can be valid reasons for these exceptions. A certain level of autonomy, even deception, is necessary for sensitive, covert work. However, when mistakes are uncovered, the sheer complexity and secrecy of these operations can make meaningful redress for the public challenging, and in some cases next to impossible. This is why it is imperative that this need for secrecy be offset with strong review mechanisms and robust measures for accountability.[21]

[21] For additional discussion of proactive review and oversight in the security context, refer to Rights and reality: enhancing oversight for national security programs in Canada (Ottawa, 2009) URL: https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2009/parl_sub_090507/

Conclusion: privacy, security and the stakes for democracy

So what is at stake as policy makers and legislators grapple with the integration of privacy and public safety? What are the implications for Canada? Foremost at stake for government is the issue of trust. Trust between citizens and their neighbours, as well as between citizen and the state, hinge on a mutual understanding about privacy, its value as both a human right and a collective good.

Governments are understandably concerned with the costs associated with properly vetting the privacy implications of security initiatives. Yet countries around the world now spend collectively tens of billions of dollars every year to collect, analyse and share intelligence information for security purposes. Government systems and analysts can probe virtually every aspect of individuals' lives; these measures are both expansive and expensive, the effort intensive and invasive.

There are aspects of the equation that are not so easily quantified: are security measures ultimately proportionate in their invasiveness? Are they effective at countering the threat they seek to mitigate? Are they necessary in the final analysis, if some other tactic, approach or logic might be better suited? As Canada's National Security Policy makes clear from the outset, one of the most important challenges for our democracy in tackling security threats is to ensure "we do not inadvertently erode the very liberties and values we are determined to uphold."[22] In conclusion, the main purpose of this document is to provide reference in the constantly evolving context of security to ensure that the fundamental right to privacy is protected.

[22] Government of Canada, *Securing an Open Society: Canada's National Security Policy* (Ottawa, 2004), p. 3 URL — http://www.pco-bcp.gc.ca/docs/information/publications/natsec-secnat/natsec-secnat-eng.pdf

Acknowledgements

Our Office would like to offer a special thank you to the two academic leads on the review and consultation phase of the project: Karim Benyekhlef, Directeur du Centre de recherche en droit public, from the Faculté de droit de l'Université de Montréal and Arthur Cockfield, Associate Professor, Faculty of Law, Queen's University. Their assistance and objectivity were invaluable.

Also we are very grateful for the insights and experiences offered by a dedicated group of experts, academics and observers. All of these individuals contributed their time and energy in reviewing the ideas put forth in this position paper and met in person to debate and comment on its final form. We would like to recognize their contribution.

Some of these reviewers included:

- The Honorable Perrin Beatty
- Pierre-Yves Bourduas
- Karine Côté-Boucher
- Horst Intscher
- Dr. Edna Keeble
- The Canadian Council on American-Islamic Relations (CAIR-CAN)

Finally, a very special thank you to Chris Prince, Strategic Policy Analyst, at the Office of the Privacy Commissioner of Canada, for his dedicated work on this report and the consultations.

Annex A: Three Privacy and Security Case Studies

Case Study #1: The Passenger Protect Program (No-Fly List)

Transport Canada's (TC) mission is to develop and administer policies, regulations and services with a view towards attaining the best possible transportation system for Canada. The Passenger Protect Program (PPP) is intended to prevent individuals that pose an immediate threat to aviation security from boarding an aircraft at designated Canadian airports. Based on information received from Canadian and international security and intelligence agencies, Transport Canada compiles and maintains a list of individuals on a Specified Persons List (SPL). Once a match between a person wishing to board an aircraft and someone on the SPL is discovered by an air carrier and subsequently confirmed by Transport Canada, the person is denied boarding.

The personal information that is managed by the Passenger Protect Program includes intelligence information on specified persons received from Canadian or foreign security intelligence agencies; information on the SPL (names, alias, gender, and date of birth); information on potential matches to specified persons received by Transport Canada from air carriers; and information to support an individual's reconsideration claims.

Transport Canada provided the OPC with a Privacy Impact Assessment (PIA) to ensure it would incorporate privacy as a core element of the Passenger Protect Program. As an example, Transport Canada points to how it intends to limit the use of program-related personal information to only one legislated purpose, namely to reduce potential threats to transportation security.

Four Part Test: Necessity, effectiveness, proportionality and alternatives

In its review of the PIA, the OPC expressed "concerns about the privacy risks associated with a 'no-fly' project." With regards to proportionality, the Office was of the view that the PPP "may represent a serious invasion of the privacy rights and the freedom of movement of air travellers in Canada." The OPC further argued that there were risks that the information collected could be used inappropriately. The Office was particularly concerned that individuals who are mistakenly put on the list or misidentified as being threats could face "serious negative consequences ranging from inconvenience and delays to highly intrusive questioning, searching and detention as a result of a match."

With regards to necessity and effectiveness, the OPC argued that "we have not seen any study or analysis from TC that would demonstrate that the SPL is a useful and effective tool to strengthen the security of the air transportation system in Canada." The Office went on to recommend that Transport Canada hire an independent and experienced third party to conduct an evaluation of the Passenger Protect Program to assess its effectiveness.

Fair Information Principles

Accountability — Transport Canada provided the OPC with copies of MOUs it had signed with CSIS, the RCMP and air carriers. While these MOUs cover a wide array of matters, the OPC found that they contained minimal privacy and data protection provisions. The OPC recommended that provisions be added to specify: the methods to be used for the sharing of personal information; the administrative and technical measures and safeguards to be taken to protect information; the retention and disposal requirements for personal information to be shared; and the obligation to perform regular audits of information management.

Limiting Use, Disclosure and Retention — At the time of writing its PIA, Transport Canada had not yet established a records retention and disposal framework for personal information related to the Program. The OPC recommended that the department develop such a framework prior to the Program becoming operational. The OPC also raised concerns about the sharing of information in the SPL with foreign governments and law enforcement agencies, as the Office was apprehensive — and still is today — that this information could be used for other purposes.

Accuracy — The OPC raised concerns regarding names being mistakenly added to the SPL as well as the possibility of "false positives" being stopped from boarding planes. Among other things, the OPC recommended that Transport Canada: develop and document policies and procedures to ensure selection criteria for putting individuals on the SPL were strong and consistently applied by all of the security agencies involved in the process; periodically review the criteria and standards used for the inclusion of individuals on the SPL; develop appropriate procedures so that an individual who has been potentially identified as being on the SPL by an air carrier is in fact an exact identity match with the person named on the SPL; and develop and document procedures to notify partners (CSIS and RCMP) when a name has been removed from the SPL due to a proceeding under the reconsideration mechanism.

Safeguards — The PIA review remarked that some specific security procedures had not yet been documented, including contingency procedures in the event of the unauthorized disclosure of personal information. In response, Transport Canada included security procedures and requirements in the MOU with air carriers and developed security and contingency procedures for TC employees. The OPC was satisfied with the department's "Privacy Incidence Response Plan," in that it provided adequate guidance to Transport Canada personal in the case of privacy breaches.

Openness — At the time of writing the PIA, Transport Canada had not created a personal information bank (PIB) that related to the Passenger Protect Program for inclusion in Info Source. Transport Canada subsequently drafted two PIBs, one for personal information maintained by the PPP and the other for personal information held in the Office of Reconsideration. However, the PIBs did not describe all of the consistent uses that may be made of the personal information collected. The OPC recommended that for the sake of public transparency, the two PIBs be revised to incorporate all of the consistent uses that may be made of the personal information involved and to whom it may be disclosed. The OPC also recommended that Transport Canada undertake an "open and detailed public education campaign via mass media," describing the personal information practices of the PPP, including recourse mechanisms.

Challenging Compliance — The PIA stated that Transport Canada did not have specific procedures for recording complaints and their processing or resolution. The OPC recommended that standard operating procedures for the Office of Reconsideration be established and documented prior to the implementation of the PPP.

Current Status

- In 2009, the OPC tabled an audit report before Parliament which examined whether TC had adequate controls and safeguards to collect, use, disclose, retain, dispose, protect and ensure the accuracy of personal information under the PPP.
- While finding TC collects and uses personal information within the PPP in accordance with the *Privacy Act* and the *Aeronautics Act*, the audit also determined that the Deputy Minister at TC was not provided with complete information when deciding to add or remove names to or from the SPL.
- This situation may raise questions about the decision-making process if an incomplete record were to

result in an incorrect change to the SPL.

- In addition, TC could not demonstrate that the computer system used to disclose SPL information to air carriers has been certified to meet Government Security standards.
- TC accepted all OPC recommendations stemming from the audit and is implementing them. The OPC will follow-up with a two-year review.

Case Study #2: CATSA's Millimeter Wave Airport Scanners

The Canadian Air Transport Security Authority (CATSA) is a Crown corporation charged with protecting the public through pre-boarding screening of air travelers, their baggage and non-travelers who have access to restricted areas. In August 2009, CATSA submitted a Privacy Impact Assessment (PIA) to the OPC on the planned deployment of Millimeter Wave (MMW) scanners in Canadian airports. This technology penetrates the clothing of travelers to reveal images of the body in order to detect explosives or weapons that otherwise might be undetectable.

Its use is controversial and there has been considerable concern expressed about it, both in Canada and abroad. According to CATSA, however, MMW technology offers an innovative approach to passenger screening, in that the technology offers a less intrusive alternative to the physical search of passengers currently used at Canadian airports. Passengers undergoing secondary screening would have the choice to be screened by physical search or by MMW technology. Furthermore, according to CATSA, MMW technology is an improvement over current threat detection systems such as metal detectors, in that it may detect non-metal based weapons.

CATSA recognizes that MMW scanners raise privacy concerns. The agency says it has implemented a number of privacy-enhancing measures to address these concerns, including: making the MMW screening process voluntary and anonymous; not correlating an MMW image in any way with the name of the passenger to whom it belongs or any other identifying information; ensuring that the Wave system's "stand-alone" images captured during screening cannot be accessed by or transmitted to any other remote location; permitting only qualified and authorized operators to use the system; and ensuring that the MMW imagers cannot store, print or save images.

Four Part Test: Necessity, effectiveness, proportionality and alternatives

The OPC received assurances from CATSA that the need for MMW technology is based on a rigorous aviation security threat and risk assessment. Nevertheless, the OPC argued that CATSA should regularly scrutinize the implementation of MMW technology and justify it against the four-part test. The OPC recommended that CATSA regularly review its perceived need for this technology against updated aviation security threat/risk assessments, as well as against refinements to the available technology. In particular, the OPC recommended that new or alternative technologies to achieve the same screening goals in a less privacy-invasive manner also be considered. CATSA countered that available software for blurring the image of specific body parts would defeat the purpose of the screening technique.

CATSA also advised the OPC it would test improved software for the MMW units allowing scanners to detect anomalies without generating actual images of travelers. The only image that would be seen by security officials would be a stickman figure with areas highlighted for targeted physical search. If the pilot is successful, the plan is to deploy the new software at all MMW scanners in Canadian airports. This responds to the OPC's recommendation to explore new technologies to enhance privacy.

Fair Information Principles

Accountability — CATSA noted that it is committed to undertaking audits for compliance with privacy policies.

Identifying Purposes — CATSA indicated that notices identifying the purpose for the collection of information through MMW technology would be made available at airport security checkpoints equipped with the scanners. The OPC further recommended that CATSA undertake a public information campaign via its website, at airports using posters and brochures, and using other sources of information.

Consent/Notification — CATSA indicated that travelers selected for secondary screening would be offered a choice between MMW screening and a physical pat-down. The OPC further recommended that CATSA communications material be accurate presentations of the images obtained during screening, in order to ensure informed consent. Finally, the OPC recommended that CATSA carefully consider specific issues affecting the use of MMW technology to screen minors and the physically challenged.

Limiting Collection — The OPC recommended that no information other than the transitory image generated by the scanner be collected.

Limiting Use, Disclosure and Retention — CATSA should clarify the estimated timeframe for the existence of transitory images.

Accuracy — The PIA notes that images generated by the MMW scanners would be that of subjects standing in scanner units, and any anomalies would be investigated and confirmed by observation and/or targeted pat-down at checkpoints.

Safeguards — The PIA notes that scanned images would be permanently deleted after screening, and that images would be sent electronically to remote viewing rooms in such a way that screening officers could not see and identify actual travelers. The OPC further recommended that CATSA undertake assessments to ensure security of electronic images and prevent inappropriate use or disclosure of images.

Openness — The OPC recommended that CATSA develop and make publicly available a privacy policy specific to its use of MMW scanners.

Individual Access — CATSA observed that access by an individual to his or her image would be impossible, as these would not be stored after viewing or individually identifiable upon viewing by security officers.

Challenging Compliance — At the time of the PIA, there were no privacy specific procedures in place for travelers to complain to CATSA. The OPC recommended that CATSA monitor and report to senior management comments of travelers, complaints and concerns.

Current status

- CATSA agreed with OPC recommendations that scanners be used only as a secondary screening method.
- CATSA also committed that:
    - participation would remain anonymous and voluntary;
    - a physical pat-down would be offered as an alternative;

- screening officers would be separated from and unable to see the individual being screened;
- the images would not be correlated with any other personal information and would not be identifiable; and,
- all images would be deleted immediately after the scanning is completed.

- The OPC continues to monitor CATSA operations and encourage them to assess emerging technology that could further limit the invasiveness of airport security measures.
- CATSA is now experimenting with software that does not need to generate and image of the body and they also piloting software that produces image more like a schematic diagram than a life-like reproduction of the body.
- The OPC has initiated an audit of air travel safety measures, to examine privacy practices and screening technologies, which will be completed next year.

Case Study #3: CBSA's Enhanced Drivers Licence (EDL)

Following September 2001, the United States government began to implement a series of new security laws, measures and programs in response to investigations of the 9/11 attacks in New York and Washington, DC. One of these was the Western Hemisphere Travel Initiative (WHTI), setting out new requirements for secure identity documents to be carried by persons travelling to the US by air, land or sea. Canadian citizens were not exempt from the WHTI requirements, developed by the US Department of Homeland Security (DHS).

Canadian officials were concerned about the negative effect the new WHTI requirements might have on trade and individual travellers. With passports or other secure documents being required to cross the border into the United States as of June 2009, there was an immediate effort in both Canada and the US to develop secure alternative documents: the Enhanced Drivers Licence (EDL) was one of those documents and the Canada Border Services Agency (CBSA) was the lead federal department in Canada.

CBSA is the federal government organization charged with ensuring the country's security by managing the access of people and goods to and from Canada. CBSA undertook an initiative to encourage the adoption of EDL plans in Canadian provinces and acts as liaison with U.S. Customs & Border Protection. CBSA also manages the database of EDL information to which the U.S. has access.

The EDL plan (Phase I, British Columbia Pilot, 2007)

In March 2007, the government of Washington State began developing an EDL to meet the WHTI requirements issued by DHS. Given the flow of goods and people across the border, Washington State officials approached the government of British Columbia to gauge their interest in participating in a pilot project. Officials at the federal level in both countries were also meeting to discuss how new ID requirements might affect border wait times. Provincial authorities in Ontario and Quebec also expressed interest in participating.

From these discussions, it was decided that once provincial governments in Canada developed EDL documents, data on all EDL holders across Canada would be consolidated by CBSA and transmitted to U.S. Customs and Border Protection (CBP). Besides standard drivers licence data, each EDL would contain a citizenship identifier, RFID chip and unique reference ID, so that US border officials would be able to instantly call up an EDL holder's file before he/she physically arrived at the border post. This would enable faster screening and processing.

EDL applicants would consent to the sharing of all this information with CBSA and DHS upon application. Applicants would also authorize the sharing of their personal information among customs and immigration authorities, law enforcement and other government agencies, both in Canada and the U.S. For example, a

background check to confirm citizenship status would be conducted. The purpose of information exchange with CBP and DHS was to allow screening against watch lists for terrorism and other U.S. border lookouts.

The sharing of information on Canadian participants would not be reciprocal, however, and CBSA made no plans to receive additional data in advance on U.S. citizens travelling to Canada. In early 2007, privacy officials at the provincial and federal level began to express concerns regarding the EDL initiative CBSA was leading. The Information and Privacy Commissioner of British Columbia also expressed a wide range of concerns. By late 2007, for greater clarity OPC officials were invited by CBSA to put these questions directly to officials from DHS and the U.S. State Department.

Four Part Test: Necessity, effectiveness, proportionality and alternatives

In OPC exchanges with CBSA, several privacy risks immediately came to the foreground: use of long-range "vicinity-read" RFID chips in the EDL card, establishment of a "mirror database" on provincial EDL holders within CBSA, bulk transfers of personal information on EDL holders from CBSA to DHS, adding a citizenship / identity element to a simple licence document. While there was a need for change (given the changes arising from WHTI were essentially mandated by US sovereignty over its own borders) the argument for necessity of the EDL model proposed was weak. A Canadian passport is still adequate for this use, and they continue to be required for air travel to the U.S.

OPC asserted that no clear reason had been advanced to explain why a CBSA server in Canada could not house EDL information, which CBP could query as needed. The overall evidence presented for the effectiveness of the program was also far from obvious: no clear analysis was presented to demonstrate how border wait times would be affected by EDL enrolments. This ambiguity greatly complicated discussion of the proportionality of the proposal.

In the end, OPC stressed the need for serious reconsideration on: a) the issue of mass data exports, b) ensuring public education and fully informed consent for applicants, c) the secure use of unencrypted vicinity RFID technology, d) limiting collection of information to that data strictly necessary to administer the program, and, e) ensuring meaningful review and oversight for the program.

Fair Information Principles

Accountability — CBSA emphasized its responsibility for the care and custody of the data. In 2009, it reversed its decision to transfer bulk data on CDs to the U.S., instead opting to establish an EDL server for U.S. border officials to query when presented with a Canadian EDL. In addition, in 2010, CBSA committed to appointing its own designated Chief Privacy Officer to oversee programs like EDL.

Identifying Purposes — CBSA worked with OPC and provincial privacy authorities to develop clear, explicit language on the purposes for which various elements of personal information was being collected.

Consent/Notification — Participation in the program was fully voluntary. Applicants were given detailed background information on the program; this information was reiterated and explained during the interview and enrolment process. Disclosure of personal information to U.S. authorities, under applicable American law, was repeated throughout.

Limiting Collection — CBSA reiterated no personal information would be stored on the RFID chip and that no additional information would be gathered to supplement necessary EDL databanks.

Limiting Use, Disclosure and Retention — CBSA stated that EDL would be used solely for the purpose of establishing identity, citizenship and admissibility of travellers entering the U.S. MOUs were developed to set out these controls.

Accuracy — The OPC initially expressed concern on the issue of ensuring accuracy of up-to-date changes on EDL data once transferred to the U.S. The decision by CBSA to keep data housed in Canada, and therefore allow for individual access and correction, ameliorated that concern.

Safeguards — All personnel handling EDL data would be cleared to secret security level, including an RCMP criminal records check and CSIS background clearance. Strict access controls were also placed on data held at both provincial and federal levels. A protective "anti-skimming' sleeve was developed for use with the EDL document to prevent remote reading.

Openness — CBSA committed to explicitly addressing the matter of U.S. government access in its communications with the public "to ensure that the Canadian public is made aware of the significant privacy safeguards that will be put in place…especially sharing with the U.S. in consideration of the USA PATRIOT Act."

Individual Access — As stipulated by the *Privacy Act* and relevant provincial statute.

Current Status

- In the summer of 2009, CBSA published a lengthy summary of the PIA process for their EDL program on their website, including details on how EDL holders could access their personal information.
- As of 2010, EDLs are available in the provinces of British Columbia, Ontario, Quebec and Manitoba.

Annex B: Treasury Board Policy, Directives and Guidance on Privacy

- Policy on Privacy Protection
- Guidance Document: Taking Privacy into Account Before Making Contracting Decisions
- Guidance on Developing Information Sharing Agreements Involving Personal Information
- Directive on the Social Insurance Number
- Directive on the Administration of the Access to Information Act
- Directive on Privacy Requests and Correction of Personal Information
- Directive on Privacy Practices
- Directive on Privacy Impact Assessment
- Guidelines — General — 2-00
- Roles and Responsibilities — Privacy and Data Protection — 2-01
- Collection of Personal Information — 2-02
- Retention and Disposal of Personal Information — 2-03
- Use and Disclosure of Personal Information — 2-04
- Right of Access to Personal Information — 2-06
- Corrections and Notations — 2-07
- Excluded Information — 2-08
- Exemptions — Privacy and Data Protection — 2-09
- Review of Decisions Under the Privacy Act — 2-10
- Annual Reports — Privacy and Data Protection — 2-11
- Delegation of Authority — 3-01
- Assistance to Individuals in Exercising their Rights — 3-02
- Employee Privacy Code — 3-03
- Forms — Privacy and Data Protection — 3-05
- Model Letters — Privacy and Data Protection — 3-06

Annex C: Other useful resources, references, materials

- Centre for Innovation Law and Policy. Personal Information Protection in the Face of Crime and Terror: Information Sharing by Private Enterprises for National Security and Law Enforcement Purposes (University of Ottawa, 2008)
- Chandler, Jennifer, "Personal Privacy versus National Security: Clarifying and Reframing the Trade-off" in I. Kerr, C. Lucock & V. Steeves, eds., *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society* (Oxford: Oxford Univ. Press, 2009), pp. 121- 138.
- Cockfield, Arthur J. Protecting the Social Value of Privacy in the Context of State Investigations Using New Technologies. *U.B.C. Law Review*, Vol. 40, No. 1, p. 41, May 2007
- Cohen, Stanley. *Privacy, Crime and Terror — Legal Rights and Security in a Time of Peril* (Butterworths, 2005)
- Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police (1979-1981)
- Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar. Analysis and Recommendations (2006)
- Ibid. A New Review Mechanism for the RCMP's National Security Activities (2006)
- Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182. Air India Flight 182: A Canadian Tragedy – Final Report (2010)
- Forcese, Craig. The Collateral Casualties of Collaboration: The Consequence for Civil and Human Rights of Transnational Intelligence Sharing (March 2009)
- Government of Canada. Securing an Open Society: Canada's National Security Policy (April 2004)
- Harvey, Frank. The Homeland Security Dilemma: Imagination, Failure and the Escalating Costs of Perfecting Security (2007)
- House of Lords Select Committee on the Constitution (UK). Surveillance: Citizens and the State (Feb. 2009)
- Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmed Abou-Elmaati and Muayyed Nureddin (2008)
- International Commission of Jurists (ICJ) Panel on Terrorism, Counter-Terrorism and Human Rights, Assessing Damage, Urging Action (2009)
- Office of the Information and Privacy Commissioner of Ontario, Privacy Risk Management (2010)
- Posner, Richard A., Orwell versus Huxley: Economics, Technology, Privacy, and Satire (November 1999). University of Chicago Law School, John M. Olin Law & Economics Working Paper No. 89
- Regan, Priscilla M. *Legislating Privacy: technology, social values and public policy* (UNC Press, 1995)
- Schienin, Martin. The Right to Privacy: Report of the Special Rapporteur on the promotion and protection of human rights while countering terrorism (United Nations Human Rights Council, December 2009)
- Schneier, Bruce. *Beyond Fear: Thinking Sensibly about Security in an Uncertain World* (Springer, 2006)
- Soghoian, Christopher, Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era (August 17, 2009). Journal of *Telecommunications and High Technology Law*, Forthcoming; Berkman Center Research Publication No. 2009-07
- Solove, Daniel J., A Brief History of Information Privacy Law. GWU Law School Public Law Research Paper No. 215
- Solove, Daniel J., Digital Dossiers and the Dissipation of Fourth Amendment Privacy. *Southern California Law Review*, Vol. 75, July 2002
- Solove, Daniel J., 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy. San Diego Law Review, Vol. 44, 2007
- W. Diffie and S. Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption* (MIT Press, 2007)
- Wright, Andrea. "Casting a light into the shadows: why security intelligence requires democratic control, oversight and review" from *The Human Rights of Anti-Terrorism* (Irwin Law, 2008), pp. 327-367