Office of the Privacy Commissioner of Canada
Commissariat à la protection de la vie privée du Canada

Fundamental Privacy Rights within a Shared Vision for Perimeter Security and Economic Competitiveness

Submission by the Office of the Privacy Commissioner of Canada to the Government of Canada's Beyond the Border Working Group public consultation

June 2011

Table of Contents

Introduction

The Office of the Privacy Commissioner of Canada (OPC) understands the importance of facilitating trade and ensuring border security. Any review of measures or new initiatives to remove some of the barriers and delays many people now face in travelling would be welcome. Canadian citizens appear widely supportive of efforts to minimize burdensome screening and enhance security measures, as well as aiding cross-border travel and trade.[1]

At the same time, it is clear that *Beyond the Border: a shared vision for perimeter security and economic competitiveness* (hereafter, the Declaration) also commits to an integrated approach to threat assessment in pursuit of collective security.[2] This program would be based on broad sharing of Canadian citizens' personal information. In the past decade, border screening and other security measures established at both national and international levels have had widespread implications for privacy.

Again, while safer travel and communities are an important goal of both the United States (US) and Canada, they must be achieved with due respect for fundamental freedoms and privacy rights. Historically, these values and principles have been pillars within the open, democratic societies that our two countries have build together. The importance of these commitments remains today: privacy and respect for individual's private lives should remain a key concern no matter if the context is a border crossing or airport, a ticket counter or home computer.

In commenting on the Declaration and programs that may flow from it, we have structured our views along the themes presented both in the official document itself and our Office's own reference document , *A Matter of Trust: Integrating Privacy and Public Safety in the 21st Century*.[3] We have prepared general observations and specific recommendations for your consideration on the following:

- general border screening and security measures,
- information-sharing, oversight and redress mechanisms,
- use of biometrics,
- development of a continental exit-entry system,
- cyber security and personal information and,
- privacy and health emergencies.

[1] Nik Nanos, "Canadians and Americans see no conflict between border security, economic partnership", *Policy Options* (March 2011) URL: http://www.irpp.org/po/archive/mar11/nanos.pdf
[2] Government of Canada, *Beyond the Border: a shared vision for perimeter security and economic competitiveness: A declaration by the Prime Minister of Canada and the President of the United States of America* (February 4, 2011) URL: http://www.borderactionplan-plandactionfrontalier.gc.ca/psec-scep/declaration-declaration.aspx
[3] Office of the Privacy Commissioner of Canada, *A Matter of Trust: Integrating Privacy and Public Safety in the 21st Century* (2010) URL: http://www.priv.gc.ca/information/pub/gd_sec_201011_e.cfm

We have also included as an Annex earlier correspondence between our Office and the Beyond the Border Working Group (BBWG) on the importance of program design based upon internationally recognized data protection standards.[4]

General border screening and security measures

The experiences of many Canadians in recent years at border crossings and airports highlight ongoing concerns over the protection of privacy rights while travelling.[5] The Office of the Privacy Commissioner of Canada (OPC) receives ongoing inquiries from the media, members of the public and their elected representatives related to these incidents in transit.[6] This is particularly evident where individuals have been delayed, detained or denied entry on the basis of documented experiences that are years, even decades, past.

In 2005, many individuals living in Canada who had previously travelled freely to and from the US began reporting difficulties (or outright denials of entry) as they attempted to cross the border for business, shopping or to visit friends and family. Research indicates this may stem from new powers authorizing agents with U.S. Customs and Border Protection (CBP) to use information from a variety of public sources and private data services to augment their background checks on individuals seeking entry.[7] In essence, CBP officers can screen not simply against dedicated systems for specific outstanding warrants or look-outs, but general publically-available information on individuals, including travel, news and academic searches.

Privacy may be defined as the right of the individual to determine when, how, and to what extent he or she will release personal information.
~ R. v. Duarte, [1990] 1 S.C.R. 30

In Canada, many side-effects of mass collection, analysis and sharing of personal information with US security agencies and border authorities have clearly been unanticipated. These cases have ranged from the inconvenience of being stopped crossing the border on the basis of a suicide attempt five years in the past to the tragic rendition of a Canadian citizen to torture in Syria.[8] As Canada and the US negotiate efforts at streamlining border processes and security measures, these experiences must be considered.

---

[4] International Conference of Data Protection and Privacy Commissioners, *International Standards for the Protection of Privacy and Personal Data* (Madrid, 2009) – URL: www.gov.im/lib/docs/odps/madridresolutionnov09.pdf

[5] For a brief collection of these concerns see: International Civil Liberties Monitoring Group, *Report on the Information Clearinghouse on Border Controls and Infringments to Traveller's Rights*, (2010) – URL: http://www.travelwatchlist.ca/updir/travelwatchlist/ICLMG_Watchlists_Report.pdf

[6] Office of the Privacy Commissioner of Canada, Checking In: Your privacy rights at airports and border crossings (February 2010) URL: http://www.priv.gc.ca/fs-fi/02_05_d_45_e.cfm

[7] *Intelligence Reform and Terrorism Prevention Act of 2004* (Pub. L. 108-458, 118 Stat. 3638) - Title V: Border protection, immigration, and visa matters / Sub: Advanced Technology Northern Border Security Pilot Program, section 5102; see also US Department of Justice, "Federal Statutes Relevant in the Information Sharing Environment (ISE)" (2010) - URL: http://www.it.ojp.gov/default.aspx?area=privacy&page=1282 and Krista Boa et al. "Can ID? Visions for Canada's Identity Policy", joint report from University of Toronto and the London School of Economics (2006) - URL: http://www.lse.ac.uk/collections/informationSystems/research/policyEngagement/can_id_report.pdf

[8] Isabel Teotonio, "Canadian woman denied entry to U.S. because of suicide attempt" *Toronto Star* (January 29, 2011) - URL: http://www.thestar.com/news/article/930110--canadian-woman-denied-entry-to-u-s-because-of-suicide-attempt; Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar* (2006)

The Declaration signed earlier this year puts considerable weight upon the importance of protecting human rights, civil liberties, and privacy. The aim of the following analysis and recommendations is to ensure both governments honour this commitment.

OPC Recommendations

1. Ongoing transparency and openness by both governments is vital: Full-body scanners, automated targeting based on Advance Passenger Information/Passenger Name Record (API / PNR), racial / religious / linguistic profiling, biometric collections and behavioural screening have all been highly controversial practices in both the US and Canada. As technology facilitates more invasive practices, channels for complaints and clear accountability must be put in place on both sides of the border and the necessity of the measures need to be reviewed in an open, on-going manner. Any new requirements should be accompanied by clear explanations to the public addressing necessity, controls and redress mechanisms.

2. The highest legal standards and thresholds must be observed in multi-jurisdictional enforcement: Adherence to fixed and clearly articulated privacy principles, to be observed in common, will be critical in the sphere of cross-border law enforcement. Where surveillance and other investigative tactics are pursued, rules of engagement and authorization must flow to the highest levels of relevant protection. Government officials should resist any move to lower standards for privacy protections.

3. Privacy impact assessments and clear legal authorities are required for all related measures: Any collaborative security measure predicated on *analysis and exchange* of sensitive personal information should be subject to full privacy impact assessments (PIA). Domestically, programs must be supported by Canadian constitutional norms and federal statutory authorities governing law enforcement and national security powers. Any security measures predicated on *joint collection* (absent any information sharing agreement) must be subject to additional control measures and oversight.

4. Develop training: Canada and the US should seriously explore the way they develop and exchange employees. International professional development for border services personnel working on the front-line can be just as important in the long-term as routine exchange of data or threat assessments. It is crucial that border units and screening officers understand the legal frameworks and broader contexts of both Canada and the United States. Professional standards and training are important controls and therefore should be commensurate with information sharing initiatives and a *precondition* of access.

5. Argue for US investment in dedicated privacy oversight: In establishing the US Privacy and Civil Liberties Oversight Board, the White House has created and begun to staff an ideal office and venue at arm's length from government to consider any problems or incidents arising from increased security screening measures.[9] This is encouraging and we hope will continue to be a priority.

---

[9] Harold Relyea, *Privacy and Civil Liberties Oversight Board: 109th Congress Proposed Refinements* (2005)—URL: http://fpc.state.gov/documents/organization/46403.pdf

Information-sharing, oversight and redress mechanisms

During the past decade, since the terror attacks of September 2001, governments have continually debated whether, and to what extent, their intelligence and security agencies should exchange information and what conditions or controls they should place on such transfers. In Canada, three lengthy Commissions of Inquiry by Justices O'Connor (2006), Iacobucci (2008) and Major (2010) have delved into these matters with each producing findings and recommendations addressing the risks and necessary oversight of information-sharing.[10] The Auditor General of Canada has also framed the issue of information-sharing as one essential to public confidence in government institutions.[11]

First, the O'Connor Inquiry focussed on the circumstances of Maher Arar's investigation, detainment and subsequent rendition to Syria. In his review of the investigation, Justice O'Connor found that Royal Canadian Mounted Police (RCMP) investigators were too quick to assume "guilt by association". Worse, in the heated aftermath of the attacks on the United States in 2001, the RCMP provided US authorities with essentially open access to their investigative files in the domain of counter-terrorism. Counter-terrorism agents with the US Federal Bureau of Investigation (FBI) were provided a complete electronic copy of a database the RCMP has developed detailing their leads and persons of interest.

This was shared without controls or caveats, and it was this information that US officials acted upon when they intercepted Maher Arar as he travelled through New York State on his way home to Canada. Indeed, the pivotal importance of constraints, controls and caveats on information and intelligence sharing between the US and Canada was one of the most resonant observations of the inquiry. Both governments should consider Justice O'Connor's very important recommendations in determining the limits to any information-sharing mechanisms that might emerge from the new Declaration.

Second, there followed the Iacobucci Inquiry into the investigation and treatment of three other 'persons of interest' within Canada with possible connections to terrorism. Here, as with Mr. Arar, the individuals were ultimately removed from Canada and subject to severe conditions and treatment while imprisoned abroad. The major observation to emerge from those reviewed cases was the sensitivity investigators need to exercise before they label citizens with the word "terrorist" or "extremist" because of the longstanding consequences arising from these individual profiles. Maher Arar, despite having been cleared of any wrongdoing in Canada, remains on the U.S no fly list to this day.

---

[10] Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar (2006) – URL: http://epe.lac-bac.gc.ca/100/206/301/pco-bcp/commissions/maher_arar/07-09-13/www.ararcommission.ca/eng/index.htm; Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin (2008) – URL: http://epe.lac-bac.gc.ca//100/200/301/pco-bcp/internal_inquiry_actions-ef/CP32-90-1-2010-eng.pdf; Air India Flight 182: A Canadian Tragedy (2010) – URL: http://epe.lac-bac.gc.ca/100/200/301/pco-bcp/commissions-ef/air_india-ef/final_report-ef/en/reports/finalreport/default.htm

[11] Office of the Auditor General of Canada, "National Security: Intelligence and Information Sharing" from the 2009 March Status Report – URL: http://www.oag-bvg.gc.ca/internet/English/parl_oag_200903_01_e_32288.html

In the charged security stance that exists at border checkpoints, careless instances of profiling or poorly-substantiated investigative files can put individuals at very real risk of harm. The most pointed observance made in Justice Iacobucci's final report is that Canadian counter-terrorism investigators failed to consider the grave effects of their snap judgements and that they must exert far more care in the future. Our Office would hope that controls and consideration of oversight with any new investigative operations, integrated units or fusion centres take the findings of the Iacobucci Inquiry with all seriousness.[12]

Finally, the exhaustive 2009 report of the Major Inquiry on Canada's investigation of the bombing of Air India in 1984 made a series of recommendations touching upon information-sharing and aviation security measures. It is worth emphasizing that Justice Major concluded, on the balance of existing evidence and programs, that Canada's system for screening individual travellers was adequate and robust.

This conclusion came to the considerable relief of the privacy and civil rights community in Canada who have felt for some time that passenger surveillance and travel monitoring systems had gone too far in screening *individuals* but neglected screening *cargo*. In his final report, specifically regarding the treatment of aviation security, Major placed his primary emphasis on the *screening of cargo* and physical *security of facilities* that handle shipments and baggage. It is our view that to focus on the physical screening of cargo, goods and facilities would be generally consistent with the government obligation to minimize the collection of personal information and protect privacy.

OPC recommendations

1. Establish clear controls and limits on information-sharing: While the final reports of the O'Connor Inquiry made many recommendations to treat issues within the RCMP, the pivotal importance of constraints, controls and caveats on information and intelligence sharing cannot be overstated. This Office believes these lessons are just as critical today. We would encourage any and all information-sharing mechanisms emerging from the new Declaration or its subsequent projects to give heavy weight to recommendations of Justice O'Connor and observations of Justice Iacobucci.

2. Expand oversight and challenge functions within cross-border intelligence analysis: The most pointed aspect of Justice Iacobucci's final report is that Canadian counter-terrorism investigators failed to consider the grave, lasting effects of the labels they applied to individuals. Review and oversight within any new investigative operations, integrated units or fusion centres provide a critical check against this problem. In particular, the growth of the fusion model creates serious privacy risks as personal information from wide, inter-sectored sources (both government and commercial data banks) is combined and re-distributed.[13] The OPC would caution strongly against any arrangements where care and custody of personal

---

[12] OPC, *Rights and reality: enhancing oversight for national security programs in Canada - Submission to the Standing Committee on Public Safety and National Security* (2009) – URL: http://www.priv.gc.ca/parl/2009/parl_sub_090507_e.cfm; see also Andrea Wright, "Casting a Light into the Shadows: Why Security Intelligence Requires Democratic Control, Oversight, and Review", from *The Human Rights of Anti-Terrorism* (Ottawa, Irwin Law: 2008), pp. 327-367

[13] Torin Monahan, *Surveillance in the Time of Insecurity* (Critical Issues in Crime and Society, 2008); see also Laura K. Donohue, "Anglo-American Privacy and Surveillance" *Journal of Criminal Law and Criminology, v*ol. 96 no. 3, page(s) 1059-1208 (May 2006) – URL: http://iis-db.stanford.edu/pubs/21219/Privacy_and_Surveillance.pdf

information is unclear or weak accountabilities are in place for its use outside of Canada.

3. Privacy impact assessment (PIA) processes should be applied: Completing a PIA for each initiative should be centralized as part of the BBWG, ideally under the review of official who have clear accountability for privacy issues.[14] These provisions should be put in place for all programs, components or agreements that follow. In Canada, our Office should be kept informed of such new initiatives, and brought into the consultation process, at the earliest stages in their development.

4. Increase privacy safeguards for cross-border data exchange: As the OPC has argued for several years, provisions in the federal *Privacy* Act governing the disclosure of personal information by the Canadian government to foreign states must be strengthened:

> *The Privacy Act places only two restrictions on disclosures to foreign governments: an agreement or arrangement must exist; and the personal information must be used for administering or enforcing a law or conducting an investigation. The Privacy Act does not even require that the agreement or arrangement be in writing. The Privacy Act does not impose any duty on the disclosing institution to identify the precise purpose for which the data will be disclosed and limit its subsequent use by the foreign government to that purpose, limit the amount of personal information disclosed and restrict further disclosure … the Privacy Act even fails to impose any basic obligations on the Canadian government institution itself to adequately safeguard personal information.*[15]

While recent guidance issued by the Treasury Board Secretariat to federal departments on inter-governmental sharing sheds important light on these issues, citizens expect such fundamental protections to be enshrined in law, not at the level of policy and regulation.

Use of Biometrics: A Double-Edged Sword

The Government of Canada has not yet legislated standards regarding minimum protections for biometric data. At the same time, international standards bodies have been active in the past decade in treating implementation of biometrics, while also considering privacy issues, risks of identification, or possible redress when information is used improperly. Currently in Canada, at the federal level, the use of biometric identifiers is governed by the provisions of the federal *Privacy Act,* which regulates the collection, use, disclosure, and access to, personal information "that is recorded in any form".

Generally any privacy-invasive measure being proposed must be demonstrably necessary in order to meet some specific need. In addition, the intrusion on privacy must be proportional to the benefit to be achieved and it must be established that no other, less privacy-intrusive measure would suffice to achieve the same purpose[16]. Together, these three principles form

---

[14] PIAs are a process that helps determine whether initiatives involving the use of personal information raise privacy risks, measures, describes and quantifies these risks, and proposes solutions to eliminate or mitigate privacy risks to an acceptable level. See *Expectations: A Guide for Submitting Privacy Impact Assessments to the Office of the Privacy Commissioner of Canada* (2011) – URL: http://www.priv.gc.ca/information/pub/gd_exp_201103_e.cfm

[15] OPC, Privacy Act Reform Recommendations (2008) URL: http://www.priv.gc.ca/parl/2008/parl_080429_02_e.cfm#rec10

[16] Parliament of Canada Research Branch, Industry, Infrastructure and Resources Division, *Biometrics and Government*

the core metric against which all new technologies must be evaluated in order to ensure that new technology can be integrated with minimal intrusion on personal privacy.

Even when processing of personal information is determined to be appropriate according to the above criteria, the nature of the implementation is also important. A central principle of privacy protection is to give individuals control over the creation, storage, and use of information about them. This means that the medium by which personal biometric information is stored is of great importance to protecting the privacy rights of Canadians. Personal information can be stored electronically in large, centralized repositories, or in e-documents and tokens held by individual citizens. In some cases it may appear that personal information is being held by the citizen when, in fact, the information is stored centrally.

> **Privacy of the person perhaps has the strongest claim to constitutional shelter because it protects bodily integrity, and in particular the right not to have our bodies touched or explored to disclose objects or matters we wish to conceal. ~ *R v. Tessling (2004) 3 S.C.R 21***

The Enhanced Driver's License (EDL) issued by British Columbia, Manitoba, Ontario and Quebec, for example, stores information in a centralized database and the RFID-enabled document is simply a unique "identifier" which allows the border agent to rapidly access the relevant information. Similarly, biometric information can be stored centrally in large databases, or stored in e-documents and tokens held by the individual citizen. Local storage of biometrics has a number of privacy-protecting advantages, including reducing the risks of covert collection, undisclosed usage for secondary purposes, cross-linking across applications or programs, "function creep", and institutional data breaches.

OPC recommendations

1. Avoid unnecessary centralization of biometric data: The OPC strongly recommends that any implementation of a biometrics program out of the Declaration should be subject to a robust governance structure and avoid centralized databases in order to minimize the risk of unnecessary secondary uses of information. Any form of central registry for such sensitive information must be subject to controls put in place by a specific statutory mandate, in addition to putting in place privacy protective measures like minimization, classification, access controls and depersonalization.

2. Trust but verify: Identification does not require the verifying agent to access any other records except those pertaining to the individual, which reduces the visibility of private data and increases individual privacy. A "one-to-many" matching system greatly increases the chances of false positives and therefore negates the efficiency and privacy of the system. Identification requires a great deal more biometric information in order to ensure a proper match and increases the temptation to sacrifice privacy for accuracy. The OPC greatly prefers the *verification* method over the *identification* method for these reasons[17].

(2010) -URL: http://www.parl.gc.ca/Content/LOP/ResearchPublications/06-30-e.htm#ftn16

[17] OPC, *Data at your fingertips: biometrics and the challenges to privacy* (2011) -URL: http://www.priv.gc.ca/information/pub/gd_bio_201102_e.pdf p.10

3. Consider the long-term, network effects of biometric-based screening systems: The OPC urges caution when implementing any program which collects biometric data. When identity is easily verifiable through the use of biometrics, and is coupled with networked databases, the potential for tracking or even the emergence of a "surveillance society" is increased. Wide scale collection of biometric identifiers which are cross-linked to many databases constitutes an undue violation of privacy without justifiable evidence of effectiveness or fairness[18].

4. Establish technical protective measures: High standards for the integrity and security of biometric and other identity information must also be put in place.

Development of continental exit-entry system

As the Canadian and American economies have grown increasing intertwined, any new security processes should seek to minimize disruption of goods and people crossing our shared border. One model for continental security proposed an "Entry/Exit Database" of some manner to log each individual as they transit ports of entry in either Canada or the US. In addition to capturing individual's issued documentation (passport, visa, etc), proponents of this model argue a biometric identifier (fingerprint, iris/retina scan, etc) should be issued to allow for simple, efficient documentation and combating fraud.

A program on such a scale would constitute a major shift in the dynamics of our current data-sharing regime. It would also raise serious privacy concerns, which generally accompany the use of any biometric identification system. Canada and the US already cooperate on API/PNR traveler screening measures, immigration controls and refugee screening processes. However, the global implications for all individuals affected by this new model – be they travelers, immigrants or refuges – should be examined to understand the net effect on broader privacy rights as set out in the *Universal Declaration of Human Rights*.

There are two principal alternatives on which such an exit/entry regime could be modeled. The first is the European model, whereby citizens of member states are granted freedom of movement within all 25 European Union (EU) states. Passports are scanned at the port of entry and the information is recorded and logged to the Schengen Information System (SIS)[19]. As more countries opt for machine-readable or chip-enabled travel documents, this information is automatically collected, shared and validated among EU customs. If information-sharing triggers particular interest by a member state, SIS provides high-level "alerts" for very specific purposes - finding missing persons, recovery of stolen luggage or prior crimes committed within the Schengen area. When the passport bearer later exits the European Union, their port of departure is recorded and also transmitted among all states.

In theory, once admitted to one EU country, an individual is granted passage to any other without having to pass through another customs checkpoint. Whether this model of integrated information-sharing is tenable in the long-term remains to be seen, as various

[18] Jay Stanley and Barry Steinhardt, *Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society*, (American Civil Liberties Union, New York : January 2003) –URL: http://www.aclu.org/files/FilesPDFs/aclu_report_bigger_monster_weaker_chains.pdf

[19] European Commission, *Schengen Convention Frequently Asked Questions* (2011) – URL: http://ec.europa.eu/home-affairs/policies/borders/borders_faq_en.htm

member states (e.g. Denmark, Italy, France) have begun to debate is effectiveness.[20] However, the major privacy concern remains that data is collected from the passport and shared with other countries which the bearer does not necessarily pass through.

The second approach is the American model, largely formulated in response to the September 11, 2001 attacks. In late 2002, the newly formed Department of Homeland Security (DHS) put in place the National Security Entry-Exit Registration System (NSEERS)[21]. Any male over the age of 16 who is a citizen from a "high-risk" state (as termed by the US State Department) was compelled to register at a port of entry or with a local DHS office and to provide fingerprints and photographs. Even when admitted legally through the visa process, these foreign nationals were forced to report to DHS and give detailed plans and updates of their activities while within the country. Such a regime demonstrates how the immediate reaction to terrorism can trump any underlying concerns for privacy.

Unlike the European model, which only collects photographs and only provides limited access to domestic law enforcement agencies, the next model to emerge was US-VISIT.[22] This exit-entry system linked to the wider US Interagency Border Inspection System (IBIS). Even risk assessment in these segmented systems is beginning to converge. Being flagged as a threat within IBIS, for example, may result in individuals being added to the US "No Fly" list. In addition, IBIS interfaces with the FBI's National Crime Information Center (NCIC), state police forces the National Law Enforcement Telecommunications Systems (NLETS), as well as twenty other agencies including Interpol, the Internal Revenue Service and Secret Service[23].

By analogy, Canada Border Services Agency keeps a record of all movements of Canadians travelling in and out of the country by air for 7 years with the E-311 customs declaration card. However, this database may *only* be used for very specific purposes laid out in the agreement and is not fully integrated with the domestic law enforcement databases of member states. Needless to say, how personal information of this sensitivity is shared with other governments should be a primary consideration of Canadian officials examining options on any broad-based passenger tracking protocol.

By entering the US as a private person, many foreign visitors now provide personal information (namely photographs and fingerprints) that their own governments would only be able compel if they were detained criminally. By adapting the EU model to suit our security needs, the Government of Canada may be able to better protect our borders and ensure efficient trade with the US. With the benefit of EU experiences, this could also be done in a manner that recognizes and gives all due weight to the importance that Canadians continue to place upon their rights to privacy and minimizing the threat of personal information being used for secondary purposes unrelated to security.

---

[20] "Defenders of the Schengen zone face a battle" *Financial Times* (May 24, 2011) – URL: http://www.ft.com/cms/s/0/5f8bfade-8628-11e0-9e2c-00144feabdc0.html#axzz1O7aj8dxk

[21] Department of Homeland Security, *Changes to the National Security Entry/Exit Registration System (NSEERS),* (2003) – URL: http://www.dhs.gov/xnews/releases/press_release_0305.shtm

[22] United States Visitor and Immigrant Status Indicator Technology (US-Visit) is considered to be the expanded version of the original NSEERS program.

[23] United States Customs and Border Protection, *IBIS- Who Uses Interagency Border Inspection System* (2010) -URL: https://help.cbp.gov/app/answers/detail/a_id/152/~/ibis---who-uses-interagency-border-inspection-system

OPC Recommendations

1. Strongly consider the European data protection scheme and their experience: The government should strongly advocate for a made-in-Canada model heavily influenced by the European approach -- that is, a model that reflects Canadians concern for care and protection of their personal information. By gathering only that information which is truly necessary for border security, such a program should limit the threat of over-collection and inappropriate use. By comparison, adopting a US model would see Canada share personal information on travelers visiting locally, and in some cases, where individuals have made a conscientious decision to not travel to the US. Such an approach would not only offend the value Canadians traditionally place in their privacy but may have the effect of hurting the reputation of Canada abroad as a destination of choice. The following considerations must be carefully considered in choosing a model for perimeter security:

- *Is the primary use of this data border security or law enforcement?*
- *What kind of biometric data will be required under this new program?*
- *Who oversees the proper use of this data?*
- *Which databases will this be linked to?*
- *Where and how will the data be stored?*
- *What redress will the Government of Canada have for unlawful secondary access?*
- *How will dual-passport holders be classified?*
- *How will disputes over "flagged" countries, specifically Cuba, be handled?*

2. Both governments should clearly explain program goals to citizens: Globally, entry/exit systems are primarily border management systems. They provide for immigration control, security screening and collection of duties. Both citizens and visitors to the US and Canada must be fully informed of the programs' stated purposes, the extent of their application and use of personal information and who individuals personal information will be properly protected.

3. Consider broader impacts of expanding collection of personal information: Globally, the use of biometrics like fingerprints for secondary purposes has raised concerns not only regarding privacy, but other human rights protections (such as mobility). For example, if a refugee is unable to migrate and in effect cannot "land" anywhere, flight in cases of duress and danger becomes near-impossible. Even domestically, design of a national exit system has been controversial. There has been much dispute in the US over the cost of infrastructure for fingerprint collection across all departure points. Beside privacy, cost, unintended consequences and other complexities need to be considered.

Cyber Security, Personal Information and Electronic Monitoring

Both countries recognize that the digital realm has become an integral part of the critical infrastructure and have taken measures to ensure that it is defended. Secure, private communications are indeed a crucial component of both our economies and wider societies. The OPC has been generally supportive of these measures, provided that they take into careful consideration the privacy concerns of our citizens, both online and offline.

Addressing cyber security is truly important, because both companies and government departments need to ensure that the personal information of citizens which they collect cannot be accessed by unauthorized entities. In the US, the recently issued *International Strategy for Cyberspace* recognizes and reinforces the primary commitment of government to citizens' legal protections. It also strongly affirms that fundamental freedoms, privacy and free flow of information are ideals that cannot be compromised, either online or offline.[24]

Similarly, as *Canada's Cyber Security Strategy* sets out, our efforts to tackle these issues must be done in accordance with Canadian values like the rule of law, accountability and privacy.[25] Over the past decade, Canada has taken a number of steps to enhance its own cyber security. Across government, there have also been expanded efforts to better protect citizens and businesses from online risks and threats.

> **The state's interest in detecting and preventing crime begins to prevail over the individual's interest in being left alone at the point where credibly based probability replaces suspicion. History has confirmed the appropriateness of this requirement as the threshold for subordinating the expectation of privacy to the needs of law enforcement.**
> ***~ Hunter et al. v. Southam Inc., [1984] 2 S.C.R. 145***

Cyber security programs must recognize that issues of sovereignty and integrity arising from local data held on Canadian servers and systems. These contain personal information that must not be compromised or undermined. The online interests of law enforcement and national security investigations – efforts to police online systems and networks – cannot proceed without due process, appropriate oversight and careful consideration. Canadian and American governments have come to realize that privacy and security are not a zero-sum game[26].

The OPC has been supportive of Canada's efforts on cyber security to date, in particular moves to effectively combat spam and identity theft. These are two examples of online cyber threats that aim to exploit the personal information of unsuspecting citizens for the purposes of fraud, forgery and other criminal activities. Indeed, we would continue to argue that work remains to be done in tackling these problems, in particular where they are being perpetrated online and where victims can often be completely unaware that they have become a target.

However, fundamental legal principles and traditional privacy protections must carry over in all cases from the offline world to the online environment. Canada's private sector privacy law, the *Personal Information Protection and Electronic Documents Act* (PIPEDA) was enacted to give Canadians confidence that as consumers and citizens their privacy rights would transfer into the digital environment as they went online to converse, shop and explore the online world. Ensuring that electronic commerce and communications remain within a trusted space

---

[24] US White House, *International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World* (May 2011), p. 5 – URL: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

[25] Public Safety Canada, *Canada's Cyber Security Strategy - For a stronger and more prosperous Canada (2010) p. 8 – URL:* http://www.publicsafety.gc.ca/prg/ns/cbr/_fl/ccss-scc-eng.pdf

[26] Mary Ellen Callahan, "The Privacy Framework for Information Sharing in Security and Border Management: A U.S Perspective." *One Issue, Two Voices,* Issue 13, Woodrow Wilson International Center for Scholars (2010) --URL: www.dhs.gov/.../privacy/dhsprivacy-privacyandinformationsharing-issue13-october2010.pdf

must remain a key commitment of our government as Canada seeks to interface with ongoing cyber security efforts by the US.

OPC recommendations

1. Reinforce the foundational protection and respect of rights and freedoms online: Cooperation and intelligence-gathering by government in the context of cyber security should not expand to the detriment of individuals' privacy, civil liberties and constitutional guarantees. Policy-makers and investigators must keep in mind that citizens expect that they maintain this crucial balance. It would be ironic, even self-defeating, if in the rush to secure our electronic systems for communication and commerce with broader security and surveillance we undercut the faith and trust that citizens have in the confidentiality and privacy of their own communications. Both Canada and the US should enter into discussions on cyber security cooperation with this risk in mind, and a clear enumeration of what initiatives are unacceptable.

2. Avoid purely technical solutions and strategies: Following from this, both governments need to broaden their approach to cyberspace. Security cannot simply amount to more spending on technological solutions. Pervasive threats like phishing, spamming, botnets, malware and spyware cannot be tackled across the public and private spheres without a broad-based strategy.[27] Any shared effort must be accompanied by clear legal guidance (setting out what is and is not acceptable), expanded education and public awareness around data security and information protection practices, stronger efforts to support independent, multidisciplinary research on cyber issues, bi-national commitment to developing better protective, privacy enhancing security standards, and ensuring regulatory bodies have the capacity and authorization to ensure better industry practices.

3. Broaden public consultation, dialogue, education and outreach: One source of ongoing confusion and criticism in both Canada's cyber security efforts and those of the United States have been the lack of public engagement, open, public reporting and transparency. The scarcity of open source information and discussion has left the average citizen (as well as many experts) completely outside policy and legal discussions around online security efforts. In this digital age, where citizens expect engagement and interaction, that lack of open dialogue is clearly unacceptable and will undermine long-term efforts. Both Canadian and US officials need to create mechanisms for regular public reporting, engagement and an open process to hear concerns and complaints as they begin cooperative cyber security efforts. These forums cannot be late-game add-on activities; they need to be planned, substantive and interactive and from the outset.

4. Expand public research and dialogue into the international challenges in cyber security efforts: Cyber security has become a major preoccupation of governments around the world, but too much of the expertise, research and discussion remain out of the public eye. Much more involvement from academics, civil society, media and individual citizens is needed. I would encourage the governments in Canada and the United States to explore creative ways to encourage long-term, stable public research in this area. In Canada, we

[27] Ron Deibert, Canada Centre for Global Security Studies, Munk School of Global Affairs, University of Toronto, "Cyber Security: Canada Is Failing The World" (May 26, 2011) - URL: http://www.huffingtonpost.ca/2011/05/26/cyber-security-canada-stephen-harper-g8_n_867136.html

have several emerging centres of excellence in this domain but the subject matter is both broad and deep. Universities in Canada and across the US should be encouraged to develop focus and expertise and to establish networks and joint events to share their research. Open sourcing, open discussion and open debate on cyber security and infrastructure protection issues should be the norm, not the exception. No one has a monopoly on good ideas (or bad experiences) in this arena and lessons from one sector, one context and one country can be invaluable to the broader public. This costs money, takes time and is contingent on people - not systems - but like training and investment in human capital, the payoff over the horizon will be extraordinary.

Privacy and health emergencies

Public fear of pandemic outbreaks is increasing as our borders become more permeable to both goods and people. The widespread concern surrounding Mad Cow Disease in 2001, the SARS outbreak in 2003, and the H1N1 virus in 2009 demonstrate the capacity of biological threats to rapidly spread across the globe. Governments and supra-national organizations such as the World Health Organization (WHO) have begun to recognize that the only method to prevent regional outbreaks of contagious disease is to identify problem areas early in order to quarantine an epidemic from spreading around the globe and becoming a pandemic.

While sanitation and proper medical care are obviously the primary defence against disease, the WHO has found that international data-sharing programs are necessary in order to track the spread and attempt to localize it. [28] Important as this may be, disclosure of this data can constitute a breach of patient privacy on the part of hospitals and health authorities. Canadians have high expectations of privacy when health records and medical histories are concerned. While medical facilities are most often careful in their disclosures, there are currently no legislative processes in place outside of a "state of emergency" which stipulate how alerts and planning should be carried out. As a result, violations of privacy must be weighed against the potential of the epidemic becoming a pandemic. Without careful legislative safeguards in place, this often results in data being disclosed purely by discretionary decisions.

This is extremely problematic as medical records are widely recognized as more important than even biometric identifiers. They contain personal information which historically has been considered inviolable and subject to strictest ethical and professional confidence. The Supreme Court of Canada has similarly recognized that health records must be held to a higher standard. As Justice LaForest notes, "the use of a person's body without his consent to obtain information about him, invades an area of personal privacy essential to the maintenance of his human dignity"[29]. Data related to health records must be safeguarded with the utmost care because "the trust and confidence of the public in the administration of medical facilities would be seriously taxed if an easy and informal flow of information...from hospitals to the police were allowed"[30].

[28] World Health Organization, *Pandemic Influenza Preparedness Framework for the Sharing of Influenza Viruses and Access to Vaccines and Other Benefits* (2011) –URL: http://www.who.int/csr/disease/influenza/pip_framework_16_april_2011.pdf
[29] *R. v. Dyment,* [1988] 2 S.C.R. 417 para. 27.
[30] *R. v. Dyment,* [1988] 2 S.C.R. 417 para. 38.

The risk of function creep is amplified when the data in question pertains to medical records. Disclosure of medical records from hospitals to law enforcement has been viewed, both legally and civilly, to be a massive violation of individual privacy. Disclosure of these records to a foreign entity is questionable because control of data flows cannot be regulated. Just as in biometric identifiers, there are many cases where health records could be used for secondary purposes. It is clear that, if such a regime is not created with the utmost care for privacy, there is huge potential for public concern.

> **The use of a person's body without his consent to obtain information about him, invades an area of personal privacy essential to the maintenance of his human dignity … the trust and confidence of the public in the administration of medical facilities would be seriously taxed if an easy and informal flow of information from hospitals to the police were allowed.**
> ***~ R. v. Dyment, [1988] 2 S.C.R. 417***

OPC Recommendations

1. **Adopt proper legislative frameworks:** These must govern the information sharing aspects of the health security partnership noted in the Declaration. These should aim to ensure there is an appropriate balance of privacy rights and regulatory powers as well as transparency, notice and accountability to those subject to the legislation and to the public.

2. **Specify narrow definitions in which medical information of Canadians is shared:** We would suggest that the reasonable grounds test is applied to inform the decisions to disclose information, and that the personal information disclosed is appropriately limited and directly relevant to a specified health emergency. We would also suggest that the information sharing agreement provide for disclosing de-identified or anonymized information if that would accomplish the stated purpose.

3. **Information disclosures must be as limited and specific as possible:** Personal information should not be used by the receiving party for any purpose other than which it was disclosed, it should be protected with appropriate security safeguards, and it should only be retained for as long as is necessary to fulfill the purposes related to the specific health emergency. As well, the receiving party should be required to hold the information in confidence unless there is a statutory obligation to disclose it.

Conclusion

Canadian and US laws may differ on key points: where there is a reasonable expectation of privacy, what is personal information, the legal effect of transferring information to third parties. However, all differences aside, the OPC does not believe that Canadians are willing to accept a "levelling down" of their privacy protections simply in pursuit of an enriched perimeter security agenda.

It is the position of the OPC that no subsequent agreements should be put in place for information sharing until an enhanced legal framework has been put in place to allow proper oversight and privacy protections and through a concerted public discussion and debate in our respective legislatures.

Given the fundamental imperative of protecting civil liberties and privacy in advancing a North American security perimeter strategy, and that privacy invasive measures are not always effective, we would urge both governments to give due regard to the our recommendations and include them as fundamental aspects of their vision for shared perimeter security and economic competitiveness.

ANNEX - Letter from the Privacy Commissioner of Canada to Mr. Simon Kennedy at the Beyond the Border Working Group following signature of Beyond the Border: a shared vision for perimeter security and economic competitiveness

Mr. Simon Kennedy
Senior Associate Deputy Minister
Industry Canada
235 Queen Street - 11th floor
East Tower - Room 1114A
Ottawa, Ontario
K1A 0H5

Dear Mr. Kennedy:

I am writing to follow up on our meeting last month, and to thank you for the briefing on the Beyond the Border Declaration as well as the work of your group flowing from it. We understand that the information provided was at a conceptual level at this point, and that much remained open for negotiation. It is the intention of my Office to provide the Beyond The Border Working Group more detailed comment once your public consultation process recommences in May. However, given that the work is unfolding very quickly and the joint Privacy Protection Principles are already in development, we hoped to provide some initial thoughts on that important first step.

International context

Clearly, we understand the importance of facilitating trade and ensuring border security. Any review of measures or new initiatives to remove some of the barriers and delays many people now face in travelling would be welcome. At the same time, the Declaration also commits to the expansion of another agenda, namely an integrated approach to threat assessment in pursuit of collective security. As you know, global security measures taken over the past decade have had an impact on both privacy rights and freedom of mobility. Again, while safer travel and communities are an important goal of both the U.S. and Canada, we often differ over approach.

For example, if traveller risk assessment or cross-border law enforcement is to be premised upon increased intelligence sharing, it is critically important that this be conducted in accordance with our national values and legal traditions, as underscored in the *Canadian Charter of Rights and Freedoms*, the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act*. It is also vital that information exchange:

- be circumscribed to the specific elements of personal information that are truly necessary,
- be bounded in its use and disclosure for very specific purposes, and,
- be subject to a robust set of safeguarding measures and oversight.

The OECD Guidelines

As you mentioned at our meeting, the 1980 *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* can serve as a starting point for this effort. I understand this element of the work is being led by representatives from Justice Canada and Public Safety Canada. While the role of my Office is clearly bound by our independent status as an Office of Parliament, we would be pleased to give them the benefit of our experience in trans-border data issues and

international instruments governing data protection and privacy rights.

However, it is worth pointing out the *Guidelines* are themselves under review. After thirty years, under the leadership of the OECD Working Party on Information Security and Privacy, many members are beginning to re-examine and debate the relationship between the Guidelines and the new global environment. Many jurisdictions are considering major enhancements to the privacy protections, for example the European Union Data Protection Directive. It goes without saying that our current understanding with many countries regarding the privacy protections we honour could be affected by upcoming changes undertaken with the U.S., so this continuing evolution in the regulation of personal data is worth bearing in mind.

Canada's experience with privacy governance

Finally, I would also like to take this opportunity to briefly highlight a few points and guiding lessons drawn from the review experience of cross-border initiatives undertaken by my own Office. My general observation would be that Canadians have high expectations of privacy and a deep commitment where personal information protection is concerned. Given these sensitivities around private information and sovereignty, I would tend to believe any movement away from these norms would quickly overshadow public debate around plans to follow.

Holding firm to Canadian standards of personal information protection will therefore be crucially important. As we have consistently found in our research and audit work, sharing data across borders must be undertaken in a manner that is both transparent and subject to specific controls. All trans-border data flows should be accounted for in meaningful detail to better inform Parliament and Canadian citizens.

As per our discussion, our Office is pleased to assist by reiterating the following high level privacy principles that may help guide this initiative. Addressing these matters openly is critical to trust, and in the best public interest. Strong privacy protection and accountability are essential to treat public concern about the flow of personal information from Canada to other countries. To that end, I could take this occasion to reiterate the following:

1. Personal information of citizens should be collected, used, retained or disclosed only for a purpose directly related to a specific operating program or activity.

2. Personal information of citizens should be accurate, up to date, complete and retained for no longer than the prescribed or necessary periods of time.

3. Personal information of citizens should be physically and electronically secured from breach or unauthorized access.

4. Accountability should be clearly defined and maintained.

5. Safeguards should be in place to ensure that access to a selected service is separate from access to other services, and that data about such access is not shared with other services.

6. Any outsourcing or expanded role for private-sector firms in meeting current government functions, operations and oversight should follow Treasury Board Secretariat's *Guidance Document: Taking Privacy into Account before Making Contracting Decisions*, especially when it comes to security requirements, employee access, inspections, audits and breach notification.

7. Any information-sharing arrangement should follow Treasury Board Secretariat's *Guidance on Preparing Information Sharing Agreements Involving Personal Information.*

8. Finally, within any new legislative initiative, security regulation or proposed surveillance program, government must assess the potential ripple effects upon our particular notion of "a free and democratic society". This means, where new security measures could lead to potential intrusion and loss of privacy, government must be prepared in advance to demonstrate:

    a. how these new steps are necessary to the specific task at hand,
    b. how they are a reasonable, proportionate response to the particular problem at hand,
    c. that they will be clearly effective in treating that unique problem, and,
    d. the proposed measure is the least invasive alternative available.

Again, we welcome the chance to exchange ideas on how the Privacy Protection Principles can be best strengthened and buttress the work to come. In the short-term, if you or your working group members would like further input or ideas, please contact Chantal Bernier, at 613-944-4289.

We appreciate your consideration of these concerns.

Sincerely,

Jennifer Stoddart
Privacy Commissioner of Canada