The Private Sector, National Security and Personal Data:

An Exploratory Assessment of Private Sector Involvement in Airport and Border Security in Canada

A Report to the Office of the Privacy Commissioner of Canada, under the Contributions Program

March 2011

Surveillance Studies Centre
Queen's University, Kingston, ON K7L 3N6
Tel: (613) 533-6000, ext. 78867; Fax: (613) 533-6499
e-mail: surveill@queensu.ca
website: http://www.sscqueens.org

Lead Author: Alanur Çavlin Bozbeyoğlu
Researchers: Harrison Smith and Christine Sebben
Advisors: David Murakami Wood, David Lyon and Arthur Cockfield
Proof Reader: Sarah Cheung

Acknowledgements:

The research team also gratefully acknowledges the work of the following individuals in the research activities and the preparation of the report: Patrick Derby, Joan Sharpe and Emily Smith.

CONTENTS

EXECUTIVE SUMMARY

Introduction

Security has become a rationale for new laws and initiatives that call in question the future of key Canadian social values and legal rights, including the right to privacy. Security tasks are increasingly carried out by the private sector. This exploratory study by the Surveillance Studies Centre (SSC) at Queen's University assesses the involvement of the private sector in border and airport security in Canada.

Private Sector Involvement in Border and Airport Security

1. Information Collection in Advance of Travel

Advance Passenger Information (API), including Personal Name Record (PNR), is created for every air traveller at the time of ticket reservation. API/PNR data are hosted by just four Global Distribution Systems (GDS) (also known Computerized Reservation Systems – CRS), Galileo, Worldspan, Sabre and Amadeus, the latter based in Spain and the former three in the US. Commercial airlines help create this data but have no official access.

Canada has PNR-sharing acts with the US, the EU, and Switzerland. Canada and the EU share a mutual concern for privacy in PNR data. However, since three of the GDS are located in the US and the US has no national law to limit usage and the disclosure of the data, PIPEDA applies but has major issues of enforceability once data moves to these sites.

PNR data is also potentially commercially lucrative, and the GDSs' own privacy policies give further cause for concern as they do not appear to exclude the renting or licensing of personal data nor their use for marketing analysis.

Other systems employed include CANPASS Air, for “low-risk” Canadian air travellers, NEXUS for citizens and selected residents of the USA and Canada countries, and the Passenger Protection Program Canada (Canada’s “no-fly” list). Whereas the OPC has previously argued that in CANPASS and NEXUS, “the privacy concerns raised by the programs are mitigated somewhat by their voluntary nature” (Stoddart 2007:3), with the expansion of such programs and international data sharing, such volunteerism is no longer a safeguard by itself.

A major concern is around the Secure Flight program of the US Transportation Security Administration (TSA), which demands personal information for flights to or from the US and for flights passing through US airspace. Moreover, it integrates many databases and enjoys large exemptions from the US Privacy Act.

2. Personnel at the Border

CATSA’s screening operations employ around 6,000 privately-employed screening officers supported by just over 390 direct CATSA employees, through four companies: Garda, Aeroguard, Shannahans’s Investigation and Security Limited in the Atlantic provinces, and Securitie Kolossal in Quebec. All are Canadian and Garda is the largest security services supplier to CATSA.

Airport employees have been trained in Behaviour Pattern Recognition (BPR) since 2009-2010. This gives rise to some serious concerns. In the previous screening process, the focus of screening was on prohibited items of all passengers, a clear and objective aim. However, with behavioural observation, the focus of screening is switched to the behaviour and appearances of people with the aim of selecting the potentially dangerous, a far more subjective and value-laden objective.

Employees are themselves subject to increasing surveillance through the biometric Restricted Area Identification Card (RAIC), and the need for Transport Security Clearance (TSC).

3. Border Technologies

These include full body scanners, e-passport systems and automated kiosks, biometric technologies and screening and X-ray Systems. Most of the corporate contracts to supply this equipment are to US-based companies.

CATSA has tried hard to mitigate the privacy risks of full body scanners, through a Privacy Impact Assessment (PIA) and multiple measures to anonymise and abstract images and limit the keeping of personal data. Though not yet formally assessed by the OPC, these measures appear to be significantly higher standards than those applied in the USA, where scanners remain controversial, particularly in the context of a larger debate about the Transportation Security Agency (TSA), its powers and practices.

Future Risks

The new proposed Perimeter Security Agreement (PSA), as foreshadowed in the 2011 formal bilateral declaration "Beyond the Border: a shared vision for perimeter security and economic competitiveness," proposes the instantaneous transmission of intimate personal data, the routine sharing of relevant personal data acquired by Canadian border security with the US, expanded investment in border technologies, trusted traveller and trader programs, and establishes a "Beyond the Border Working Group" (BBWG), which will report directly to the national leaders, not to Parliament or to Congress.

Conclusions and Recommendations

Personal data now flow with growing frequency between different governmental and private channels in relation to international travel. In Canada, this has created a number of difficulties for individuals, but they have largely been limited by the effective observance of applicable legislation, regulation and policy.

With the expansion in the numbers of "voluntary" programs for trusted travel, and the sharing of data across borders, volunteerism in itself no longer provides a safeguard, and the OPC should look again at privacy in these programs.

PIPEDA remains the primary act for safeguarding personal data where there is private involvement. However, the storage of Advance Passenger Information in US-based corporate servers, with unclear data protection policies and weak US laws provides little privacy protection for Canadians. Canadian law can apply, but enforceability would appear to depend on either a coincidence of the economic interests of particular corporations with those of Canadian law, or mutual agreement with other jurisdictions.

There are general concerns in information relationships with the USA and US companies, including the relative lack of accountability within US data-handling organisations, the out-sourcing to private companies of data transferred south to the US, and the exemptions that many state and private organisations involved in US Homeland Security enjoy even from US privacy law.

The new Perimeter Security Agreement (PSA) threatens to intensify these concerns and undermine Canadian expectations of privacy at the border. The agreement might also have knock-on effects on Canadian relationships with other countries and regions, particularly the EU, which at present shares a mutual high level of concern for privacy.

The OPC should develop a response to the PSA, and either:

- challenge the emerging agreements on grounds of the diminution of the privacy rights of Canadians; and/or
- work for the adoption of Canadian standards of privacy and data protection within any new agreement; and/or
- initiate or encourage new efforts at generating stronger international safeguards for the privacy of personal information and data protection above the bilateral level.

1. Introduction

1.1 National Security, which is always a central task of government, has become a matter of intensified concern in the wake of the 9/11 attacks on the United States and the following invasions of Afghanistan and Iraq. As shown by subsequent attacks on the United Kingdom, as well as failed attempts to attack the USA and alleged plots within Canada, the position of Canada as a key ally of the USA has introduced new matters of concern for national security (Lyon, 2003).

1.2 At the same time, national security has been used as a rationale for new laws and initiatives that call into question the future of key Canadian social values and legal rights, such as privacy and equal treatment under the law (Cockfield, 2004 and 2010). In particular, an emphasis on national security and the sharing of personal information in such a "climate of fear" can:

0 Produce profiles of individuals, that may be erroneous or based on everyday prejudice (OPC, 2009), and unjustly restrict individual freedom of movement, as with the "Watch Lists" and "No-Fly Lists" operated by individual governments and the UN (ICLMG, 2010);

1 Expand databases of personal information, and lead to the introduction of new practices and technologies of surveillance that have the potential to erode privacy rights, for example airport body scanners and behavioural observation;

2 Produce a "chilling effect" that reduces normal freedom of expression, political activity and demands for state accountability; and

3 In contrast, produce an "overheating effect", whereby national security becomes an overriding priority, often eclipsing the time-honoured commitment to freedom of movement and equality before the law.

1.3 While certain individuals and groups have been subject to targeted surveillance and intervention, particularly those who are most vulnerable, like asylum-seekers, immigrants and ethnic minorities, increasingly national security has become something that almost all citizens are likely to encounter. This happens most commonly through the operation of new laws that mandate the retention of extensive amounts of ordinary personal data, particularly those relating to telecommunications and international travel, in case it might one day prove useful or incriminatory (Zedner, 2009). Much contemporary security policy rests on expanded mass surveillance of this kind.

1.4 The increase in personal data collection, handling and sharing has drawn greater attention to the human rights that are actually and potentially damaged through such collection and sharing; in particular, the right to privacy. In Canada, under the oversight of the federal Office of the Privacy Commissioner (OPC) and the provincial Privacy Commissioners, the Privacy Act and the Personal Information Protection and Electronic Documents Act (PIPEDA) provide the legislative framework for personal data protection and privacy in government and private sector organisations. However, current developments may harm traditional Canadian democratic values and may, in the long run, make our nation less secure and damage Canada's international reputation as a guardian of privacy rights (McClennan and Schick, 2007). Results from the Globalization of Personal Data survey demonstrate that more than half of the people in Canada are skeptical with respect to protection of their personal information by the government (The Surveillance Project, 2008: 13). The effectiveness and relevance of Canada's privacy protective framework must therefore be under constant scrutiny.

1.5 However there is a further significant dimension emerging. Although a public interest, national security is increasingly provided either through government and private sector partnerships, or by private sector organisations operating on behalf of the state, part of an expanding "security economy" (Alyson et al., 2004; Stevens, 2004). Security is being outsourced to both Canadian and foreign companies and this has been a specific goal of national security strategies in several countries (see e.g. Morabito and Greenberg, 2005, on the USA). These initiatives involve:

0 The movement of personal information (handling, transfer, data-sharing and copying) between private and proprietary, and public and state systems, and across national borders (Gunasekara, 2007);

1 The transfer of security technologies between public and private sectors; and

2 Changes in practices and cultures of data management, which may be to the detriment of personal privacy and other social values.

1.6 Emerging research examines the private sector's role in shaping national security initiatives in other countries (Michaels, 2008; Lahav, 2008). However, no such research has been undertaken on Canada itself, leaving questions unanswered regarding the nature of Canada's government and private sector partnerships in pursuing national security and its social and privacy implications.

1.7 This exploratory study by the Surveillance Studies Centre (SSC) at Queen's University assesses the involvement of the private sector in national security in Canada, particularly in the area of borders and airports (O'Connor and Lippert, 2003; Adey, 2004a, b; Lyon, 2006; Côté-Boucher, 2008). There is significant private sector involvement in the shaping of Canada's national security agenda, and the management of specific initiatives (see Lippert and O'Connor, 2003), the collection, handling and sharing of personal data in national border and airport security in Canada, and the privacy concerns that arise. However, detailed specific and useful data are not currently available. In the last decade, we have witnessed an expansion and intensification of border security measures, both in Canada and in the wider world, along with an increasing demand from states for personal data on passengers and passengers-to-be. In this period, the quantity and types of data collected for the sake of border security has increased enormously; furthermore, data sharing between different organisations now appears to be taken more for granted.

1.8 The report has two main parts. The first consists of an inventory of private organisations involved in national border and airport security in Canada. In this section, the actual role of private firms, their areas of interest, their countries of origin, and their business connections are outlined. This is, of necessity, an overview rather than an in-depth analysis.

1.9 The extent of private sector involvement in Canadian national security initiatives opens a number of questions and concerns about the social and privacy implications of new security measures currently under discussion,[1] not just for Canadian citizens and residents, but also for those vulnerable populations which are subject to the most scrutiny at borders, in particular asylum-seekers, migrants and ethnic and religious minorities (ICLMG, 2010). The second part assesses the privacy challenges facing the Office of the Privacy Commissioner (OPC) in regards to the various types of data gathering, handling and sharing, either by the private firms, or the state, at the borders and airports. In this part, the type and amount of personal data that are currently shared, and are likely to be shared, between the private sector and the state are detailed. This part aims to reveal possible patterns of collection and sharing for various types of data. Therefore the corresponding data sharing programs and agreements, along with legal frameworks for safeguarding by the OPC, are also included in the assessment.

1.10 Furthermore, recent discussions on changes to border control regimes, in particular between Canada and the US towards the so-called "North American Perimeter," and changes to personal data sharing arrangements, either as a result of such border regime changes or through specific provision, create an important area of future challenges to Canadian privacy legislation and practices. Therefore, this report also considers such international data flows via private sector firms and agencies.

[1] e.g.: Bills C-46 and C-47

1.11 All four ways of transportation, air, marine, rail, and road, are used for cross-border travel in Canada. In the fiscal year 2006-2007, out of a total 95 million travellers, 74 per cent used highways while 23 per cent used airways and only three per cent used rail and marine.[2] The report aims to cover data flow in the different ways of transportation.

2. Methodology

2.1 Existing literature, including published and unpublished reports, books, and articles were reviewed and analysed to create a comprehensive picture of the legal frameworks and previous works on border security.

2.2 The websites, reports, action plans, budgets, and acts of Canada Border Services Agency (CBSA), Canadian Air Transport Security Authority (CATSA), Transport Canada and the OPC pertaining to the legal framework on personal data collection and sharing in national borders, were collected and analysed.

2.3 Other than Canadian national legislation, the national regulations of other countries are crucial for assessing Canadian privacy due to increasing international data sharing of many kinds, in particular the regulations of the US as the bordering country of Canada. As a result, the websites and documents of some key institutions, such as the US Department of Homeland Security (DHS) and the European Union (EU), are consulted in this research project.

2.4 A major initial data source for this research was a media review of websites, newspapers and magazines, which was employed to identify private sector firms in border security. For this media review, Canadian newspaper articles published since 2001 were searched using the Canadian Newsstand on ProQuest as the primary database.

[2] CBSA (2008) *Pre-arrival Targeting Evaluation Study*. http://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/ae-ve/2008/target-ciblage-eng.html [Accessed March 22, 2011].

Through a content analysis of Canadian news media publications approximately 143 news articles were indexed and summarised.

2.5 The results were then refined into a second database of private companies involved in border security. The company index includes information in following interests: country of origin, state beneficiary (partner), date of establishment, Canadian and non-Canadian partners, and main products/surveillance technologies. This index serves as a baseline for the inventory of private organisations involved in national border and airport security in Canada.

2.6 A third database of personal stories and complaints from individuals at the Canadian border was also compiled from news stories.

2.7 We sought to increase our knowledge on specific practices of private firms and key state institutions beyond their open sources and documents through a preliminary inquiry. We emailed them to inquire about their contracting partners and privacy polices. However, the private firms did not supply further documents regarding their confidentiality and non-disclosure policies, while state agencies provided their privacy policy documents.

2.8 The critiques of Canadian and US non-governmental organisations (NGOs), such as the International Civil Liberties Monitoring Group (ICLMG), Canadian Civil Liberties Association (CCLA),[3] Electronic Privacy Information Centre (EPIC),[4] the Identity Project,[5] and American Civil Liberties Union (ACLU)[6] provided significant insight into changing border security regimes and in some cases arguments for alternative approaches towards both border security and privacy. Personal communications with non-

[3] http://ccla.org/ [Accessed March 20, 2011]
[4] http://epic.org [Accessed March 20, 2011]
[5] http://www.papersplease.org/wp/ [Accessed March 20, 2011]
[6] http://www.aclu.org[Accessed March 20, 2011]

governmental organisations were also employed to summarise their critiques in this research.

2.9 Finally, recent national and international meetings and discussions concerning border security were reviewed for this project. Most such discussion and meetings (e.g. International Civil Aviation Organization Sixth Symposium and Exhibition on ICAO MRTDs, Biometrics and Security Standards, November 2010) were considered through their websites,[7] documents, and publications. However research team members participated in two related events. SSC team members contributed to a workshop entitled, The Political Economy of Surveillance, supported by SSHRCC through the New Transparency project, which took place in September 2010 in the UK. This event served as a good opportunity to discuss preliminary findings of this research. In November 2010, one of the team members participated in a panel titled "Privacy and Information Sharing: The Search for an Intelligent Border," organised by The Canada Institute of the Woodrow Wilson International Center for Scholars, Maclean's magazine, IBM, and CIBC. Panelists at this event included Mary Ellen Callahan, Chief Privacy Officer of the US Department of Homeland Security, and Wesley Wark, Munk School of Global Affairs, University of Toronto. This event was useful to comprehend some logical differences in the discussion of the border security and privacy between Canada and the US besides their tendency to harmonise regulations at the border (Callahan and Wark, 2010).

3. The Legislative and Institutional Framework

3.1 The Privacy Act and the Personal Information Protection and Electronic Documents Act (PIPEDA)

3.1.1 The Privacy Act and the Personal Information Protection and Electronic Documents Act (PIPEDA) have together formed the primary federal legislative framework for commercial transfers of personal data in Canada since January 2004. According to PIPEDA, commercial activities is an umbrella term which includes "selling, bartering or

[7] http://www.icao.int/MRTDsymposium/2010/Documentation.htm [Accessed March 20, 2011]

leasing of donor, membership or other fundraising lists" (PIPEDA, s.2[1]). The acccountability principle of PIPEDA (principle I) acknowledges that responsibility for personal information lies with the data collector.

3.1.2 Under PIPEDA, Canadian companies can outsource their personal information to foreign third party service providers. But the Canadian company remains accountable for the treatment of this personal information. So if the personal information is mistreated by the foreign third party then the Canadian company is liable for this mistreatment (Cockfield, 2010). However, determining who is the "owner" of personal data collected for travel, i.e., who is responsible for it, has become difficult; this has been complicated by the types of technologies being used for collection, process, and transfer, and role of private sector and government for the collection and the transfer of the personal data.

3.1.3 The third principle of PIPEDA, consent, requires individuals' knowledge and consent for the collection, use, or disclosure of personal information. However, for certain circumstances, knowledge and consent are not required: security is one such exception to this principle. Yet for some personal data collection processes at the border, industries' needs for their commerce and governments' needs for security cannot be easily separated. If we take the example of PNR data, this data can be collected for commercial reasons, then used and stored for security reasons, and stored by private firms and reused for commercial purposes. This sort of data collection and disclosure also creates complications for the second principle of PIPEDA, i.e. that of "identifying purposes." These issues are discussed in the Section 6.4.

3.1.4 According to PIPEDA's fourth principle, the collection of information shall be limited and collected for fair and lawful means. This principle applies to data collection that is supplementary to PNR data and the Passenger Protection Program (the Canadian no-fly list). This principle has also been acknowledged by the European Commission with regards to the PNR data exchange agreement between Canada and the EU (Hobbing, 2008: 37). However, as already noted by the OPC, Transport Canada uses lists which are established by other countries and which use methods of data collection and compilation that are not necessarily fair or lawful according to Canadian standards (OPC 2007a). The usage of the US no-fly list in Canada is a good example of this issue. These issues are detailed and discussed in Section 6.5.5.

3.2 The Aeronautics Act and Bill C-42, an Act to amend the Aeronautics Act

The Aeronautics Act, launched in 1985, is the primary document regulating aviation facilities. It includes regulation regarding the collecting of personal information of air passengers and crew, information required by foreign states, and prohibition of persons and goods in an aircraft.[8] Bill C-42 was introduced by the Minister of Transport as an Act to amend the Aeronautics Act on 17 June 2010. Bill C-42 creates an exception from PIPEDA and basically supplies the legal framework to provide information to foreign countries' authorities without consent when a flight is due to land in a foreign state or fly over the US.[9] Pragmatically, Bill C-42 extends usage of the US no-fly list to flights that fly over the US, including some domestic flights between two cities of Canada.[10] Despite remarkable public and parliamentary debates related to sovereignty issues, Bill C-42 was passed by the Canadian Parliament on March 2, 2011 and came into force following Royal Assent on March 23, 2011.[11]

[8] *Aeronautics Act.* http://laws.justice.gc.ca/PDF/Statute/A/A-2.pdf [Accessed March 20, 2011]

[9] Bill C-42 An Act to amend the Aeronautics Act. Available: http://www2.parl.gc.ca/HousePublications/Publication.aspx?Docid=5002078&file=4 [Accessed March 20, 2011]

[10] Very recently in February 2011, a British citizen, Dawood Hepplewhite, was stranded at Toronto airport when he attempt to fly from Toronto to the UK (flying over the US) because of the US no-fly list. http://www.allvoices.com/contributed-news/8222470-british-citizen-stranded-in-toronto-by-being-on-us-no-fly-list-finally-goes-home [Accessed March 22, 2011]

[11] See for related debates: Jennifer Stoddart (2010) Appearance before the House of Commons Standing Committee on Transport, Infrastructure and Communities on Bill C-42, *An Act to amend the Aeronautics Act November 18.* http://www.priv.gc.ca/parl/2010/parl_20101118_e.cfm [Accessed March 22, 2011]

3.3 The interaction of Canadian law with other legal regimes

3.3.1 Legal frameworks are not stable but dynamic. National laws interact with international laws and they are subject to changes. Therefore privacy watchdogs and ombudsmen such as the OPC have to deal with changing and interactive legal frameworks. In terms of transborder data flow, other states' legal frameworks are also crucial for data protection.

3.3.2 The US, for example, has no comprehensive and detailed personal information protection or privacy act but has particular acts for certain sectors such as banking and health. It is crucial for the focus of this study that there is no federal legislative framework in the US for the protection of personal data collected at borders. Moreover, the US government legalised the exemptions of the passenger monitoring program, Secure Flight, from the US Privacy Act in 2007. On the other hand, in recent years, Canada has put in place several agreements and border security programs, and has increased data exchange with the US. Potential threats with regards to interactions within North American territory and joint border security laws are discussed in the Section 8.

3.3.3 Canada has increased its exchange of personal data with EU countries. A comparison between the privacy frameworks in Canada and the EU demonstrates that the EU's privacy legislation, known as the General Directive (GD), has a high degree of compatibility with PIPEDA. The GD has become a "global standard," since it was the first legislative framework for protection of personal data, (1981). However, not all EU member-states meet the requirements of the GD.[12]

3.3.4 On January 14, 2010, CBSA published a guideline, Memorandum D1-16-3, on the rules concerning the usage and disclosure of PNR/API data to third parties and outside agencies.[13] Furthermore, Canada regulates the sharing of PNR data based on agreements with the US, the EU, and Switzerland. The Canada-US Smart Border Declaration and

[12] For a detailed international comparison with the PIPEDA see Cockfield, 2010: 67-68.
[13] http://www.cbsa-asfc.gc.ca/publications/dm-md/d1/d1-16-3-eng.pdf [Accessed March 22, 2011]

associated 32-point Action Plan regulate passenger data sharing with the US, API/PNR between the Government of Canada and the European Union (Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information and Passenger Name Record Data,[14] dated March 22, 2006) regulates data sharing with the EU, and finally a Memorandum of Understanding on API/PNR between CBSA and the Swiss Federal Office for Civil Aviation (dated March 17, 2006) regulates data sharing with Switzerland.[15]

3.4 Canadian State Agencies in Border Control

3.4.1 State agencies are the institutions primarily responsible for border and airport security in Canada. There are three key agencies involved: Canada Border Services Agency (CBSA); the Canadian Air Transport Security Authority (CATSA); and CATSA's regulatory body, the Ministry of Transport, Infrastructure and Communities (Transport Canada).

3.4.2 The main body is CBSA, which was established in 2003 and manages Canadian borders at 119 land-border crossings and 13 international airports. However, while there is a strong emphasis on state control over borders in Canada, CBSA strongly acknowledges the importance of public-private partnership:

> "As leaders and innovators in border management, we value our strong domestic and international partnerships and are dedicated to working together on critical safety, security and trade issues."[16]

3.4.3 Another state agency, CATSA was formed in 2002. CATSA works under the regulatory body of Transport Canada and reports to the Minister of Transport,

[14] Agreement between the European Community and the Government of Canada (Luxembourg, 3 October 2005) on the processing of Advance Passenger Information and Passenger Name Record data, OJ L 82/15, 21.3.2006. Available http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:082:0015 [accessed March 20, 2011]

[15] CBSA International Agreements available http://www.cbsa-asfc.gc.ca/security-securite/api_ipv-eng.html#intl [accessed February 10, 2011].

[16] http://www.cbsa-asfc.gc.ca/agency-agence/charter-charte-eng.html [accessed July 30, 2010].

Infrastructure and Communities. CATSA is responsible for pre-board screening (of passengers and their belongings), hold baggage screening, non-passenger screening, and restricted area identity card implementation at 89 airports. CATSA presents its objective as follows:

> "Before 9/11, screening at airports was the responsibility of airlines which, in turn, contracted these services to private companies. The use of private companies to screen passengers, using various standards and methodologies, quickly became a concern to the government. CATSA was created to deliver security screening services…" (CATSA 2009:4)

3.4.4 There are also several other state bodies, for instance Citizenship and Immigration Canada (CIC), the Royal Canadian Mounted Police (RCMP), and the Canadian Security Intelligence Services (CSIS), which work in cooperation with CBSA and CATSA on border security.

3.4.5 Other than national institutions and policies, international agreements provide the institutional framework for data collection and sharing in border security. Canada has changed or adapted many regulations in accordance with external negotiations and agreements, in particular in aligning its laws increasingly towards those of the US. In the years following the 9/11 attacks, the US has proposed agreements and programs to advance the monitoring and control over movements of both people and goods between the two countries. These will be considered in Part 2: Assessment.

PART I: INVENTORY OF PRIVATE ORGANISATIONS INVOLVED IN NATIONAL BORDER AND AIRPORT SECURITY IN CANADA

4. The Changing Security Business

4.1 There are many private companies in the border security business. In the last decade, particularly after 9/11, the number of security companies has expanded and their areas of business have diversified. Even so, the sector is still growing rapidly. Besides a remarkable increase in the number of firms and variation in their size, there is concentration of capital into larger firms, particularly American firms, via takeovers and mergers. According to the Treasury Board Contracting Policy of March 2004,[17] CBSA provides information about contracts over $10,000.[18] Although these contracts seem useful to evaluate private sector involvement, disclosure is limited to the value of the contract and a general description of services rendered.

4.2 This sectoral expansion results not least from an increasing reliance on the corporate sector to provide security “solutions,” and a major feature of this new security landscape is intensified state-corporate partnership. A large amount of research has underlined the growing importance of private sector in the areas of national (or homeland) security (e.g. Alyson et al., 2004; Asgary, 2009; Harknett and Stever, 2009; Kilibarda, 2008; Lahav, 2008; Salter, 2008; O'Connor et al., 2008; Spearin, 2009).

4.3 Private sector organisations have been intimately involved in the movement towards key developments such as the standardisation of national passports, the introduction of biometrics (in various circumstances), and the ‘light touch’ regulation that leads to a lack of public or even parliamentary scrutiny of state technological choices in the area of security. Technological improvements do not simply aim to satisfy increasing demand in

[17] http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=14494 [Accessed March 20, 2011]

[18] Disclosure of contracts over $10,000, http://www.cbsa-asfc.gc.ca/pd-dp/contracts-contrats/menu-eng.html [Accessed August 9, 2010].

security but rather aim to create increasing demand (Sparke, 2006: 159; Lippert and O'Connor, 2003).

5. Private Involvement in Canadian Border Security

5.1 In advance of travel

5.1.1 The main collection and processing, and therefore flow, of personal data occurs during reservations and subsequent transfers. According to the Immigration and Refugee Protection Act (IRPA), commercial transporting companies are obligated to provide *Advance Passenger Information* (CBSA 2008).

Table 1: Summary of Pre-Arrival Information by Mode of Transportation for Passengers and Crew

Mode	Information	Timeframes
Air - crew and passengers	API/PNR	Data must be provided upon takeoff or within 15 minutes of arrival in Canada. (Mandatory)
Marine - crew of commercial vessels	API from the crew manifest	As far in advance as possible, a minimum of 7 days prior to arrival (updated at the last port of departure before Canada). (Mandatory)
Marine - crew and passengers of cruise ships	API from passenger and crew manifests	As far in advance as possible, a minimum of 96 hours prior to arrival (updated at the last port of departure before Canada). (Upon request)
Rail – crew	Rail crew report	At least 2 hours prior to arrival at the port of entry. (Upon request)
Rail – passengers	API from passenger manifest	Information provided upon departure from the last station prior to arrival in Canada. (Upon request)
Bus	API	If requested, information provided upon departure from the last station prior to arrival in Canada. (Upon request)

Source: CBSA (2008)

5.1.2 The *Personal Name Record* (PNR) is the most well-known type of passenger data and was first introduced by travel companies for practical and commercial interests, namely in order to create a flexible and central travel booking system;[19] however, PNR subsequently became an indispensable tool for security controls. A Personal Name Record (PNR) is created for every air traveller at the time of ticket reservation and consists of an alpha-numeric record that links to the personal information of the passenger that are, other than name, specific to his/her travel. If passengers have more than one flight in order to reach their destinations, their PNRs are transferred to the other airlines. This record is also employed for hotel reservations and car rental services. In fact, PNR data is potentially open to yet more commercial interests and uses. The amount of information carried by the PNR differs from company to company, however, the mandatory information that should be included on the PNR are: (1) the name of the passenger(s); (2) contact details for the travel agent; (3) ticket (travel) details; (4) itinerary of at least one leg of travel; and (5) the name of the person making the booking. However, the PNR usually involves a variety of extra information. Information of interest in Canada is listed by CBSA (2010: 1-2) as follows:

- PNR locator code
- Travel agency
- Seat information
- Date of reservation
- Travel agent
- One-way tickets
- Dates of intended travel
- Split/divided PNR information
- Any collected Advance Passenger Information (API)
- Passenger Name
- Ticketing information
- Standby
- Other names on PNR
- Ticket number
- Check-in information
- All forms of payment information
- Seat number
- Billing Address
- Date of ticket issuance

[19] The automated reservation system was used by American Airlines for the first time in 1946 (Hobbing 2008: 4).

- Contact telephone numbers
- No show information
- All travel itinerary for specific PNR
- Bag tag numbers (baggage information)
- Frequent flyer information
- Go show information

5.1.3 Advance Passenger Information (API) is gathered for all travellers regardless of type of transportation. The API has an immediate surveillance background, and is collected for state authorities. The API includes information on the traveller's full name, date of birth, gender, citizenship or nationality and travel document data (reservation record locator) (CBSA 2010: 1). The API system used in Canada is PAXIS (Passenger Information System), which was launched in 2002. The API data is transmitted to the Canadian authorities prior to arrival of the traveller(s) but only after the departure of the commercial vehicle (ICAO 2003). Therefore, API data does not have a no-fly purpose in Canada.

5.1.4 Because PNR data originates in multiple locations and in multiple interactions, large numbers of travel companies all around the world are involved in its creation, analysis and sharing. However, the API/PNR data are hosted by Global Distribution Systems (GDS) (also known Computerized Reservation Systems-CRS). There are four global systems for GDS management: (1) Galileo, (2) Worldspan, (3) Sabre[20] and (4) Amadeus. Of these, Galileo and Worldspan are owned by Travelport, a private travel conglomerate held by the Blackstone Group, One Equity Partners and Technology Crossover Ventures. Sabre is property of Sabre Holdings Inc, owned by Silver Lake Partners and TPG Capital. Amadeus is owned by the Amadeus IT Holding S.A. Amadeus is based in Spain, while other three companies are based in the US. Recently, Edward Hasbrouck (2010) from the Identity Project launched a PNR map which follows transfers of PNR data between different countries including the EU countries and the US.[21] Our own illustrative diagram of the data transfers involved is in Appendix 1 (below).

[20] The first computer based reservation system, launched in 1959 (Hobbing 2008: 4).

[21] http://hasbrouck.org/IDP/IDP-PNR-BRU-8APR2010.pdf [Accessed March 20, 2011]

5.1.5 *CANPASS Air* is the pre-approved custom clearing program for “low-risk” Canadian air travellers. In this program, besides the assessment of a number of personal, criminal, and civil records, iris recognition is used for biometric confirmation of travellers.

5.1.6 *NEXUS* is another pre-approved custom clearing program which is open to air, highway, and marine travel between Canada and the US for citizens and selected residents of the both countries. RFID chips for the NEXUS program are manufactured by Intermec Corporation.[22]

5.1.7 *The Passenger Protect Program* (sometimes referred to as the ‘Canadian no-fly list’) was launched in 2007 and is operated by Transport Canada. Transport Canada collects personal data from various sources including Canadian and international security and intelligence agencies, private companies (mainly air carriers) to maintain a Specified Persons List (SPL). There is no confirmed case of information flows from the Passenger Protect Program to private companies. However one concern, which the OPC has already raised, is that Canada shares this SPL with foreign governments. Therefore this information could be disclosed regardless of consent and used for other purposes (OPC 2010)

5.2 Personnel at the Border

5.2.1 The Canadian Air Transport Security Authority (CATSA)’s screening operations function primarily through the contracting of private companies with a small internal support staff. Currently there are around 6,000 privately-employed screening officers supported by just over 390 direct CATSA employees. There are four contracted security companies that operate at airports across Canada:[23]

[22] See for Intermec’s brochure: http://www.intermec.com/public-files/case-studies/en/NEXUS_cs_web.pdf [Accessed March 20, 2011]

[23] CATSA ‘Pre-board Screening Officer’ Available: http://www.catsa-acsta.gc.ca/Page.aspx?ID=41&pname=AgentDeControle&lang=en [accessed August 9, 2010].

5.2.2 Garda holds contracts at both airports in Toronto (Lester B. Pearson and Toronto City Centre Airport). Garda also has contracts in British Columbia, Quebec, and in the Prairies (Calgary, Edmonton and Fort McMurray). In the contract period 2009-12-01 to 2012-11-30, CBSA awarded Garda a $2,173,934.68 contract.[24]

5.2.3 Aeroguard operates in the remaining airports in Ontario (i.e. all but the two Garda operates in Toronto), Vancouver International Airport (North and South Terminals) and Saskatchewan, Manitoba, Yukon, Northwest Territories and Alberta (apart from the three that Garda operates). In the contract period 2010-10-15 to 2010-12-31, CBSA awarded Aeroguard a $39,000.00 contract.

5.2.4 Shannahans's Investigation and Security Limited holds the Atlantic contracts (New Brunswick, Nova Scotia, Newfoundland and Labrador, and PEI).

5.2.5 Securitie Kolossal maintains the contracts in Quebec with the exception of Montreal, Roberval and Riviere-Rouge Mont-Tremblant airports.

5.2.6 This area, supplying as it does, human operatives, is unusual amongst the areas considered here in that all four companies are Canadian. Among them, Garda is the largest security services supplier to CATSA. In 2009, CATSA awarded Garda a $300 Million contract for airport security screening operations at 26 airports until 2011.

5.2.7 *Behavioural observation* became part of the new security measures for CATSA as of 2009/10 (CATSA, 2009a: 24). ASERO Corporation was given a $240,000 contract by CATSA to give behavioural observation training to CATSA employees, similar to the Screening Passengers by Observation Techniques (SPOT) program conducted by the US DHS. ASERO Worldwide, a Washington, D.C. based security consulting firm offers a

[24] For contracts with CBSA see http://cbsa-asfc.gc.ca/pd-dp/contracts-contrats/reports-rapports-eng.html [accessed March 22, 2011]

Homeland Security Executive Certificate Study Program with its two partners, ASIS International and Tel Aviv University.[25]

5.2.8 *Non-passenger monitoring.*

All employees and other individuals whose workplace is an airport and who provide service or deliver goods to an airport are themselves subject to different levels of security monitoring. Besides random security screening, all individuals who have access to airport restricted areas are required to hold the mandatory Restricted Area Identification Card (RAIC) which involves iris recognition and fingerprints as biometric identifiers. They are also required to hold a valid Transport Security Clearance (TSC) (CATSA, 2009a:7-8).

5.3 Technologies at the Border

5.3.1 Full Body Scanners.

There are two primary firms involved in manufacturing full body scanners for airports: Rapiscan Systems and L-3 Communications.

5.3.2 Rapiscan Systems, a division of OSI Systems, manufactures backscatter passenger screening technology, as well as hold baggage screening systems. Since 2004, Rapiscan has been receiving a steady supply of contracts from both the TSA and the DHS to research and manufacture backscatter and baggage screening technology, and it was recently named the official security equipment supplier for the London 2012 Olympic Games.[26] Based on an overview of the company's press releases, the majority of their contracts are centred around baggage screening, including a $325 Million indefinite delivery, indefinite quantity (IDIQ) contract by the TSA for the Rapiscan 620DV Advanced Technology checkpoint x-ray baggage inspection system.[27] Rapiscan's headquarters are located in Torrance, California, and has offices throughout the world including the United Kingdom, Australia, Malaysia and India.

[25] http://www.asero.com/content/newsroom/index.cfm?mmid=4&smid=5 [accessed February 18, 2011].

[26] http://www.london2012.com/press/media-releases/2011/03/london-2012-signs-rapiscan-as-tier-three-sponsor.php [accessed March 20, 2011]

[27] http://www.rapiscansystems.com/fullarticle.asp?newsid=206 [accessed March 20, 2011]

5.3.3 The second major contractor for full-body scanning technology is military and security contractor L-3 Communications, under their Security & Detection Systems branch, who manufacture the ProVision Whole Body Imager, a millimeter wave advanced imaging technology (AIT) passenger screener, the scanner currently used in Canadian airports.[28] In 2008, L-3 announced it was being awarded a US $24 Million contract to supply the TSA with 30 ProVision scanners.[29] In 2009 the TSA announced that the ProVision scanner was approved for use in aviation checkpoints,[30] and in 2010 the TSA awarded L-3 a US $164 Million IDIQ contract for ProVision scanners.[31]

5.3.4 E-Passport and Automated Kiosks.

The most important corporation identified in this area is 3M, and in particular its subdivision, 3M Security Systems. 3M became an active player in the electronic ID and document authentication market after acquiring the Canadian firm Advanced Information Technologies Corp. (AiT) in 2002.[32] It was AiT that, in 2001, was first awarded a CDN $1.7 Million contract to develop ePassport software called EnTReX for the Canadian Government. During the 2002 merger with AiT and 3M, a controversy developed over AiT CEO, Bernard Ashe, who was implicated by the Ontario Securities Commission (OSC) in a series of unusual trading in AiT shares, culminating in the OSC accusing Ashe, and associate Deborah Weinstein, for failing to disclose the merger with 3M. After an in-depth inquiry, it was determined by the OSC that there was no material change in the business and AiT was therefore not required to make timely disclosure of its negotiations with 3M.[33] In 2010, the CBSA announced 3M had awarded a CDN $2 Million con-

[28] http://www.l-3com.com/products-services/productservice.aspx?type=ps&id=866, http://www.catsa.ca/File/Library/72/English/full_body_scanner.pdf [accessed March 20, 2011]
[29] http://www.sds.l-3com.com/pdf_news/2008_10_28_L-3_Supplies_TSA_wRevolutionary_MillimeterWave_Imaging_Portals.pdf [accessed March 20, 2011]
[30] http://www.sds.l-3com.com/pdf_news/2009_12_03_TSA_Approves_L-3's_ProVision_MillimeterWave_CheckpointScreeningSystem.pdf [accessed March 2, 2011]
[31] http://www.sds.l-3com.com/pdf_news/2010_02_23_TSA_Awards_IDIQ_Contract_L-3_ProVision_CheckpointScreeningSystem.pdf [accessed March 20, 2011]
[32] http://www.businesswire.com/news/home/20020719_222002097_legacyID/en/3M-AiT-Conclude-Merger [accessed March 20, 2011]
[33] http://www.osc.gov.on.ca/documents/en/Proceedings-SOA/soa_20070208_aitadvanced.pdf and http://www.dwpv.com/en/17623_22380.aspx [accessed March 20, 2011]

tract to produce its Full Page Document Reader "to capture data from travellers' documents and enhance security at border crossings."[34]

5.3.5 Furthermore, in 2010, 3M acquired Biometrics giant Cogent Systems Inc. for approximately US $943 Million.[35] Cogent has been a major supplier of automated biometrics technology, a US $4 Billion global market. The merger effectively enables 3M to gain a stronger foothold in vertical integration of ePassport technology. This position was further emphasised when, in January 2011, 3M debuted the world's first Multilateral Border Crossing Program for participating nations of the Caribbean Community (CARICOM), called CARIPASS, a voluntary travel card program which provides "secure and simple border crossings for citizens and legal residents of ten CARICOM nations."[36] We expect to see 3M and others to make a strong marketing effort to infiltrate such multilateral border crossing technologies into other multinational agreements for regulating traveller mobility in the Americas and beyond.

5.4.6 3M has also been working with ePassport pioneer Entrust. In 2008, Entrust announced a partnership with 3M to provide end-to-end secure ePassport readers to help governments ease the transition towards ePassport technology.[37] In 2010, an Entrust press release stated that Entrust was working in consultation with the Government of Canada to advance Canada's Digital Economy Strategy, including developing proper security and citizen privacy policies, including ePassport initiatives.[38]

[34] http://multimedia.3m.com/mws/mediawebserver?mwsId=66666UuZjcFSLXTtnXf2lXMVEVuQEcuZgVs6EVs6E666666--&fn=ePassport%20CBSA.pdf [accessed March 20, 2011]

[35] http://www.businesswire.com/portal/site/3m/index.jsp?ndmViewId=news_view&ndmConfigId=1000941&newsId=20100830005617&newsLang=en[accessed March 20, 2011] http://www.businesswire.com/portal/site/3m/index.jsp?ndmViewId=news_view&ndmConfigId=1000940&newsId=20101201006920&newsLang=en&vnsId=3M-Completes-Acquisition-Cogent[accessed March 20, 2011]

[36] http://multimedia.3m.com/mws/mediawebserver?mwsId=66666UuZjcFSLXTtOXTynxM_EVuQEcuZgVs6EVs6E666666--&fn=Multilat_Border_Crossnig_PR.pdf [accessed March 20, 2011]

[37] http://www.entrust.com/news/index.php?s=43&item=628[accessed March 20, 2011]

[38] http://www.entrust.com/news/index.php?s=43&item=713 [accessed March 20, 2011] http://www.ic.gc.ca/eic/site/ic1.nsf/eng/05531.html[accessed March 20, 2011]

5.3.7 Biometrics.

Although biometrics are in many respects on the horizon for passengers, it has been a requirement for airport personnel, most notably with CATSA's Restricted Access Identification Card (RAIC) system. A number of firms were contracted to develop the RAIC system. In terms of fingerprint readers, CATSA contracted out Canadian firm Acme-Future Security Controls Inc (A-FSC) in 2005 to be the exclusive supplier of RAIC biometric fingerprint readers. A-FSC in turn subcontracted out the manufacturing to another Canadian firm, BioScrypt Inc. In 2008, BioScrypt was purchased by U.S. L-1 Identity Solutions, a major firm involved in biometrics and border security technologies. This concentration of firms became even more intense when, in 2010, it was announced that European defence contractors Safran and BAE Systems were planning to absorb L-1. BAE purchased L-1's consulting division for $300 Million whereas Safran announced it was purchasing L-1 for $1 Billion,[39] clearly indicating that biometrics technology is quickly becoming a concentrated, yet highly valuable, market for future border security concerns. In addition to fingerprinting, the RAIC system uses LG300 iris readers and contactless access cards manufactured by HID Global and off-the-shelf products from ImageWare Systems, such as the IWS biometric engine – the centrepiece of the RAIC system responsible for enrollment of airport workers, which captures and processes their biometric data and issuing biometric-enable smart cards.[40]

5.3.8 In addition to the biometric component, CATSA's RAIC system depends also on database technology. In 2004, Unicom, was awarded a CDN $2.3 Million contract to build the RAIC database. The contract soon became embroiled in massive overspending and poor oversight; an audit revealed the contract was over-budget by approximately CDN $11 Million and Unicom was quickly dropped. In 2008, CATSA awarded a new CDN $ 4.5 Million contract to Unisys.[41]

[39] http://www.ibtimes.com/articles/63842/20100920/safran-buys-us-biometrics-firm-l1-for-1-09-bln-to-bolster-homeland-security-business.htm[accessed March 20, 2011]

[40] http://www.canadiansecuritymag.com/Securing-the-Nation/News/Unisys-to-integrate-new-ID-management-system-for-airports.html?print=1&tmpl=component[accessed March 20, 2011]
http://www.hidglobal.com/documents/lgiris_irisaccess_catsa.pdf[accessed March 20, 2011]

[41] https://www.unisys.com/about__unisys/news_a_events/05078877.htm[accessed March 20, 2011]

5.3.9 Cross Match Technologies has also been identified as an important firm in the biometrics market as they have been involved in developing ePassport technology, the TSA's version of the RAIC system, known as the Transportation Worker Identification Credential (TWIC), and the US-VISIT program which utilises Cross Match fingerprint scanners at 115 airports and 14 seaports.[42] Cross Match is a major supplier of fingerprint reading technology for law enforcement agencies, visitor management and computerised access control.

5.4 Future Integration

5.4.1 As the security industry continues to become evermore concentrated into more powerful, vertically integrated firms such as 3M and Safran, and moreover as biometric and e-documents continue to proliferate, future integration will likely continue into the well foreseeable future. This is particularly supported by the fact that a variety of firms are already experimenting with seamless border management systems. As already mentioned, 3M is currently testing multi-national border management systems in the Caribbean, however there are other examples to support this prediction.

5.4.2 Farelogix, an industry leader in the travel industry in developing "lower-cost distribution models" for travel suppliers, is currently developing a number of systems designed to provide total content acquisition for travel suppliers and sellers. In essence, the various software packages seek to redefine PNR and GDS systems to make them far more robust, effectively allowing the system to operate "underneath" any third party or proprietary point-of-sale application, allowing multiple point of sale options and total content sourcing.[43]

5.4.3 Another prominent example is the Swiss firm, SITA, arguably one of the biggest firms in the aviation industry. SITA is currently developing ubiquitous border manage-

[42] http://www.crossmatch.com/transportation.php[accessed March 20, 2011]

[43] For an interactive diagram, see: http://www.farelogix.com/flx.php[accessed March 20, 2011]

ment solutions, a product known as iBorders BioThenticate, which is designed to allow governments, airlines and airports to automate identity management for passengers and airport workers. Using a combination of biometrics and e-documents, SITA is developing a seamless system to process passengers from port-to-port, from check-in to arrival, covering any steps in between. Moreover, the system is designed to maximise self-service while ensuring integrated security, effectively requiring a ubiquitous surveillance apparatus based on massive information exchange.[44] SITA is specifically problematising the way passenger information is collected and processed, and seeks to market themselves as able to develop a seamless system of information collection, integration, processing and identity management throughout all stages of a passenger's experience. This includes the collection of passenger identifiers such as personal information and biometrics for seamless border management and control.[45]

[44] http://www.sita.aero/product/iborders-biothenticate [accessed March 20, 2011]
[45] http://www.sita.aero/content/border-management[accessed March 20, 2011]

PART II: ASSESSMENT

This part of the report aims to assess actual and potential threats to privacy resulting from the collection, handling and sharing of personal data for the purposes of border security, with a specific emphasis on the involvement of the private sector. CBSA has the main responsibility for personal data collection for state security at the border. However, data can be shared with other state organisations, acquired in the first place by other state or private organisations (such as airlines), shared between state and private organisations, between different states, and between foreign states and the private sector. Considering possible patterns of data flow, we analyse and assess what data is known to be currently shared and what data is likely to be shared in the future.

6. Pre-arrival Data Collection

6.1 The processes involved in immigration and granting visas necessarily include security assessments. The Citizenship and Immigration Canada (CIC) and Canadian visa offices are responsible for these tasks. Information collected during these procedures is shared by different state bodies in Canada. The Immigration Intelligence network of the CBSA is a strong partner.[46]

6.2 Pre-arrival risk assessment for travellers is based on the idea of sorting dangerous and low-risk travellers plus goods as well as enabling the pre-emptive banning of dangerous passengers and goods in advance of travel.[47] In Canada, Protection of Passenger Information Regulations (PPIR) under the Immigration and Refugee Protection Act (IRPA) is the legal framework for mandatory collection of passengers' information by

[46] For further information, see: http://www.cbsa-asfc.gc.ca/media/facts-faits/031-eng.html [accessed August 16, 2010].

[47] For further information, see: http://cbsa-asfc.gc.ca/agency-agence/reports-rapports/ae-ve/2008/target-ciblage-eng.html [accessed August 25, 2010].

commercial transporting companies. The PPIR also regulates the use and disclosure of PNR/API data.[48]

6.3 Advance Passenger Information (API) and Personal Name Record (PNR)

6.3.1 After being introduced and used by airline companies for commercial and practical uses related to air travel for around 40 years, governments in different countries, beginning with the US government, have started to use PNR data for security purposes. Since November 19, 2001, as a result of the US Aviation and Transportation Security Act, PNR has become mandatory information before take-off for US destinations. This act has affected regulations in other countries and was followed by the Canadian Public Safety Act of November 22, 2001 and the US–Canada Smart Border Declaration of December 3, 2001.

6.3.2 In Canada, PNR data is collected primarily for air travel, while API data, which is mainly collected for surveillance purposes, is mandatory for all modes of travels. Table 1 demonstrates the mode, information, and time frames of pre-arrival information by type of transportation. API/PNR is used by targeting and intelligence officers for the first 72 hours then depersonalised and stored for three and a half years (42 months). The information can be used for no other purpose than border management. During this period the API/PNR data can only be re-personalised by the President of the CBSA.[49] Commercial airlines have a role in creating and using PNR data. However, commercial airlines have no official access for the use of this data, including meal and seat preference. The usage, storage, and sharing of API/PNR data are regulated by the OPC, based on a Privacy Impact Assessment (PIA).

6.3.3 However, even though the procedure may appear clear and comprehensive, the globalised nature of PNR data results in some complicated privacy concerns (see Section

[48] For further information, see: http://cbsa-asfc.gc.ca/agency-agence/reports-rapports/ae-ve/2008/target-ciblage-eng.html [accessed August 25, 2010] and CBSA (2008).

[49] For further information, see: http://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/api_ipv_20051003-eng.html [accessed July 29, 2010].

3, above), which has been discussed by NGOs, academics, and Privacy Commissioners of different countries.

6.3.4 Bennett (2005: 118-119) followed the route of his own PNR data for domestic flights in Canada and international flights to the US, and describes data transfers through one of the GDSs, Galileo, for his journey. He highlighted the delocalisation of the border and extraterritorial data flow, however he remained optimistic about the level of protection for personal data – at least within Canada (Bennett 2005: 131).

6.3.5 Another important report was produced by Hobbing (2008) as part of the EU–Canada project, funded by the "Relations with the US and Canada" section of the European Commission Directorate-General for External Relations. In this report, Hobbing comments on three significant acts regulating the flow of PNR data between the EU and Canada, and the EU and the US. The European Union itself and privacy watchdogs in the EU countries seem comfortable with the legal framework and agreement on international data sharing for border security between Canada and the EU (Hobbing 2008: 40). The EU seems satisfied with the clear agreement with Canada concerning API/PNR data, whereby data is not transmitted before flight departure but prior to flight arrival. This prevents the PNR data from being employed for no-fly purposes; instead it is only employed for secondary screening.

6.4 Key vulnerabilities in PNR/API data

6.4.1 PNR data is not collected by one single institution. After the code is created by the travel agent who made the reservation, the total content of data is made up by inputs from different agents (travel agencies, hotels, rental services). Even if there is only one data subject, passenger or passenger to-be, the multi-agent procedure by which the data is created results in some complications as to who is the owner of (and thereby responsible for) the data, according to the accountability principle in PIPEDA.[50]

[50] See: PIPEDA, 2000, c.5. s.4[1]

6.4.2 While governments insist on PNR data for security checks, there are two methods of data transfer from travel agencies to states: “push” and “pull” methods. In the case of the pull method, the state has access to all of the data and can work with the whole data set. In the case of the push method, travel agencies select and transfer data considered of interest to the state. Travel agencies do not pay significant attention to this difference, and if there is no regulation they adopt the pull method. The EU is very conscientious about this difference but reports its concerns about the US tendency to use pull method without first trying “push”. This concern has not been yet introduced in Canadian official documents.

6.4.3 Many concerns surround data sharing with the US. Three of the four GDSs are located in the US and the US has no federal law to limit usage and the disclosure of the travellers’ data. However, there appears to be an absence of research on global commercial interests in passenger data. Since PNR data is essentially a huge store of information about the preferences and tastes of travellers, they are a very attractive source of potential added value for private companies.

6.4.4 According to PIPEDA, private firms are not legally allowed to share, sell or disclose the personal data. However, PNR data, even those created for domestic flights, are hosted by the four GDSs, none of which are Canadian-based. As noted in Section 3 (above), Canadian law remains applicable to Canadian-derived personal information in US-based GDSs. The key case in establishing this was that of the OPC vs. the Society for Worldwide Interbank Financial Telecommunication (SWIFT), the European-based money transfer system between banks in different countries. The findings concluded that SWIFT is subject to PIPEDA but that in this particular case it had not broken the law by disclosing personal information from Canadian financial institutions to the US Treasury Department (OPC 2007b). The Commissioner was quoted as arguing that “[s]imply because companies might operate in two or more jurisdictions does not relieve them of their obligations to comply with Canadian law” (OPC 2007c). In addition, the OPC has some successful stories with respect to extraterritorial law enforcement against large accumulators of personal data such as Facebook (Davies, 2010) and Google.[51] The enforcement in these cases is essentially a form of "shaming" where the OPC issues a letter and press release to remind the foreign party that they must comply with PIPEDA. In the case of Google, where Google Street View photographic cars had been secretly collecting personal information from unsecured wireless networks as they drove around, Canada was the only one of a large number of Privacy Commissioners, most of whom were in Europe, to put pressure on the company; essentially this was concerted or at least synchronous international action from countries with very similar privacy laws. In the case of Facebook, one could argue that the ease with which the company agreed to the request of the OPC – and indeed went further than necessary and applied the same changes worldwide – has as much to do with the limited costs and difficulties involved in compliance, and might not have given in so easily had the stakes been higher. Enforcement thus remains a major issue, even when applicability of national law beyond borders is recognised.

6.4.6 GDSs have their own privacy policies, which have several noteworthy features. The first point concerns further commercial usage of the data. Edward Hasbrouck alerts us to GDSs' tricky language with respect to the limits on commercial usage of the data.[52] According to Travelport's Privacy policy,[53]

> "We do not sell GDS Personal Information for purposes of allowing third parties to conduct direct marketing for their own products or services."

Similarly it is mentioned within Sabres's privacy policy[54] that

> "We will not sell or give the personal information individuals provide through the use of any of our products or services to any unaffiliated party."

[51] Privacy Commissioner Investigates Google WiFi Data Collection. Available: http://www.priv.gc.ca/media/nr-c/2010/nr-c_100601_e.cfm [Accessed March 19, 2011].

[52] Personal communication with Edward Hasbrouck, February 17, 2011.

[53] http://www.travelport.com/legal/privacypolicy.aspx [accessed March 20, 2011]

[54] http://www.sabre-holdings.com/privacy/coreData.html

Such statements make it seem like the data is protected from the use of third parties. But these are useless when the company does not “sell” or “give [the data] as a gift,” but instead “rent” or “license” the data. And in practice, such data is more convenient for renting or licensing rather than selling. This concern includes, but is not limited to, the terms of contract between Canadian travel agencies which produce the data because personal data of travellers is potentially global in scope. Sabre states in its privacy policy that

> “We or our affiliates (including those affiliates partly owned by third parties) may use personal travel information for individuals that we acquired through the use of any of our products or services for marketing analysis.” [55]

In other words, Sabre may use the PNR data for marketing analysis.

6.5 Other Pre-Arrival Programmes

6.5.1 Besides pre-arrival assessment using an API/PNR for every traveller, there is a strong tendency to categorise people (travellers) and companies (in cross border business) in terms of their level of trust. Various programs are employed to sort trusted, neutral, and high risk travellers.

6.5.2 Trusted Traveller Programs

FAST and Partners in Protection (PIP) are CBSA programs for trusted companies. CANPASS Air and NEXUS are trusted traveller programs, where CANPASS is for Canadians arriving in Canada.

NEXUS is for low-risk pre-approved passengers crossing the border between Canada and the US. CBSA and US Customs and Border Protection (CBP) are cooperating on the program. In April 30, 2010, after eight years of operation, NEXUS reached its

[55] *ibid.*

400,000th member. NEXUS is available at all major Canadian airports, at 17 land border crossings and at over 430 marine ports of entry. NEXUS cards can be proof of identity for air (in participating airports), land and marine travel.[56] Besides the personal information provided and the security background checks that an applicant needs to undergo, biometrics, fingerprints of two index fingers and a digital photograph of the face are provided by the applicant.

The NEXUS program makes use of RFID cards. The US government declares that the RFID only store a limited amount of data, specifically, a GES number (Global Enrollment System), meaning that the RFID consists of just a number, a key, to access another database. So in effect, there is not any confidential information on the RFID; the GES simply acts as a key to access a database at the officer workstation at the border.[57]

Members of the NEXUS program are under the protection of both the Canadian and the US Privacy Statements.[58] In these acts it is noticed that data may be shared with other government agencies in Canada and the United States of America.

NEXUS is offered at the following airports:

3 Halifax Robert L. Stanfield International Airport
4 Montréal-Pierre Elliott Trudeau International Airport
5 Ottawa Macdonald-Cartier International Airport
6 Toronto Lester B. Pearson International Airport
7 Winnipeg James Armstrong Richardson International Airport
8 Calgary International Airport
9 Edmonton International Airport
10 Vancouver International Airport

[56] News Release National 2010 http://www.cbsa-asfc.gc.ca/media/release-communique/2010/2010-04-30-eng.html [Accessed March 20, 2011]
[57] http://www.dhs.gov/xlibrary/assets/foia/US-VISIT_RFIDattachD.pdf[Accessed March 20, 2011]
[58] http://www.cbsa-asfc.gc.ca/prog/nexus/privacy-privee-eng.html [Accessed March 20, 2011]

6.5.3 High Risk Travellers.

While current border security strategy aims to select trusted travellers, it also, on the other hand, aims to find – and ban – high-risk people. The well-known 'no-fly list' is created by the US. The list is in use not only for flights with a US destination but also for transit flights, i.e. flights transferring in the US as well as those whose path of travel goes into US airspace.

6.5.4 Transport Canada conducted a PIA of its own 'no-fly list', the Passenger Protect Program, about which the OPC expressed several serious concerns (OPC 2010). In particular, with regard to the relationship with private companies, it found that a Memoranda of Understanding (MoU) signed with air carriers in order to obtain API "contained minimal privacy and data protection provisions" and indeed Transport Canada itself had "no records retention and disposal framework for personal information related to the Program." Finally, the procedures for checking the accuracy of data and for the correction of false information were inadequate. Overall, the OPC remains "apprehensive" about the misuse of personal data in this program, despite Transport Canada's acceptance of all the OPC's recommendations.

6.5.4 Canada-United States Integrated Border Enforcement Teams (IBETs) is another program to discover and stop the movement of high-risk passengers and goods between the Canada-US border. The mission of the program, in their words, is as follows:

> "IBETs will enhance border integrity and security at our shared border by identifying, investigating, and interdicting persons and organizations that pose a threat to national security or are engaged in other organized criminal activity."[59]

6.5.5 The Secure Flight program was introduced by the US Transportation Security Administration (TSA) in order to extend their scrutiny of travellers and airport personnel in October 2009.[60] According to this program, personal and travel information of people

[59] http://www.cbsa-asfc.gc.ca/security-securite/ibet-eipf-eng.html [accessed July 29, 2010]

[60] http://www.tsa.gov/assets/pdf/nprm_pae.pdf [Accessed March 20, 2011]

in the program apply not only for flights to or from the US Integrated Border Enforcement Teams, but also for flights passing through US airspace. Moreover, on November 9, 2007, the United States Federal Register published a document, 49 CFR Part 1507, detailing the exemptions of Secure Flight from the US Privacy Act. The exemptions were the result of an ongoing process, following a Notice of Proposed Rulemaking (NPRM) and public comment to amend TSA regulations by exempting the Secure Flight database from several provisions of the Privacy Act. Of interest is that the document reveals that the TSA received numerous comments from the Electronic Frontier Foundation (EFF) and Electronic Privacy Information Center (EPIC).[61]

This program has already received important criticism from civil initiatives and the OPC itself. The Canadian Parliament never adopted nor discussed the Secure Flight Program, thus it was effectively accepted without any Canadian democratic process being involved. However Bill C-42[62] now provides a legal framework to apply the Secure Flight Program No-Fly List, not only for flights which terminate in the US but also those which merely enter US airspace.

It is pertinent here to draw attention again to the enormous data processing ability of the program and its potential threat to privacy. The Secure Flight Program enables the TSA to access the full Terrorist Screening Database (TSDB) or other US government databases. Under the Secure Flight Program, airlines submit flight manifest (list of passengers) 72 hours prior to take off. The TSA then uses Infoglide, a package of 50 "identity resolution" algorithms to conduct a risk assessment on the submitted flight plan. Although Infoglide is a small firm, it is partnered with the security giant L-3 Communications, who resells Infoglide's Identity Resolution Engine to customers in the federal homeland security market.

The core of Infoglide's software is the patented Identity Resolution Engine (IRE) which

[61] A detailed report of the comments made by EPIC and EFF can be found here: http://www.tsa.gov/assets/pdf/nprm_pae.pdf [Accessed March 20, 2011]

[62] See Section 3, above.

is, in short, the ability to collate discrete data elements from a myriad of unrelated databases and then merge them into one for the purposes of hierarchical sorting, a process necessary for risk and compliance assessment. It is essential to know that the IRE does not require the migration of data from one database to another larger one or data centre. It performs instead what is known as federated searches. The software simply accesses the database in its native location and does not require the data be copied.[63] The implication is that Secure Flight does not necessarily need to take responsibility for the accuracy of the information it accesses on other agency databases. Incidentally, the TSA also sought an exemption on record maintenance from the 1974 Privacy Act, on the grounds that they cannot verify the quality of information collected by other agencies such as law enforcement departments. The TSA also believes that seemingly benign information collected today may acquire significance in the future, stating that:

> "In the collection of information for law enforcement, counterterrorism, and intelligence purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation reveals additional details" (49 CFR Part 1507, 2007: 63708).

6.5.6 Appendix 1 (below) is our own illustrative diagram of the corporate connections and potential data transfers involved around API and Secure Flight.

7. At the Airport

7.1 *Full Body Scanners*

7.1.1 After full body scanners were first used at the Kelowna Airport, BC for a one year trial period, a PIA was carried out by CATSA in Nov 2009 (CATSA, 2009b). Following OPC recommendations (OPC, 2010), CATSA then reported that they were addressing all

[63] Infoglide Software Identity Resolution Engine, http://www.infoglide.com/PDF/IRE-for-Government-US.pdf [accessed March 3, 2011], and Infoglide Software Identity Resolution Engine Datasheet, p.4, http://www.infoglide.com/PDF/IRE-Datasheet.pdf [accessed March 3, 2011].

risks through risk mitigation strategies that are in line with privacy best practices, including the following in relation to personal data:

- Making the screening process voluntary and anonymous;
- Ensuring that the images are immediately and permanently deleted once the screening process is complete;
- Ensuring that the imager cannot store, print or save the images;
- Ensuring that the images reviewed during the screening process cannot be accessed by or transmitted to any other location;
- Ensuring that the images are exclusively reviewed by a Screening Officer located in a remote viewing room;
- Not correlating the images in any way with the name of the passenger or any other identifying information.

7.1.2 Their usage has already moved beyond the trial stage. Scanners have been in place at other airports since January 2010 following the attempted attack on a Delta Airlines flight from Amsterdam to Detroit on December 25, 2009.[64]

7.1.3 Since full body scanners as used in Canada do not collect, store, or share personal information, the potential privacy threat from these systems is more in the domain of physical bodily privacy, and even then the affective (emotional-psychological) perception of intrusion or infringement varies and may or may not be considered by any individual as more intrusive than that a physical search. Such issues are important and need to be discussed, however they are beyond the scope of this report. In this regard, the OPC is already aware that CATSA is developing software that will generate a more schematic rather than lifelike image of the body (OPC, 2010), which may help allay some concerns about bodily privacy.

[64] http://www.catsa.gc.ca/File/Library/72/English/full_body_scanner.pdf [accessed August 24, 2010].

7.1.4 Such issues remain more controversial in the US, where fewer steps have been made to allay privacy concerns than in Canada. If US laws and expectations begin to influence or supplant Canadian ones more generally, this could throw progress towards the control of body scanners on grounds of privacy into disarray (see Section 8).

7.2 Behaviour Recognition

The Canadian Government approved Behaviour Pattern Recognition (BPR), the development of the Critical Restricted Area (CRA), and screening at Fixed-Base Operations (FBO) as new security measures for CATSA from 2009/10 (CATSA, 2009a: 24). In the previous screening process, the focus of screening was on prohibited items of all passengers. However, with behavioural observation, the focus of screening is switched to the behaviour and appearances of people, with the aim of identifying the potentially dangerous. CATSA has now contracted for training and the project has started.

7.3 Passenger data collected and processed by duty-free shops

7.3.1 Shops at airports and land border crossings provide tax-free sales for customers who are about to leave Canada. Personal information is collected and stored for confirmation of the eligibility of travellers in order to avoid abuse of tax exemptions as well as for any control of duty free shops by authorities. There is no specific act for the protection of personal data collected at duty-free shops but PIPEDA applies for duty-free shopping.

7.3.2 A European Commission working party has produced a report on privacy concerns about passengers' data collected and processed by duty-free shops.[65] Some of the key points that came out of this report are useful in the Canadian context, namely that the quantity and the quality of data collected and stored at duty-free shops should be limited for its purpose, and that subjects (travellers) should be informed about the data gathering.

[65] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp167_en.pdf[Accessed March 20, 2011]

8. Towards a North American Perimeter?

8.1 This project demonstrates that while data remain in the care of Canadian corporations there are safeguards in place that appear to work, and that once data has been transferred outside of the Canadian border PIPEDA continues to apply although, as with any extraterritorial application of national law, this applicability is always limited by practical problems of enforcement beyond Canadian territory.

8.2 However everything could change with the new proposed Perimeter Security Agreement (PSA). The PSA is still in negotiation between Canada and the US, with the aim of harmonising rules and practices for goods and people at borders. The perimeter debate is not a new one and was on the agenda of both governments before 9/11 (Gilbert, 2008; Haggart, 2001), and its background and prospects are important to consider here.

8.3 Canada has several joint border security laws with the US. These Acts have various foci in terms of types of border (air, marine, rail, or highway), units of targeting (individual/passenger or good/cargo), level of risk (high risk passengers/firm or trusted passengers/firms), and legal and illegal border traffic. Canada and the US have (or had) the longest non-militarised border in the world.

8.4. Government and industry recognise that Transborder Data Flows (TBDF) continue play a vital role in all sectors of the economy, and are seen as having the capacity to enhance productivity and innovation, particularly in the context of the global marketplace. In 2004, Canadian e-commerce sales in the public and private sector totalled CDN $28.3Billion, an almost 50 per cent increase from 2003. The United States totalled US $69.2Billion (SPP 2005: Annex A). Because such trends are likely to continue, there have been numerous efforts to bolster North American prosperity, both in terms of the economy and security, through TBDF.

8.5 The Security and Prosperity Partnership of North America (SPP)

8.5.1 One such method of increasing TBDF has been through hybrid organisations comprised of both actors from the public and private sector, either officially or not, working on relevant policy issues such as border harmonisation and economic fitness.

8.5.2 The Security and Prosperity Partnership of North America (SPP) is an ideal example of this type of organization. Established in 2005 and dismantled in 2009, the SPP was a tri-national partnership between Canada, Mexico and the United States that sought to increase North American economic competitiveness and security via facilitating Transborder Data Flows (TBDF).

8.5.3 Under the SPP, ministers for the Department of Industry Canada, Mexico's Ministry of the Economy and the US Department of Commerce developed in 2005 an agreement on developing and conducting electronic commerce and online business throughout North America known as "A Framework of Common Principles for Electronic Commerce." (SPP 2005) The framework sought to assess potential barriers to TBDF under an overarching framework of online security and privacy protection, arguing that increased partnerships and co-operation amongst all sectors of governance and business are necessary to reduce impediments to TBDF and secure eCommerce initiatives. The document argues that in order to maximise North American innovation, governments should continue to work towards facilitating the free flow of information across borders by developing internet-based business solutions by enterprises, and stress that mutual co-operation is essential in order to foster transborder commerce. This requires:

- governments to establish and maintain legal and policy frameworks for online commerce and "facilitate agreements between jurisdictions on like approaches to domestic policy."
- the private sector to become active participators to complement governmental efforts.
- "an environment favorable to electronic commerce."
- the development of accessible and affordable IT infrastructure for TBDF.

8.5.4 Furthermore, the document identifies key emerging threats to online commerce, particularly illicit activities such as phishing, spyware, illegal spam and “other wrongful practices” which undermine the value of the internet for both consumers and business. The document argues that governments should work together to facilitate the “seamless nature” of the internet by creating initiatives to “identify and take compatible technological steps to combat fraudulent and deceptive practices” and urges the private sector to also take appropriate steps to improve deterrence by reporting criminal and civil violations to law enforcement agencies. In this respect, the somewhat vague language suggests that government and industry should co-operate to combat illicit or un-civil activities through enhanced visibility on the internet.

8.5.5 In terms of privacy, the document recognises that privacy concerns have been emerging through online commerce, and suggest that governments should “encourage the private sector to develop and implement self-regulatory mechanisms, including industry guidelines and effective verification and recourse methodologies.” In other words, the SPP recommends that the private sector should regulate itself by developing a privacy framework which they deem sufficient for their business needs; industry is to implement the appropriate guidelines and government should provide the appropriate enforcement backstop mechanisms as necessary “to complement and strengthen industry initiatives.” Privacy concerns have extended beyond allowing the private sector to develop their own self-regulatory mechanisms, but another document released by the SPP states that North American governments should “expand or enhance regulatory cooperation in areas that have an impact on cross-border data flow, notably in relation to the enforcement of rules for the protection of personal privacy,” arguing that in consultation with the private sector it is possible to “reconcile important public values regarding the privacy and security of information with the goal of promoting prosperity for business and consumers through online trade and commerce” (SPP 2008).

8.6. The Trilateral Committee on Transborder Data Flows

8.6.1 The North American Leaders Summit (NALS), an offshoot of the SPP, is a trilateral relations group that meets annually to discuss a range of North American objectives. The Trilateral Committee on Transborder Data Flows, one such example, was established in 2008 to further the goals of the SPP, although the committee now operates as part of NALS.

8.6.2 The Trilateral Committee on TBDF (currently under Canada's oversight) seeks to further the goals of the SPP in removing impediments to TBDF to foster trade and economic innovation.

> "The committee is composed of government representatives from Canada, Mexico and the United States and has been working in consultation with the business communities, civil and law societies, and academia in each country to identify and address impediments to electronic information flows across the borders that affect the economic growth. The purpose of the Committee is to provide strategic direction for addressing these problems and increase recognition of the importance of free information flows in supporting a growing and efficient North American market." (NALS 2010: 2)

8.6.3 Economic imperatives form the core of the document's views on TBDF. The report emphasises global outsourcing as it enables companies and governments to focus on their core operations, separating these from the peripheral ones by leveraging global supply operations and utilising the potential of ICTs to allow companies and governments to respond in a flexible manner to market flows. ICTs enable the institution to maintain access to knowledge bases and in turn this will help stimulate innovation. As such, the report is keen on emphasising the obstacles in outsourcing operations, namely, privacy laws and anti-offshoring (outsourcing) legislation.

8.6.4 The report continues to emphasise many of the objectives of the SPP, and continues to place significant importance on TBDF and data outsourcing activities, effectively portraying such TBDF as essential for business prosperity:

> "When businesses are restricted from outsourcing functions related to data management to other jurisdictions or when restrictions are placed on the location of that data, this can result in higher labour and data storage costs to the business" (NALS 2010: 12)

8.6.5 After three stakeholders forums, a final report on TBDF was published in January 2010 in which five major regulatory frameworks posed challenges to TBDF:

1. Privacy Laws
2. Anti-Spam Legislation
3. Anti-Money Laundering and Terrorism Financing Legislation
4. Anti-Offshoring Legislation
5. National Security Legislation

8.6.6 The report does not explicitly say such impediments should be removed but rather governments should "...reduce the impediments while still achieving policy and legislative objectives." (NALS 2010: 5)

8.6.7 On the matter of privacy laws and security legislation, the report notes that the business community had expressed concern over lack of clarity with both PIPEDA and the USA PATRIOT Act in relation to TBDF. Furthermore, the report also states that there is a lack of harmonisation of US federal and state privacy laws. In Mexico, the committee states that their lack of privacy laws is having an impact in that it impedes confidence in the government's ability to protect personal information (NALS 2010). The report not only recommends further harmonisation of privacy legislation (particularly US federal and state harmonisation), but also close partnerships with the private sector in order to maximise economic benefits of TBDF and outsourcing.

8.6.7 The SPP and its progeny, the NALS, both emphasise TBDF as the key to developing commerce and economic prosperity in a post-9/11 environment. They place special emphasis on harmonisation initiatives, particularly initiatives which seek to benefit the private sector. In terms of privacy recommendations, it is largely a self-regulating approach in which businesses would be encouraged to develop their own framework and the appropriate mechanisms to safe guard personal information. However, such policy recommendations are quite ambiguous and tend to illustrate a relatively lax concern for privacy concerns.

8.7 North American Competitiveness Council

8.7.1 The NACC is an organisation comprised of private sector actors, created by the SPP in 2006, to advise the SPP with recommendations on how to build upon its framework for border harmonisation. Comprised of many CEOs from across North America and under three secretariats – the Canadian Council of Chief Executives, the Mexican Institute for Competitiveness and the Council of the Americas – the NACC is a high profile private sector policy recommendation body specifically concerned with facilitating cross-border trade and economic fitness in the global marketplace.

8.7.2 NACC's primary emphasis has been to recommend the development of low risk or trusted traveller programs for both people and goods across North America. In 2007 for example, the NACC released a report, "Building a Secure and Competitive North America: Private Sector Priorities for the Security and Prosperity Partnership of North America," which recommended that governments continue to develop trusted traveller programs and that governments continue to recognise the need for seamless economic and security cooperation, particularly in a time of increasingly aggressive global competitors and mounting security threats (NACC 2007: 4) However, unlike NALS, NACC makes no mention of potential privacy as an obstacle to further harmonisation and cooperation

8.8 The US Government Accountability Office Report

In a recent report, the US government complained that the threats on the Canadian border related to illegal cross-border activity were much higher than the threats on the Mexican border (GAO 2010: 1). As the report notes, Canada and the US already have different acts to prevent illegal trafficking of many kinds which are necessarily facilitating information sharing (GAO 2010: 19-20); however, the US side is not satisfied with the current situation. It is worth remembering that this report was published and under discussion within the same time period and in the same context as the Perimeter Security Agreement.

8.9 The Perimeter Security Agreement

8.9.1 Late in 2010, news about a perimeter deal between the US and Canada leaked to various media outlets,[66] and the existence of discussions about a deal was then confirmed by Prime Minister Stephen Harper.[67] According to the Prime Minister's speech, negotiations were continuing and he had not confirmed any date for signing an agreement.

8.9.2 In early 2011, Harper met US President Barack Obama, and a formal declaration entitled "Beyond the Border: a shared vision for perimeter security and economic competitiveness" was produced on February 4th (Office of the Prime Minister of Canada 2011). The declaration outlined several "Key Areas of Cooperation": Addressing Threats Early; Trade Facilitation, Economic Growth, and Jobs; Integrated Cross-border Law Enforcement; and Critical Infrastructure and Cybersecurity. Each area has several proposals for changes to border security.

[66] *Globe and Mail*, Canada Negotiating Perimeter Security Deal with U.S., Dec 08, 2010, http://www.theglobeandmail.com/news/politics/canada-negotiating-perimeter-security-deal-with-us/article1830782/ [Accessed March 20, 2011]

[67] *National Post* Dec 26, 2010, http://www.nationalpost.com/Canada+holding+talks+security+perimeter+Harper/4026826/story.html [Accessed March 20, 2011]

8.9.3 Under Addressing Threats Early, the declaration promises to “work together to establish and verify the identities of travellers and conduct screening at the earliest possible opportunity” and to “work toward common technical standards for the collection, transmission, and matching of biometrics that enable the sharing of information on travellers in real time.”

This would seem to imply the instantaneous transmission of intimate personal data. In addition, the two nations:

> “expect to work towards an integrated Canada-United States entry-exit system, including work towards the exchange of relevant entry information in the land environment so that documented entry into one country serves to verify exit from the other country.”

Again, the concept of exchange of information would seem to imply that all relevant personal data acquired by Canadian border security would be shared with the US, and vice-versa.

8.9.4 Under Trade Facilitation, Economic Growth, and Jobs, the declaration proposes “investment in modern infrastructure and technology at our busiest land ports of entry, which are essential to our economic well-being,” which would seem to be necessary if the aims above were to be fulfilled. Also proposed are “expanding trusted traveller and trader programs, harmonising existing programs, and automating processes at the land border to increase efficiency”; in other words, once again, to increase the sharing of personal data between the two countries. Finally in this area, the declaration also signals the intention to develop “an integrated cargo security strategy that ensures compatible screening methods.”

8.9.5 Under “Integrated Cross-border Law Enforcement” there is much talk of “leveraging” cross-border resources and programs and, particularly relevant for this report, “the sharing among our law enforcement agencies of relevant information to better identify serious offenders and violent criminals on both sides of the border."

8.9.6 Finally, under Critical Infrastructure and Cybersecurity, the declaration proposed to "strengthen cybersecurity [and] enhance the security of our integrated transportation and communications networks."

8.9.7 The declaration also establishes a "Beyond the Border Working Group" (BBWG), which will report directly to the national leaders, not to Parliament or to Congress.

8.9.8 The declaration is a clear signal of intent. It is premised on concepts of risk / security and free trade / economy. The language of the declaration makes it clear the North American Perimeter proposal is very much the direct descendant of both the SPP and the NALS.

8.9.9 Nowhere in the declaration are common concepts of human rights and values mentioned. This is of major concern to the remit of the OPC. Canadian and US privacy laws and exemptions in the area of national security and border control are very different. Unless Canadian standards of data protection and privacy were to be adopted as part of this agreement, this proposal could render PIPEDA and other Canadian privacy regulations largely academic when it comes to border control. The question would no longer be one of the applicability of Canadian privacy law in the USA, but of "required" changes to that law in order to facilitate the new agreement.

9. CONCLUSIONS

9.1 Among the various concerns raised by the artificial elevation of national security above all other values, the fate of personal data is a key problem. Already the subject of major controversies due to its promiscuous processing in communicational, informational, employment and commercial settings, personal data now flow with growing frequency between different governmental and, increasingly, private channels in relation to international travel.

9.2 In Canada, this has created a number of difficulties for individuals, but they have largely been limited by the effective observance of applicable legislation, regulation and policy.

9.3 It is often held that privacy, along with other civil liberties and human rights, is in a balance with security. The (false) assumption is that privacy and security represent a zero-sum game where more of one spells less of the other. It should not be forgotten that what should be "secured" by security are the rights and freedoms of citizens.

9.4 On the other hand there is a growing assumption in government that security and economic prosperity can be mutually inclusive. However, the notion is increasingly promoted, by influential organisations like NALS, that this inclusivity must rest on both an unequal distribution of rights, especially when it comes to travel and the crossing of borders, and the levelling down of particular universal rights, including privacy, in cases where they are stronger in one nation than another.

9.5 Both features can be found not just in Canada, but as key directions in contemporary policies at the global level. The well-established NEXUS program and the PSA declaration and its precursor initiatives are key examples of this trend in the Americas.

9.6 What are the solutions? The OPC has previously argued that in the context of the trusted traveller programs, CANPASS and NEXUS, "the privacy concerns raised by the programs are mitigated somewhat by their voluntary nature" (Stoddart 2007:3). But it is important to note that safeguarding of the disclosure and sharing of the data other than for the original purpose of its collecting is a never ending concern. Trusted traveller programs, especially NEXUS have steadily increased their number of members. Plus the international nature of data sharing has resulted in a complex diffusion of the data into and between both state agency and private hands. Volunteerism in itself no longer provides a safeguard.

9.6 Currently PIPEDA remains the primary legislative tool for protecting personal data where there is private involvement. However, the Act applies to privacy concerns within Canadian frameworks. With clear trends towards increasing data sharing for both border security and economic reasons, in particular with the US, this national-level safeguard is under increasing strain. As can be seen in the PNR/API data storage by GDSs or Infoglide's Identity Resolution Engine (IRE), transborder data flows and new methods of processing data have complicated the picture. Privacy regulations within national boundaries are no longer sufficient.

9.7 PIPEDA remains applicable beyond Canadian borders. In the Facebook case, it seems that when compliance across the whole world is easier than observing individual rulings only in those jurisdictions, an active Privacy Commissioner may have a positive effect worldwide. However, OPC "success stories" like the Google and Facebook cases should not be overestimated. It remains to be seen what would happen when compliance demanded by the OPC was difficult, expensive or otherwise opposed. It seems hard to see what effective sanction could be applied that would be persuasive in the case of noncooperation, avoidance or outright refusal to comply. Indeed a refusal to cooperate might simply mean a withdrawal of the product or service involved to Canadians, who remain a very small market in global terms. With the rise of China, India and other emerging economic powers, this market share will only decrease further in importance.

9.8 With Canada and the US on the cusp of a new Perimeter Security Agreement that will directly affect the handling of personal data, a range of specific new challenges is arising. These will bring to the fore the issues of the relative lack of accountability within US data-handling organisations, the out-sourcing to private companies of data transferred south to the US, and the exemptions that many state and private organisations involved in US Homeland Security enjoy even from US privacy law.

9.9 Agreements between Canada and the US will inevitably have knock-on effects on Canadian relationships with other countries. For now, other supranational and international bodies, particularly the European Union, are comfortable with the agreements reached with Canada privacy and and transborder data-sharing. However this goodwill could suffer if Canadian standards are lowered in order to be meet US demands.

9.10 As "hoping for the best" is not a course we would recommend, there are three more or less compatible options for the OPC faced with the emergence of the PSA:

- the OPC could challenge the PSA, as there are good reasons to suppose that Canadian expectations of privacy and data protection would suffer if it proceeds;
- the OPC, and other regulatory bodies concerned with human rights, could demand a voice within the PSA process to make sure that Canadian standards are the basis for privacy and data protection within any new agreement;
- the OPC could pursue renewed efforts at generating wider international safeguards for personal data at a higher level than the bilateral agreements that are being negotiated between the US and Canada, such that standards or protection for privacy and personal data are increased in both countries alongside others.

Glossary

ACIIS	Automated Criminal Intelligence Information System
ACLU	American Civil Liberties Union
API	Advance Passenger Information
BEST	Border Enforcement Security Task Force
BPR	Behaviour Pattern Recognition
CANPASS (Air)	Trusted air travelers program for Canadian citizen at the Canadian border
CATSA	Canadian Air Transport Security Authority
CBP	Customs and Border Protection (US)
CBSA	Canada Border Services Agency
CCLA	Canadian Civil Liberties Association
CIC	Citizenship and Immigration Canada
CRA	Development of the Critical Restricted Area
CSIS	Canadian Security Intelligence Services CSIS
DHS	Department of Homeland Security (US)
EPIC	Electronic Privacy Information Centre
EU	European Union
FAST	Free and Secure Trade
FBO	Screening at Fixed-Base Operations
GDS	Global Distribution Systems (also known Computerized Reservation Systems-CRS)
GES	Global Enrollment System
IBETs	Integrated Border Enforcement Teams (Canada-United States)
ICAO	International Civil Aviation Organization
ICLMG	International Civil Liberties Monitoring Group
IRE	Identity Resolution Engine
IRPA	Immigration and Refugee Protection Act
MMW	Millimeter Wave
NEXUS	Trusted travellers programs between Canada and the US
Non-passengers	Flight crews, refuellers, caterers, aircraft groomers, maintenance and construction personnel, baggage handlers, and concession staff
OPC	Office of the Privacy Commissioner
PAPS	Pre-Arrival Processing System
PAXIS	Passenger Information System (2002)
PBO	Passenger Behaviour Observation: a screening methodology that uses risk-based security principles to screen passengers and identify those with malicious intent
PIA	Privacy Impact Assessment
PIP	Partners in Protection

PIPEDA	Privacy Act and the Personal Information Protection and Electronic Documents Act
PPP	Passenger Protect Program (the Canadian No-fly List)
Privacy Act of 1974	(US)
PNR	Passenger Name Record
PSA	Perimeter Security Agreement
RAIC	Restricted Area Identity Card: an identification card issued to all employees authorized to enter the restricted areas of Class I and II airports
RCMP	Royal Canadian Mounted Police
RFID	Radio-frequency identification
SMART	Smart Border Accord
SPOT	Screening Passengers by Observation Techniques (US)
SPP	Security and Prosperity Partnership of North America (Mexico-Canada-the US
TBDF	Transborder data flows
The USA PATRIOT Act	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (US)
TSA	Transportation Security Administration (US)
TSC	Transportation Security Clearance
TSDB	Terrorist Screening Database
TWIC	Transportation Worker ID Credential (US)

Bibliography

Alyson J., K. Bailes and I. Frommelt (eds.) (2004) Business and Security: Public-Private Sector Relationships in a New Security Environment. Oxford: Oxford University Press.

ARTICLE 29 Data Protection Working Party under the European Commission (2009) Opinion 8/2009 on the protection of passenger data collected and processed by duty-free shops at airports and ports. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp167_en.pdf [Accessed: March 22, 2011].

Avis, P. (2010) 'Gateways and Corridors in Canada: Evolving National Security' in National Defence and the Canadian forces. Available at: http://www.journal.forces.gc.ca/vol10/no3/10-avis-eng.asp. Accessed November 12, 2010.

Bennett, C. J. (2005) 'What happens when you buy an airline ticket? The collection and processing of passenger data post 9/11.' In Zureik, E. and M.B. Salter (eds.) Global Surveillance and Policing: Borders, Security, Identity, pp. 113-139. Devon UK: Willan.

Callahan, M. E. and W. Wark (2010) 'Privacy and information sharing: The search for an intelligent border.' One Issue Two Voices 13.

CBSA (2010) Memorandum D1-16-3. 'Administrative Guidelines for the provision to others, allowing access and use of API and PNR data.' Ottawa: CBSA.

CBSA (2009) CBSA Information Manual. Part 7, Chapter 3: Enforcement systems information and intelligence: Information sharing policy for the enforcement program (released under access to information act). Ottawa: CBSA.

CATSA (2010) Summary of the 2010/11 – 2014/15 Corporate Plan, Capital and Operating Budgets. http://www.catsa-acsta.gc.ca/File/Library/88/English/plan2010-11-2014-15v2.pdf [Accessed: March 22, 2011]

CATSA (2011) 'Pre-board Screening Officer'http://www.catsa-acsta.gc.ca/Page.aspx?ID=41&pname=AgentDeControle&lang=en [Accessed: March 22, 2011]

CATSA (2009a) Summary of the 2009/10 – 2013/14 Corporate Plan, Capital and Operating Budgets. Accessed by July 29, 2010. http://www.catsa-acsta.gc.ca/File/Library/14/English/plan2009-2010_2013-14.pdf [Accessed: March 22, 2011]

CATSA (2009b). Final report The Protech Integrated Checkpoint Trial Kelowna Airport. Ottawa: CATSA.

Cockfield, A. J. (2010) 'Legal Constraints on Transferring Personal Information across Borders: A Comparative Analysis of PIPEDA and Foreign Privacy Laws.' In E. Zureik, L. L. Harling Stalker, E. Smith, D. Lyon, and Y. E. Chan (eds) Surveillance, Privacy and the Globalization of Personal Data, pp. 50-70. Montreal and Kingston: McGill-Queen's University Press.

Cockfield, A. J. (2004) 'The State of Privacy laws and Privacy-Encroaching Technologies after September 11: A Two-Year Report Card on the Canadian Government,' University of Ottawa Law and Technology Journal, 1: 325-344.

Davies, A. (2010) 'Social Media: 3. Privacy and the Facebook Example'. http://www2.parl.gc.ca/Content/LOP/ResearchPublications/2010-06-e.htm [Accessed March 19, 2011]

European Union Committee (2007) The EU/US Passenger Name Record (PNR) Agreement. London: The Authority of the House of Lords.

Gilbert, E. (2008) The Implications of a Perimeter Approach to Security for Canadian Border and Immigration Practices. Report for the Metropolis Project. Available: http://canada.metropolis.net/pdfs/Gilbert_Border_Immigration_practices_e.pdf [Accessed February 11, 2011].

Hasbrouck E. (2010) PNR in Practice. http://hasbrouck.org/IDP/IDP-PNR-BRU-8APR2010.pdf [Accessed March 22, 2011]

Haggart, B. (2001) Fortress North America? What "Perimeter Security" Means for Canada: Seminar Report. PRB 01-25E, Library of Parliament.

Harknett, R. J. and J. A. Stever (2009) The Cybersecurity Triad: Government, Private Sector Partners, and the Engaged Cybersecurity Citizen,' *Journal of Homeland Security and Emergency Management*: 6(1): 1-14

Hobbing, P. (2008) Tracing Terrorists: The EU-Canada Agreement in PNR Matters. Centre for European Policy Studies (CEPS) Special Report. http://www.ceps.eu/files/book/1704.pdf [Accessed: March 22, 2011]

Infoglide Software Identity Resolution Engine (2011), http://www.infoglide.com/PDF/IRE-for-Government-US.pdf [Accessed: March 22, 2011]

Infoglide Software Identity Resolution Engine Datasheet (2011), http://www.infoglide.com/PDF/IRE-Datasheet.pdf [Accessed: March 22, 2011]

International Civil Liberties Monitoring Group (ICLMG) (2005) Brief to the House of Commons Subcommittee on Public Safety and National Security, Of the Standing Committee on Justice, Human Rights, Public Safety and Emergency Preparedness. Submission Concerning The Review of the Anti-Terrorism Act, April, 2005. http://www.interpares.ca/en/publications/pdf/ICLMG_Brief_on_C-36.pdf

Kilibarda, K. (2008) Canadian and Israeli Defense – Industrial and Homeland Security Ties: An Analysis, November 2008, The New Transparency Project, Working Paper II, IRSP IV, http://www.sscqueens.org/resources/online-reports [Accessed: March 22, 2011]

Lahav, G. (2008) 'Mobility and Border Security: The US Aviation System, the State and the Rise of Public-Private Partnerships.' In M. B. Salter (ed.) Politics at the Airport. Minneapolis: University of Minnesota Press.

Lippert, R. and D. O'Connor (2003). "Security Assemblages: Airport Security, Flexible Work, and Liberal Governance." Alternatives 28(3): 331-358.

Lyon, D. (2003) Surveillance after September 11th. Cambridge: Polity.

Lyon, D. (2006) 'Airport screening, surveillance and social sorting: Canadian responses to 9/11 in context.' Canadian Journal of Criminology and Criminal Justice, 48(3), 397-411.

Michaels, J. D. (2008) ‘All the President’s Spies: Private-Public Intelligence Partnership in the War on Terror.’ California Law Review, 96, 901-966.

North American Leaders Summit (NALS) (2010) ‘Report on the Trilateral Committee on Transborder Data Flows.’ http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/vwapj/Report_Trilateral_Committee_Jan_2010.pdf/$FILE/Report_Trilateral_Committee_Jan_2010.pdf [Accessed: March 22, 2011]

North American Competitiveness Council (NACC) (2007) ‘Building a Secure and Competitive North America: Private Sector Priorities for the Security and Prosperity Partnership of North America.’ http://www.ceocouncil.ca/publications/pdf/test_5c7bd813dfeec2b52e2dba62584a3f13/NACC_Report_to_Leaders_August_21_2007.pdf [Accessed: March 22, 2011]

O’Connor, D., R. Lippert, D. Spencer and L. Smylie (2008). ‘Seeing Private Security Like a State.’ Criminology and Criminal Justice 8:203-226.

O’Connor, D. and W. de Lint (2009) ‘Frontier Government: The Folding of the Canada-US Border.’ Studies in Social Justice 3(1), 39-66.

Office of the Privacy Commissioner of Canada (OPC) (2007a) Resolution of Canada’s Privacy Commissioners and Privacy Enforcement Officials, Passenger Protect Program – Canada’s Aviation No-fly List, OPC, Ottawa. http://www.privcom.gc.ca/nfl/res_20070628_e.asp [Accessed: March 22, 2011]

Office of the Privacy Commissioner of Canada (OPC) (2007b) Report of Findings: Privacy Commissioner of Canada v. SWIFT, April 2, 2007 http://www.priv.gc.ca/cf-dc/2007/swift_rep_070402_e.cfm [Accessed: March 22, 2011]

Office of the Privacy Commissioner of Canada (OPC) (2007c) News Release: Privacy Commissioner concludes investigation of SWIFT http://www.priv.gc.ca/media/nr-c/2007/nr-c_070402_e.cfm [Accessed: March 22, 2011]

Office of the Privacy Commissioner of Canada (OPC) (2010) A Matter of Trust: Integrating Privacy and Public Safety in the 21st Century. http://www.priv.gc.ca/information/pub/gd_sec_201011_e.cfm [Accessed: March 22, 2011]

Office of the Prime Minister of Canada (2011) '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, Washington DC. http://www.pm.gc.ca/eng/media.asp?id=3938 [accessed March 10, 2011]

Personal Information Protection and Electronic Documents Act (PIPEDA) (2000, c. 5) http://laws.justice.gc.ca/en/ShowDoc/cs/P-8.6//20090818/en?page=1 [Accessed: March 22, 2011]

Salter, M. B. (ed.) (2008) Politics at the Airport. Minneapolis: University of Minnesota Press.

Security and Prosperity Partnership (SPP) (2005) 'Framework of Common Principles for Electronic Commerce'. http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/vwapj/Framework23june05ECDA.pdf/$file/Framework23june05ECDA.pdf [Accessed: March 22, 2011]

Security and Prosperity Partnership (SPP) (2008) 'Statement on the Free Flow of Information and Trade in North America.' http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/gv00515.html [Accessed: March 22, 2011]

Spearin, C. (2009) 'The Changing Forms of Utility of Force: The Impact of International Security Privatization on Canada.' International Journal Spring (2009): 481-500.

Stoddart, J. (2007) The Privacy Implications of Security Measures: Office of the Privacy Commissioner of Canada's Submission in Response to the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182. Office of the Privacy Commissioner of Canada: Ottawa. Available: http://www.priv.gc.ca/information/pub/asm_071107_e.pdf. Accessed August 23, 2010.

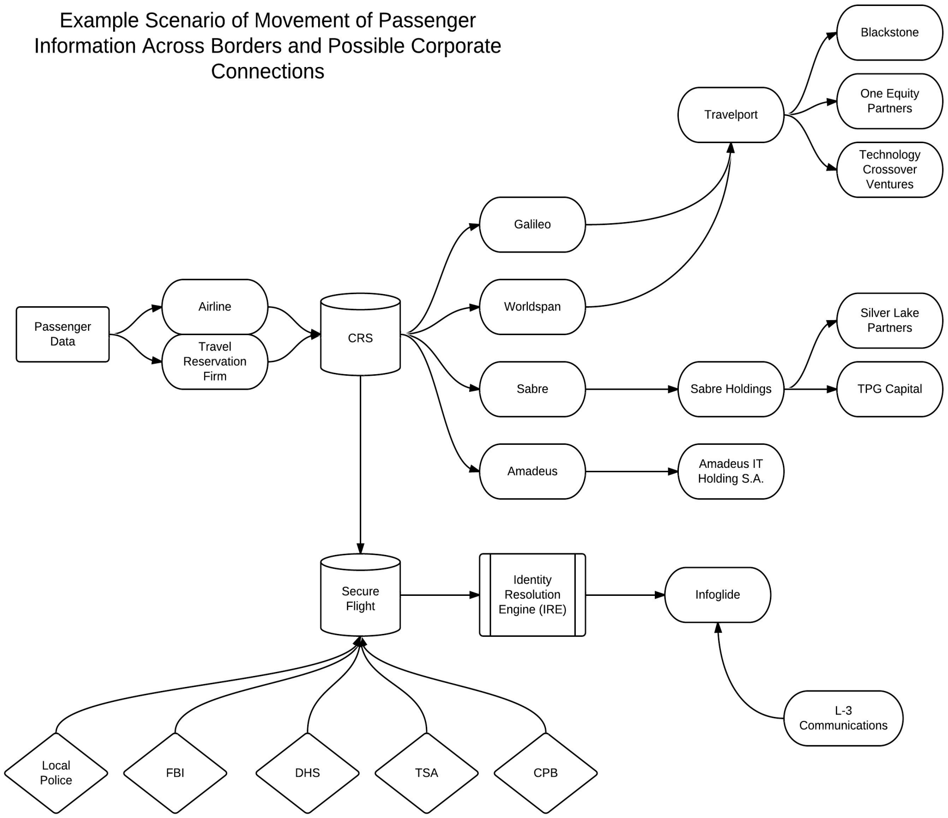
The Surveillance Project (2008) 'The Globalization of Personal Data Project: An International Survey on Privacy and Surveillance Summary of Findings'. Kingston ON: Queen's University.

The Treasury Board of Canada Secretariat (2006) ‘Privacy Matters: The Federal Strategy to Address Concerns about the USA PATRIOT Act and Transborder Data Flows.’ Available: http://www.tbs-sct.gc.ca/pubs_pol/gospubs/tbm_128/pm-prp/pm-prp01-eng.asp. Accessed February 21, 2011.

United States National Archives and Records Administration. (2007) ‘Part III: Department of Homeland Security: Transportation Security Administration: 49 CFR Part 1507: Privacy Act of 1974: Implementation of Exemptions and System of Records; Secure Flight Records; Final Rule and Notice.’ Federal Register 72(217): 63706 - 63710.

United States Government Accountability Office (GAO) (2010) Border Security Enhanced DHS Oversight and Assessment of Interagency Coordination is Needed for the Northern Border, GAO. http://www.gao.gov/new.items/d1197.pdf. [Accessed: March 22, 2011]

Appendix 1


Example Scenario of Movement of Passenger Information Across Borders and Possible Corporate Connections