CONSUMER PRIVACY AND STATE SECURITY: LOSING OUR BALANCE

Written by John Lawford and Sharon Roberts
Public Interest Advocacy Centre
1204 – ONE Nicholas St.
Ottawa, Ontario
K1N 7B7

November 2004

With Funding from Industry Canada

The Public Interest Advocacy Centre
(PIAC)
Suite 1204
ONE Nicholas Street
Ottawa, ON
K1N 7B7

Canadian Cataloguing and Publication Data

Lawford, John
Roberts, Sharon

Consumer Privacy and State Security: Losing Our Balance

ISBN 1-895-060-67-2

EXECUTIVE SUMMARY

Canadian citizens and consumers are facing an unprecedented challenge to their privacy rights. State security measures implemented in Canada since the terrorist attacks of September 11, 2001 have seriously reduced these privacy rights. There has been little public debate over the public policy and legal changes made in Canada to support the "war on terrorism". However, these changes have made Canadians' privacy rights possible "collateral damage" in this war. Canadians seem largely unaware of these measures and still supportive of government efforts to quell terrorist threats.

Nevertheless, Canadians are protective of many privacy rights that are necessarily or unnecessarily compromised in seeking to boost national security. These include the right and expectation that their movements and other clues they give about themselves as they purchase and live their way through life will not systematically be made available to government. They continue to have an expectation of privacy in their personal communications, whether these are conducted over the phone or over the Internet. They do not like surveillance of their daily activities. They do not appreciate business helping the government to collect profiles of their consumer habits. In short, they do not accept that their personal privacy necessarily must be compromised to increase national security. Above all, they are concerned that the Canadian government will allow the sharing of their personal information with other countries, especially the United States.

This report examines three challenges to Canadian privacy rights posed by the new security agenda of government and business. First, it looks at legal requirements that rely upon, or that risk, a systematic violation of usual privacy rights, including: the collection, use and disclosure of airline flight information; the outsourcing of personal information processing to entities subject to the USA PATRIOT Act; and the information requirements of the US VISIT traveler information program. Second, the report examines the increase in surveillance technologies of all kinds that has been hastened and expanded by national security concerns, including: interception of private communications; national identity cards/biometrics; and closed-circuit television and video surveillance of the public. Third, the report focuses on marketplace-driven and -assisted potential privacy violations, including: radio-frequency identification; datamining; and, finally, the virtual conscription of Canadian business into being "agents of the state" to collect and process "suspicious" data on Canadians.

The Report includes significant national polling results of Canadians' attitudes towards, and knowledge of privacy and national security conflicts. The poll reveals Canadians wish to assist with national security efforts but are unclear on the trade-offs with personal privacy involved. The poll finds, significantly, that most Canadians expect a similar treatment of their privacy rights even in the new post 9/11 world.

The costs of reducing privacy rights to increase state security, both financial and in terms of lost confidence in business and government, has the potential to be large and appears to be growing. The report concludes with calls for increased accountability of government and business in this "balancing" of privacy rights and security measures.

Table of Contents

INTRODUCTION

Since the September 11, 2001 terrorist attacks on the U.S., Canada has responded to perceived threats of terrorism with several new laws, policies and even business practices, all in the name of promoting "national security".

This report examines the issue raised by the Privacy Commissioner of Canada in her 2003-4 Report to Parliament: "Recent attempts to make us safer and more secure, both from international terrorism and more traditional public safety threats, raise serious privacy concerns."

The report does not directly confront the wider issue of the wisdom of national security measures or the possible effects of the national security agenda upon Canadians' constitutional rights. This report examines privacy concerns and notes that citizens and consumers, whose tax dollars and expenditures are footing the bill for this "war", have demanded little government or business accountability for increased intrusions into consumer privacy for national security and public safety reasons. Finally, this report seeks to examine Canadians' attitudes to privacy and national security by reporting on the results of a national poll. The Public Interest Advocacy Centre retained POLLARA Inc., a major public opinion and marketing research firm, to survey consumers. The survey of 1,260 adults was conducted in late October 2004.[1]

STATE SECURITY AND ANTI-TERRORIST INITIATIVES

Since September 11, 2001, terrorism – and the "war" against it – has drawn unprecedented attention from the media, politicians, and legislators.[2] It is difficult to underestimate the effect this event and its aftermath have had upon North America society and government. A number of national security measures – some novel, some considered well before September 11th – are in place, with more on the way. Any time there is as fundamental a shift in government priorities as there has been post-9/11, there are likely to be effects that touch consumers and citizens. This report considers whether there has been any "collateral damage"[3] to consumer and citizen privacy rights in the global "war on terror."[4]

---

[1] The questions asked by POLLARA were included in a bi-weekly telephone omnibus survey *Consumer Perspectives*. The survey has an accuracy of ±2.7 per cent. The survey questions and unweighted averages are found in Appendix A.

[2] Justin Lewis, "At the service of politicians" *The Guardian* (4 August 2004), online: Guardian Unlimited <http://www.guardian.co.uk/analysis/story/0,3604,1275467,00.html>. Lewis points out that while news coverage of terrorist related items "is at its highest-ever sustained level," a literature review shows "little relation between the number of international terrorist incidents in any given year and the use of the term in the press." The fact that since September 11 "there have been fewer terrorist attacks than at any time in the last two decades" is not a testament to growing threats of international terrorism, but to "an increase of political rhetoric". See also Doug Saunders, reference *infra*.

[3] This idea is essentially the same as that of L. Austin, "Is Privacy a Casualty of the War on Terrorism?," in R.J. Daniels, P. Macklem, and K. Roach, (eds.), *The Security of Freedom: Essays on Canada's Anti-terrorism Bill* (Toronto: University of Toronto Press, 2002), pp. 251-267. However, the concept of "collateral damage" includes more of a judgment that there is a "common enemy" and that the forces of "privacy" and "security" actually are on the same side. This report takes this position rather than viewing consumers as "innocent bystanders" or "civilians" in the debate, but rather as necessary partners. (We do not, however, in any way suggest by this analogy that consumers should be recruited as agents of the state to report "suspicious" behaviour to security forces.) Consumers are in fact supporting both security efforts and wishing to stand up for personal privacy in a seemingly contradictory way. This is explored below.

[4] United States President George W. Bush first characterized state response to terrorism as a "war" in The White House, News Release, "Statement by the President in His Address to the Nation" (11 September 2001). The phrase "war on terror" has since been used by the Canadian and other governments and the media has reported and appears to have accepted this characterization largely without question (see *contra*

Policy Changes

Canada swiftly developed an "Anti-Terrorism Plan" following the events of September 11, 2001. The *Anti-Terrorism Plan* committed Canada to pass legislation,[5] to fund anti-terrorism efforts and to increase cooperation with other countries (in particular the U.S.) on counter-terrorism efforts.[6]

In an effort to further the *Anti-Terrorism Plan*, in April 2004 the federal government introduced Canada's first *National Security Policy*.[7] This document represents a sea change in Canadian domestic policy: the fact that a policy position is required on the previously diffuse issue of "national security" is in itself significant, since, as the *National Security Policy* notes, it is the first such comprehensive statement. The *National Security Policy* makes assertions of "an increasingly complex and dangerous threat environment" in both the world and in Canada. It is stated that such threats to Canada's national security exist, are growing in number, seriousness and scope, and that the issue must be addressed with immediate, concrete action.

The Deputy Prime Minister has described the *National Security Policy* as having three broad goals:

> "First, we must protect the physical safety and security of Canadians at home and abroad.
>
> Second, we need to continue to ensure Canada is not a base for threats to others.
>
> And third, our National Security Policy should contribute to the development of a more effective international security system."[8]

A number of other initiatives "to help build a more integrated security system," and to meet Canada's *National Security Policy* objectives presently are being considered or are under development by various government agencies.

The *National Security Policy* is to be coordinated and overseen by the (soon to be Department of)[9] Public Safety and Emergency Preparedness Canada (PSEPC). The Government announced its creation of PSEPC on December 12, 2003.[10] It groups border security, intelligence, policing and emergency preparedness, among others areas, under its very wide umbrella. The Minister for PSEPC is presently also the Deputy Prime Minister. PSEPC was created in part to rationalize Canada's response to security threats. It is one of the major departmental reorganizations of the Government of Canada in recent memory.

W. Wesley Pue, "The War on Terror: Constitutional Governance in a State of Permanent Warfare?" (2003) 41 Osgoode Hall L.J. 267 at 268).

[5] Members of the United Nations were bound by international law to pass their own legislation to combat terrorism after September 11. Canada met its obligation by passing Bill C-36, the *Anti-terrorist Act*, detailed below, only two months later.

[6] Speech delivered by The Honourable Anne McLellan, Deputy Prime Minister and Minister of PSEPC to the Canadian Club, Ottawa, "Securing Canada: Laying the Groundwork for Canada's First National Security Policy" March 25, 2004, online: http://www.psepc-sppcc.gc.ca/publications.speeches/20040325_e.asp>.

[7] Canada, Privy Council Office, *Securing an Open Society: Canada's National Security Policy* (Ottawa: Her Majesty the Queen in Right of Canada, 2004) [*National Security Policy*]. Online: http://www.pco-bcp.gc.ca/docs/Publications/NatSecurnat/natsecurnat_e.pdf.

[8] Speech delivered by The Honourable Anne McLellan, *supra*, March 25, 2004.

[9] See Bill C-6, *An Act to establish the Department of Public Safety and Emergency Preparedness and to amend or repeal certain Acts*, 38th Parl. 1st Session.

[10] Canada, Office of the Prime Minister, "Changing Government: Prime Minister announces appointment of Cabinet," News Release (12 December 2003).

Government Promises Of Balance And Transparency

According to its drafters, Canada's *National Security Policy* strikes a balance between "the needs for national security" and "the protection of core Canadian values of openness, diversity, and respect for civil liberties." The press release accompanying the *National Security Policy* states that Canadians "understand" the "new reality" of living in "an often dangerous world" in which Canada faces "threats to security and public safety"[11] that warrant increased spending and state action to bolster national security and contribute to international security.

In theory, transparency in government allows citizens to hold the state accountable for its actions by making government actions transparent or openly accessible to individuals. When individuals do not understand what decisions their government makes, how it makes decisions, or how those decisions might affect them, individuals are unable to actively participate in the democratic process by raising questions or challenging state actions and decision-making.[12] Neither the *National Security Policy* nor the press release that accompanied it offers evidence of Canadians' knowledge or understanding of national security issues despite its assertions.

Publication of the National Security Policy itself is not itself well known amongst the Canadian population: in the POLLARA poll, 77% of Canadians were unaware it was released in April 2004. In Canada's *National Security Policy*, the government insists that it "needs the help and support of all Canadians to make its approach to security effective." It also acknowledges our government's promise to work with its "partners and with all Canadians," to balance state and individual interests, and to preserve civil liberties, individual rights, and consumer privacy in the sober face of our "new reality."

Costs Of Prioritizing Security

Increasing state security costs money. Someone ultimately will pay the bill for security measures legislated or otherwise implemented by both federal and provincial governments in Canada. The first two payors are perhaps obvious candidates: taxpayers and business.

In its 2001 Budget, the Government of Canada announced its plans to spend an increase of 7.7 billion dollars over five years on "Public Security and Anti-Terrorism."[13] The Auditor General's March 2004 Report to Parliament concentrated on the federal government's public security agenda. The Auditor General found that the majority of money spent in the first year of that initiative was appropriately used to address "priority areas," but critiqued the government's failure to establish adequate oversight to co-ordinate departmental efforts and maximize results.[14] In particular, despite spending vast sums to "enhance security for Canadians," in fact, "[t]he government as a whole failed to achieve improvements in the ability of security information systems to communicate with each other," resulting in lengthy delays of several years before the government can realize many security promises it has made since September 11.[15] The Auditor General also found that a number of existing measures are not monitored or applied effectively,

---

[11] Office of the Prime Minister, News Release, "Government of Canada releases comprehensive National Security Policy" (27 April 2004).
[12] Center for Democracy and Technology (CDT), "Transparency" in *E-Government Handbook* (Washington, DC: Center for Democracy and Technology, 2004), online: CDT <http://www.cdt.org/egov/handbook>.
[13] *Report of the Auditor General 2004*, March 2004, online: < http://www.oag-bvg.gc.ca/domino/reports.nsf/html/04menu_e.html> at 1.
[14] *Ibid*. Specifically, "the government did not have a management framework that would allow it to direct complementary actions in separate agencies or to make choices between conflicting priorities".
[15] *Ibid*. at 1; see also 14-22.

meaning that security practices currently in place are costing consumers, government, and industry money, time, and effort without so far meeting their stated objectives.[16]

Nonetheless, these efforts are funded directly from taxation. The government is accountable to the people for their cost and effectiveness. The Auditor General's Report of 2004 and future reports will undoubtedly continue to scrutinize these large expenses.

In addition to government spending on security measures, other material costs of the "war on terrorism" fall to corporations, such as airlines and Internet service providers. State-mandated airline "security charges" are a measure that has already been approved despite industry objections that the charge would make air travel less attractive to consumers and thereby reduce sales and profit.[17] Likewise, the federal government's *Lawful Access Proposal*, as noted below, proposes saddling ISPs and other network providers with the costs of building surveillance-capable systems. As noted by the Electronic Frontier Foundation in relation to similar proposals in the U.S. to new communications technologies, this may have the effect of changing the business model for many of these businesses and effectively killing off development of privacy enhancing technologies.[18]

However, the significant costs of increased state security are increasingly being paid by a third group, consumers. This is done either through direct security charges on products or services levied by the government (such as the "air travellers security charge"[19] which, despite industry protestations at having to collect it, is actually charged to the consumer), or indirectly, through costs passed on by business. An example of the latter is the expense of permitting state access to electronic communications fall to Internet service providers; for example, those costs would likely be passed on to their customers.[20]

Less direct costs include: travel-time delays[21]; more expensive travel and identification documentation and the costs of reading it[22]; and even government guarantees of corporate liability.[23]

---

[16] *Ibid*. at 34-37.

[17] See "Airlines blast $24 round-trip air security fee" CBC News, online: CBC News <http://www.cbc.ca/stories/2002/04/01/fee020401>.

[18] Electronic Frontier Foundation, "Communications Assistance to Law Enforcement Act: The Perils of Wiretapping the Internet", online < http://www.eff.org/Privacy/Surveillance/CALEA/>. The EFF concludes its section of this document entitled "The Cost of CALEA Will Be Passed on to Consumers" with the statement: "The needs of government, not consumers, would guide the marketplace." Note that this does create, however, a counter-market for surveillance-compliant technologies. See The Register, "Milking the Internet surveillance cash cow" (April 6, 2004). Online: <http://www.theregister.co.uk/2004/04/06/fbi_wiretap_bonanza/>.

[19] The *Air Travellers Security Charge Act*, (enacted by S.C. 2002, c. 9, s. 5), in s. 11 requires all persons boarding a plane to pay the charges set out in the act.

[20] See John Leyden, "Spooks want more Web-tapping powers" *The Register* (15 March 2004), online: The Register <http://www.theregister.co.uk/2004/03/15/spooks_want_more_webtapping_powers>.

[21] See Steven E. Polzin, "Security Considerations In Transportation Planning : A White Paper" online: < http://www.mcb.fhwa.dot.gov/Documents/SecurityPapers/SecurityConsiderations_Polzin.htm>. Travel costs increase in several ways due to increased security: "Regardless of who pays, the long-term cost of air travel is likely to go up, due to greater security costs, higher risk costs, and perhaps fewer economies of scale. Time costs of air travel may also go up as security clearances slow boarding. And, somewhat unique to air travel, there may be an increase in those who have a mode-choice-altering fear of flying."

[22] See the Economist, "Biometrics: Prepare to be scanned" December 4, 2003, online: < http://www.economist.com/science/tq/displayStory.cfm?story_id=2246191>, which quotes the U.S. General Accounting Office figures: "Worse, spending the billions of dollars that the GAO estimates will be necessary to implement biometric systems at border-crossing points—$1.4 billion to $2.9 billion initially, and $700m to $1.5 billion annually thereafter—may mean there is less to spend on other areas of security".

[23] "The Government of Canada has issued an Order in Council providing full indemnity to the

The problem with downloading costs to consumers is twofold. First, it reduces consumer confidence and consumer spending. Quite simply, it raises prices. An airline ticket to a domestic destination incurs a security charge of up to either $6.54 or $7 each way. This can represent on short flights such as Montreal-Toronto an average 5% of the total cost. This is in addition to airport improvement fees (some of which may seek to recover investments in increased security measures) and GST and possibly provincial sales tax. This is double dipping on taxation revenues and may retard the economy.

The second problem is more political: should we be paying for the government to spy on us? The answer to that question may be yes, if there is a severe threat of terrorist action. However, this question should be settled in a political forum, with consumers wearing their taxpayer hats, not their consumer hats. Governments are accountable to citizens, taxpayers, voters. They are not directly accountable to "consumers". If costs are downloaded to consumers via charges for products and services, the true cost of such measures is never passed upon by the electorate. The true cost of security then is hidden, and it may be staggering.[24] Ultimately, citizens may conclude that the level of security being sought is too expensive, or that the value in terms of security for the money spent is not proportionate. But this accountability (in the financial and political senses) can only be achieved by taxation and budgeting for security measures in a transparent way.[25] To date, this transparency has not been clearly present.

COUNTER-TERRORISM LEGISLATIVE CHANGES

The government's main tool for implementing promises of a balanced policy is in Acts of Parliament, and it is therefore to that legislation that this report now turns.

Anti-Terrorism Act (Bill C-36)

In accordance with the Anti-Terrorism Plan, the federal government swiftly introduced Bill C-36, the *Anti-terrorism Act*,[26]. It is fair to say that Bill C-36 was written and adopted in extreme haste with less than the usual public scrutiny, coming less than 2 months after the 9/11 attacks. Even so, there was sufficient public scrutiny to require some acknowledgement in the legislation that its sweeping changes were of an extraordinary nature (and therefore likely temporary, being akin to emergency powers). Accordingly, the law provided a "sunset clause": by December 2004 the Canadian government must commence a review of whether several, though not all, of the changes it introduced remain necessary or ought to be repealed.

Canadian aviation industry for any coverage that was lost due to the cancellation of war and terrorism insurance. The Order in Council has been approved for 2004. Official declarations of its status occur every 90 days to account for the potential of change in the insurance industry.": *Management's Discussion and Analysis and Consolidated Financial Statements of the Greater Toronto Airports Authority,* June 30, 2004, p. 15. Online: <http://www.gtaa.com/documents/corporate/quarterly_financials_mda_june_2004.pdf>

[24] For example, estimates for the creation of a National ID Card top $5 billion.

[25] For example, Real Time Identification Project, created by virtue of the Smart Border Action Plan promises to "enable the RCMP to access FBI fingerprint data directly via real-time electronic link. However, according to the Auditor General's 2004 Report, the savings and reduced turnaround times that were promised as part of the business plans associated with real time identification have been "marginal at best." This sort of public scrutiny will not be available in consumer-downloaded security efforts.

[26] S.C. 2001, c. 41.

There are several aspects of the *Anti-terrorism Act* that are not directly related to consumer privacy but that set the context in which the changes that do directly affect consumer privacy operate.[27] These are summarized below:

1. Canada's *Anti-terrorism Act* requires, in relation to national security (terrorism), that superior court judges hold "judicial investigative hearings" relating to the offences, and to do so *in camera*. These hearings are "secret trials" in all but name; judges must limit or prohibit media coverage, deny public attendance, and may refuse accused persons the right to be present or to have legal counsel appear before the court on their behalf. The *Act* only entitles accused persons in such situations to a summary of the evidence against them – in contrast with the individual rights and freedoms guaranteed by the *Charter*.[28]
2. Similarly, our new *Immigration and Refugee Protection Act* authorizes government officials to issue a security certificate and to detain or deport any individual whom they suspect of facilitating or participating in terrorist activity.[29] An accused person can challenge her security certificate before a judge of the Federal Court of Canada, who is limited to deciding whether or not the choice to issue the certificate was reasonable. The judge can hear the government's case for issuing the certificate in secret and can deny the accused any opportunity to review a complete record of the evidence against her or to be present or represented by legal counsel at the hearing.
3. Police in Canada can now preventively stop and detain people for several days. Under the *Anti-terrorism Act*,[30] police can lay an information and obtain a judge's permission to detain individuals as a form of "preventive arrest."[31] Officers can then imprison individuals for up to 72 hours without charging them with any offence and without either advising them of or providing them with reasonable opportunities to exercise a right to counsel or the other rights normally accorded accused persons in Canada.[32] The decision to preventatively detain individuals is not based on reasonable and probable grounds to believe that they are knowingly and intentionally involved in or supporting terrorism. Rather, to preventatively detain individuals in Canada, police need only suspect them of facilitating terrorist activity – whether or

[27] Note that this does not summarize the entire number and effect of the amendment made under Bill C-36. For example, the changes to the *Proceeds of Crime (Money Laundering) Act*, which became the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*.

[28] The Supreme Court of Canada has recently upheld the majority of the judicial investigative hearing procedure in *Application under s. 83.28 of the Criminal Code (Re)*, 2004 SCC 42 (June 23, 2004).

[29] S.C. 2001, c. 27, ss. 77-85 [*IRPA*]. Canada's previous immigration law also provided limited opportunities for the government to deport refugees suspected of threatening Canada's national security. However, unlike the *IRPA*, the earlier provisions applied to refugees (not permanent residents) and were rarely implemented or enforced with the same success (see *e.g. Suresh v. Canada (Minister of Citizenship and Immigration)*, [2002] 1 S.C.R. 3).

[30] S.C. 2001, c. 41, amending s. 83.3(4) of the *Criminal Code*. Note that although this provision has not been tested at the appeal level, it appears from the case of *R.* v. *Hurrell*, (2002), 60 O.R. (3d) 161 (C.A.) that such "preventative arrest" may well be constitutional, provided the officer involved has "reasonable grounds to believe" an offence is to be committed. However, see below the discussion of the legal protection of privacy under the Charter and the comments of Dickson C.J. in relation to "national security".

[31] For a discussion of the implications of preventative arrest, see Ronald J. Daniels, "Introduction" in Ronald J. Daniels, Patrick Macklem & Kent Roach, eds., *The Security of Freedom: Essays on Canada's Anti-Terrorism Bill* (Toronto: University of Toronto Press, 2001) 1 at 4.

[32] This can include the right to liberty and security of the person, the right not to be arbitrarily detained or imprisoned; the right to be informed without delay of the reasons for detention, to consult legal counsel and to be advised of that right; and the right to be informed of the reasons for one's arrest if charged, to be appear before an impartial tribunal in a reasonable period of time to answer those charges, to be presumed innocent until proven guilty, and not to be denied bail without reasonable cause, all of which are guaranteed by the *Charter*, ss. 7, 9, 10, 11.

not they knew that a particular terrorist activity was facilitated or that any terrorist activity was ultimately carried out.[33]

4. The *Anti-terrorism Act* also allows Canadian security to search individuals and their homes or places of business without a warrant and to seize any property in their control if law enforcement agents suspect that it is related to, may be used, or has been used to support terrorist activity.[34] Excepting the emergency powers that the government temporarily used by invoking the *War Measures Act* in 1970, the forfeiture provisions of the *Anti-terrorism Act* far exceed any criminal law power that Canadian officials have previously held.
5. Under the *Anti-terrorism Act*, anyone in Canada or any Canadian abroad who "knowingly deal[s] directly or indirectly in any property that is owned or controlled by or on behalf of a terrorist group" can have private property in their control seized under the new forfeiture laws, regardless of whether they are its rightful owner.[35] For a Federal Court judge to issue a forfeiture order, the Attorney General of Canada must swear an affidavit "on information and belief."[36] Forfeiture orders presume that any property in the control of an individual suspected of being connected to terrorist activity is itself related to terrorism. They empower state agents to seize private property in an individual's possession or control regardless of whether or not that person is ultimately convicted of a terrorism-related offence. In effect, judges hearing applications for forfeiture orders may have little alternative but to issue them. The affidavits that support such applications are not subject to the usual rules of evidence. Nor can judges receiving them draw adverse inferences "from a failure to provide evidence of persons having personal knowledge of material facts" to justify a forfeiture order.[37]
6. Another major change was the amendment of the *Official Secrets Act*, which became the *Security of Information Act*. It addresses national security concerns, including:
   a. threats of espionage by foreign powers and terrorist groups,
   b. espionage and coercive activities against émigré communities in Canada.

   It creates new offences to counter intelligence-gathering activities by foreign powers and terrorist groups, as well as other offences, including the unauthorized communication of special operational information (including reporting "leaked" security information in a newspaper).[38]

There was, however, not much direct amendment of privacy legislation as the result of the *Anti-terrorism A*ct. In fact, there were only two amendments to "privacy legislation" in the *Anti-terrorism Act*.[39] These amendments prohibit a person accused of a terrorism-linked offence from obtaining personal information about themselves under the "individual access" provisions of either the *Personal Information Protection and Electronic Documents Act* (PIPEDA) or the *Privacy Act*.

However, Bill C-36 did usher in a climate in which several other statutes did directly and profoundly affect consumer privacy. This was done largely by defining "terrorism" as a subject of domestic law. Canada's *Anti-terrorism Act* now defines "terrorist activity" and "terrorist

---

[33] *Criminal Code*, s. 83.19. Individuals can be accused of facilitating terrorism for their actions or for providing financial or other support, whether or not they know that a particular terrorist activity occurs and whether or not it was facilitated, foreseen, or planned at the time.

[34] *Criminal Code*, ss. 83.08 – 83.17.

[35] Gary T. Trotter, "The Anti-Terrorism Bill and Preventative Restraints on Liberty" in Daniels, Macklem & Roach, eds., *supra*, at 244.

[36] *Criminal Code*, s. 83.14(2).

[37] *Ibid*.

[38] This was the amendment used to search the home of Ottawa Citizen reporter Juliet O'Neill on January 21, 2004. See, for example: "RCMP raids reporter's offices over Arar case" CTV.ca (January 22, 2004), online: <http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/1074704091441_70113291>

[39] See sections 103 and 104 of the *Anti-terrorism Act*, creating new s. 4.1 of the *PIPEDA* and new s. 70.1 of the *Privacy Act*.

organization" for domestic law enforcement and intelligence purposes. Critics charge that trying to fight "terrorism" is really a quest to achieve ultimate "security",[40] which is unobtainable.

Critics also charge that the rhetorical allusion in the United States to the "war on terror" may sow public fear and with it an increased acceptance of promised "public safety" and "national security" gains through legislation, at the expense of constitutional rights, especially when passed in the immediate aftermath of a devastating event.[41],[42] The *USA PATRIOT* Act has been described as operating on such a model.[43] Whether the *Anti-Terrorism Act* will have as profound an effect on constitutional rights in Canada is not yet clear. However, by defining terrorism as a domestic priority, the government may have left scope for the expansion of powers to fight this "enemy" into areas of previously struck balances of privacy rights, policing and national security.

Public Safety Act, 2002

The second major piece of anti-terrorism legislation affecting consumer privacy was not as easily created as the *Anti-Terrorism Act*. However, it was to have a far more profound effect upon consumer privacy.

The federal government introduced several versions of what is now the *Public Safety Act, 2002* before it was passed in 2004.[44] Many individuals and organizations, including the Privacy Commissioner of Canada, sharply criticized all versions of the Act over concerns that certain parts of the law violate Canadians' privacy and individual rights.[45] Most of these criticisms were directed to new ss. 4.81-4.83 of the *Aeronautics Act*[46] that permitted gathering of flight information. Others dealt with its amendment of PIPEDA, which allows collection, use and disclosure of personal information for reasons of national security, without the subject's knowledge or consent. For example, on this amendment, the Privacy Commissioner stated: "These provisions raise serious issues of privacy. The proposed amendment to PIPEDA, in effect, allows organizations to act as agents of the state by collecting personal information, without consent for the sole purpose of disclosing this information to government and law enforcement agencies. Under the existing provisions of PIPEDA, this information is collected with the knowledge and consent of the individual. This is fair. The proposed amendment that would allow collection without consent is not." Both subjects are deal with in detail below.

---

[40] Mariana Valverde, "Governing Security, Governing through Security," in R.J. Daniels, P. Macklem, and K. Roach, (eds.), The Security of Freedom: Essays on Canada's Anti-Terrorism Bill (Toronto: University of Toronto Press, 2002), at p. 85: "The impossibility of guaranteeing security is rooted in the fact that like justice, and like democracy, 'security' is not so much an empirical state of affairs but an ideal—an ideal in the name of which a vast number of procedures, gadgets, social relations, and political institutions are designed and deployed."

[41] Peter K. Manning, *Security in High Modernity: Corrupting Illusions* (Boston: Northeastern University, 2002).

[42] Oren Gross, "Cutting Down Trees: Law-Making Under the Shadow of Great Calamities", in R.J. Daniels, P. Macklem, and K. Roach, (eds.), *The Security of Freedom: Essays on Canada's Anti-terrorism Bill* (Toronto: University of Toronto Press, 2002), pp. 39-61.

[43] American Civil Liberties Union, Letter to the House Urging Rejection on the Final Version of the *USA PATRIOT Act* (October 23, 2001), online: < http://www.aclu.org/NationalSecurity/NationalSecurity.cfm?ID=9222&c=111>.

[44] *An Act to amend certain Acts of Canada, and to enact measures for implementing the Biological and Toxic Weapons Convention, in order to enhance public safety*, S.C. 2004, c. 15 [*Public Safety Act, 2002*] was finally introduced as Bill C-7; previous versions were introduced as Bills C-16, C-17 (37th Parliament - 2nd Session (Sept. 30, 2002 - Nov. 12, 2003)) and C-55 and C-42 (37th Parliament - 1st Session (Jan. 29, 2001 - Sept. 16, 2002)).

[45] Most recently in the comments of Jennifer Stoddart, Privacy Commissioner of Canada, to the Senate Standing Committee on Transport and Communications on Bill C-7, the Public Safety Act, 2002, March 18, 2004. Online: < http://www.privcom.gc.ca/speech/2004/sp-d_040318_e.asp>.

[46] See *Public Safety Act, 2002*, s. 5, enacting new ss. 4.7 and 4.8 of the *Aeronautics Act*.

LEGAL PROTECTION OF PRIVACY RIGHTS IN RELATION TO STATE SECURITY

What is the present law regarding the balancing of privacy rights and state security in Canada? Knowing the baseline of the legal protection of privacy is of great assistance in deciding if the balance between security and privacy struck by the government in recent initiatives is reasonable.

Charter *Protection of Privacy*

As for constitutional (*Charter*) protection of privacy, despite some suggestions that privacy is part of fundamental s. 7 rights (life, liberty and security of the person),[47] the majority of analysis has been in the context of s. 8, search and seizure applications. In *Hunter* v. *Southam*,[48] Chief Justice Dickson discussed the relevant balancing of a "reasonable expectation of privacy" and the state's interest in state security:

> The state's interest in detecting and preventing crime begins to prevail over the individual's interest in being left alone at the point where credibly-based probability replaces suspicion. History has confirmed the appropriateness of this requirement [page 168] as the threshold for subordinating the expectation of privacy to the needs of law enforcement. Where the state's interest is not simply law enforcement as, for instance, where state security is involved, or where the individual's interest is not simply his expectation of privacy as, for instance, when the search threatens his bodily integrity, the relevant standard might well be a different one. [Emphasis added.]

This confirms that the legal standard for balancing privacy rights and state security could be less than a "credibly-based probability". However, the Supreme Court did not decide what the new standard was, and subsequent cases have not yet considered the standard at the Supreme Court level. This means it is open, legally, for the government to assert that mere suspicion is a constitutionally defensible standard in certain cases of dealing with threats to state security. It is a position the government has taken in the legislation described below.

As noted by one author, the Supreme Court of Canada also has adopted the sliding scale of interpretation of "reasonable expectation of privacy."[49] That is, where a reasonable person would expect surveillance, such surveillance no longer is a privacy violation. This goalpost moving approach is unfortunate, in that all the government therefore must do is adopt a new set of surveillance rules, habituate people to the surveillance, and then rely upon that familiarity to justify the surveillance. Very recent Supreme Court decisions on privacy rights and the *Charter* suggest this will be the law for some time.[50] What this means, however, is that the central

---

[47] See Legal Opinion of Roger Tassé for George Radwanski, Privacy Commissioner of Canada, "whether the API/PNR Initiative of CCRA under the aegis of the *Customs Act*, is objectionable on constitutional grounds, because it contravenes the requirements of the *Canadian Charter of Rights and Freedoms*." Online: <http://www.privcom.gc.ca/media/nr-c/opinion_021122_rt_e.asp> (Tassé Opinion). This opinion concludes that: "It is clear from these decisions that the courts in Canada have integrated privacy rights as part of the concept of liberty in s. 7." The authors think this opinion is too hopeful. There is no constitutional protection of privacy *per se* in the *Charter*. In addition, locating the right to privacy within the "liberty" interest in s. 7 reduces the "offensiveness" of surveillance by either asserting that surveillance does not affect liberty, or that one's reasonable expectation of privacy, like one's liberty, is bounded by overriding societal requirements.

[48] [1984] 2 S.C.R. 145. Quote is from pp. 167-8.

[49] See Austin, *op. cit.*, at pp. 262-3.

[50] See *R.* v. *Tessling*, 2004 SCC 67 (October 29, 2004) where the Supreme Court of Canada concluded that infrared scanning of homes without a warrant for "heat pictures" to look for marijuana grow-operations was not a violation of s. 8 of the *Charter*, as the accused had no reasonable expectation of privacy in the "informational" aspect of the heat loss.

question of whether systematic state surveillance and other privacy-intrusive government actions such as data aggregation and matching may never be balanced against the freedom of action that citizens and consumers had become accustomed to in Canada prior to September 11.

Personal Information Protection and Electronic Documents Act (PIPEDA)

Quite outside of the Charter jurisprudence, the federal privacy legislation the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*) sets out a different legal regime that attempts to define standards for the respect of privacy in the private sector,[51] and provides individuals recourse to the Office of the Privacy Commissioner of Canada (OPCC) for redress if those standards are not met. The companion federal *Privacy Act* (governing information in the public (government) sector) has been described by the Supreme Court of Canada as "quasi-constitutional" legislation and PIPEDA is similar. However, neither the OPCC nor the courts have found a violation of privacy principles in PIPEDA by state security efforts thus far. Indications are that the question of this "balance" will not be favourable to the privacy rights. In addition, as noted below, any risk of this violation of PIPEDA has been sought to be avoided by recent amendments to PIPEDA that exempt "national security" questions from scrutiny. In this environment, consumers and citizens cannot look to the fledgling PIPEDA for legal support in the balancing of privacy rights and state security. What PIPEDA does provide, however, is a logical, legal framework in which to analyze the extent of the effect of security measures upon privacy (notably, the concepts of personal data, consent, collection, use and disclosure of personal data, and data retention).

In sum, therefore, privacy law in Canada has left open the door to more restrictive state security measures that on their face appear to violate privacy rights and standards of Canadians. Nonetheless, this paper relies on these concepts to articulate the reasonableness of the balance of privacy and security struck so far. This report relies upon a description of the privacy intrusions of state security efforts, whether "legal", "constitutional" or otherwise justified and public perceptions of this rebalancing of security and privacy. It also notes the possible (perhaps unconsidered, unexpected or undesirable) consequences of such a shift upon consumers and their behaviour. Finally, it attempts to answer if increasing privacy protection in response to increased security is possible, and if possible, if it simply is a placebo for the public in lieu of more direct political action.

STATE SECURITY MEASURES TARGETTING CONSUMER PRIVACY RIGHTS

A number of privacy rights have been modified directly by the introduction of national security measures that rely upon what would otherwise be a privacy breach for their effectiveness. This report details three major developments: the provision of air travel information by airlines to national security agencies; the possible access to personal information of Canadians under the *USA PATRIOT Act*; and the institution of fingerprinting and other profiling at the border under the US VISIT program.

Passenger Name Record/Advance Passenger Information (Flight Information)

One of the great pushes to obtain information since September 11 has been, understandably, in the area of information on those boarding aircraft. The move to share passenger information with the U.S. had predated September 11, but that occurrence spurred legislative action. Then the

[51] See the ten privacy principles in the schedule to PIPEDA. These form the core of privacy rights under the Act. Note that several provinces have adopted "substantially similar" personal information acts for the private sector that effectively replace PIPEDA within that province. These are: B.C., Alberta and Quebec. In some provinces a subset of privacy rights regarding health information only has been exempted from PIPEDA application: Manitoba, Alberta and soon, Ontario.

Anti-Terrorism Plan of October 2001 committed Canada to systematic sharing of flight information to combat risks to air security due to terrorist threats. In June 2003, the government took the first steps towards this goal by amending the *Customs Act*[52] and introducing the new *Passenger Information (Customs) Regulations*.[53]

It is important to realize that the information authorized to be collected and by the Canada Customs and Revenue Agency (CCRA)[54] under the new *Customs Act* amendment (s. 107.1) only affects persons on board aircraft arriving in Canada. It does not cover travel within Canada, nor from Canada to other nations. It does, however, include information on Canadians returning to Canada, not only foreign nationals. The main difficulty with the new s. 107.1 and the regulations was that the data derived from the requirement was to be matched with virtually any other information in the databases of the Canadian federal government under the interdepartmental information sharing provisions of the *Customs Act* (s. 107).[55] It is notable that the *Customs Act* allows the Minister discretion to decide if "the public interest in providing the information clearly outweighs any invasion of privacy" (s. 107(6)(a)). In addition, under the *Customs Act*, a broad range of persons can be given access to customs information for regular law enforcement purposes.[56] Further, under s. 107(8), the customs information may be transferred to a foreign government if there is in place an agreement for such information sharing. Canada signed the *Agreement on Air Transport Preclearance between The Government of Canada and The Government of the United States of America*, on January 18, 2001.[57]

In an October 2002 "Fact Sheet" CCRA confirmed that this API/PNR[58] information on people entering Canada was "customs information" and that it would be disclosed not only for the

---

[52] The amendment (S.C. 2001, c. 25 s. 61, (in force: 2001 Nov 29, SI/2001-115)) added new s. 107.1 to the *Customs Act*, which reads:

> *Passenger information*
>
> 107.1 (1) The Minister may, under prescribed circumstances and conditions, require any prescribed person or prescribed class of persons to provide, or provide access to, prescribed information about any person on board a conveyance in advance of the arrival of the conveyance in Canada or within a reasonable time after that arrival.
>
> *Disclosure*
>
> (2) Any person who is required under subsection (1) to provide, or provide access to, prescribed information shall do so despite any restriction under the *Aeronautics Act* on the disclosure of such information.

[53] SOR/2003-219, registration June 12, 2003, the Regulations are deemed to have come into force on October 4, 2002.

[54] To be the Canada Revenue Agency (CRA). Note that the CRA and Citizenship and Immigration Canada have been administratively amalgamated under the Canada Border Services Agency (CBSA), and departmental legislation for CBSA is pending: see *An Act to establish the Canada Border Services Agency*, introduced as Bill C-26 in the 38th Parl., 1st Sess.

[55] The API/PNR information gathered under Section 107.1 and the new regulations is deemed to be information under s. 107(1)(a) of the *Customs Act*, and therefore "customs information".

[56] See *Customs Act*, s. 107(4), (5) and (7) for a very long list.

[57] Note that Canada brought into force the *Passenger Information Regulations (Preclearance Act)*, SOR/2002-147 (in force May 1, 2002), which in a schedule lists the advance passenger information and passenger name record information the U.S. requires for travel to that country. Thirty-four items of information were to be transferred under this regulation for each passenger flying to the U.S.

[58] It is also important to understand the difference between Advance Passenger Information (API) and Passenger Name Record. API is name, birthdate, gender, citizenship, nationality and passport number. PNR is much wider and is whatever information the authorities involved have decreed is relevant in

purposes of fighting terrorism but also to help track pedophiles, prevent money laundering and even for the vague purpose of "protecting the health and safety of Canadians".[59]

The European Union was concerned with the Canadian *Customs Act* regime due to the collection and disclosure of personal information of European Union citizens coming to Canada, which it feared was not in accord with the *European Convention on Human Rights* and the *Fundamental Rights of the European Union* and could be transferred without consent to other countries.[60]

In Canada, the Office of the Privacy Commissioner of Canada also assailed the new *Customs Act* amendment and regulations. The then Privacy Commissioner, George Radwanski, was worried about the precedent of allowing systematic data collection on any group of persons, but especially "law abiding Canadians", without a warrant, from a non-government source and its combination with any other government data. His second concern was the length of the retention of the data, which was initially stated by CCRA to be 6 years. In his *Annual Report* to Parliament of 2001-2, at p. 6, he said this about the Customs API/PNR database:

> All this personal information - more than 30 data elements including every destination to which we travel, who we travel with, how we pay for the tickets (sometimes including credit card numbers), what contact numbers we provide, even any dietary preferences or health-related requirements we communicate to the airline - will be available for an almost limitless range of governmental purposes under the broad information-sharing provisions of the Customs Act.
>
> Those purposes, by the Government's own account, include everything from routine income tax investigations to trying to flag Canadians as potential pedophiles or money launderers solely on the basis of their travel patterns.
>
> This is unprecedented. The Government of Canada has absolutely no business creating a massive database of personal information about all law-abiding Canadians that is collected without our consent from third parties, not to provide us with any service but simply to have it available to use against us if it ever becomes expedient to do so. Compiling dossiers on the private activities of all law-abiding citizens is the sort of thing the Stasi secret police used to do in the former East Germany. It has no place in a free and democratic society. [Emphasis added.]

Because of, or perhaps despite, the rhetorical flourishes of the Privacy Commissioner, the criticism did lead to the Minister for the CCRA, in a letter to the Privacy Commissioner, to undertake to limit both the purposes for which the data would be disclosed and the retention of the data.[61] Although somewhat complex, the Minister generally agreed that data would be disclosed for certain purposes within certain timeframes. Although all API/PNR data would be

---

relation to travel, but generally includes all information gathered by airlines and reservation systems to make bookings, such as itinerary information, payment information and customer service information. CCRA began by collecting API on October 7, 2002 and PNR on July 8, 2003 (see EC WP Canada Report below, p. 6.).

[59] This Fact Sheet was available as of 18 November 2002 at http://www.ccra-adrc.gc.ca/newsroom/factsheets/2002/oct/api-e.html, but now is superseded by the "CCRA Fact Sheet: Advance Passenger Information/Passenger Name Record", (July 2003). Online: < http://www.cbsa-asfc.gc.ca/newsroom/factsheets/2003/july/july_api_pnr-e.pdf>.

[60] Opinion 3/2004 on the level of protection ensured in Canada for the transmission of Passenger Name Records and Advanced Passenger Information from airlines (Brussels, European Commission, Data Protection Working Party). ("EC WP Canada Report") Online: <http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp88_en.pdf>

[61] See "News Release: Breakthrough for Privacy Rights" Office of the Privacy Commissioner of Canada, April 9, 2003, containing Letter from Revenue Minister Elinor Caplan, April 8, 2003 and reply of the Privacy Commissioner.

retained for 6 years, in the first 72 hours PNR information would be used by customs officers to "assess risk". (What "assess risk" means, or how it functions, was not inquired into by the Privacy Commissioner and was not detailed by the CCRA. On one reading of the *Customs Act*, it could be shared with other departments and agencies to check it against, for example, known terrorist profiles or outstanding warrants.) The next period was from 72 hours to 2 years. During this period, the information is "depersonalized" or anonymized and used on an aggregate basis by customs intelligence analysts. However, "re-personalization" can occur if either the Customs department is using it for "customs purposes" or if another department requests it and has a warrant. Finally, from 2 years to 6 years (since shortened to 3½ years), the information is depersonalized, except where Customs is using it to "fulfill the CCRA's mandate regarding the security of Canada",[62] and, where necessary for a national security (terrorism) investigation or the "defence of Canada", the CCRA Minister can depersonalize and share the information with "agencies that have a national security or defence mandate".[63,64]

Interestingly, the *Passenger Information (Customs) Regulations* were deemed to have come into force on October 4, 2002 although they were registered on June 12, 2003. This is unusual for regulations, which normally come into force upon registration or later. However, even this backdating leaves the period from September 12, 2001 to May 1, 2002[65] without explicit legal authority for transfer of API/PNR to the U.S. (to October 3, 2002 for other countries). Did Canadian airlines transfer passenger information during this period despite the lack of a legal requirement to do so? In the United States, commercial airlines did admit to providing API/PNR information to government soon after the September 11 attacks, and well before there was any legal requirement to do so.[66] Recent class action lawsuits for privacy violations due to this disclosure of personal information have so far, however, been unsuccessful.[67] Although there is no indication any Canadian air carrier did provide API/PNR information during this window, it is without doubt that they would have felt pressure to do so.

There is also a fair level of legislative legerdemain still continuing to this day regarding API/PNR information. However, to understand this, it is necessary to turn to the provisions of the *Public Safety Act, 2002*.

The *Public Safety Act, 2002* amends the *Aeronautics Act* to allow disclosure of API/PNR to the Minister of Transportation, and, once certain other amendments come into force, to CSIS and the RCMP. These changes to the API/PNR collection scheme create a new regime, parallel to, but different than, the *Customs Act* regime for dealing with API/PNR. In effect, the new *Aeronautics Act* regime uses the idea of threats to "transportation safety" as a basis for demanding access to API/PNR from airlines and reservation systems operators. What separates this regime most from the Customs regime is that the *Aeronautics Act* regime applies to flights out of Canada, as well as Canadian domestic flights.

---

62 *Ibid*.

63 See Thomas B. Riley, "Security vs. Privacy: Striking the Balance: Riley, "Security vs. Privacy: Striking the Balance: A Comparative Analysis Of Canada, The United Kingdom And The United States", prepared for the Commonwealth Centre for E-Governance (September, 2003) at p. 11. Online: < http://www.electronicgov.net/pubs/research_papers/slp/Sec&PrivPaper03n03.pdf>.

64 See "CCRA Fact Sheet: Advance Passenger Information/Passenger Name Record", *supra*.

65 See above footnote regarding the *Passenger Information Regulations (Preclearance Act)*, which came into force May 1, 2002.

66 See CNN.com, "Northwest: Passenger data given to government", January 18, 2004, online: < http://www.cnn.com/2004/TRAVEL/01/18/northwest.privacy.ap/> and see "American Air Admits Passenger Data Disclosure", Airwise News, April 12, 2004, Online < http://news.airwise.com/stories/2004/04/1081762776.html>. JetBlue Airways first announced this had been done by that airline in September 2003. Other U.S. airlines since have admitted a similar role.

67 Associated Press, "Judge Rejects Passenger Data Lawsuits", available at Forbes.com, June 9, 2004, online: < http://www.forbes.com/feeds/ap/2004/06/09/ap1405352.html>. Decision at: < http://www.nysd.uscourts.gov/courtweb/pdf/D08MNXC/04-04317.PDF>.

At present, if the Minister of Transport believes there is an "immediate threat" to life or transportation property, the Minister may ask for the API/PNR information from the air carrier or reservation system. He or she may disclose the information further, but only for the purposes of transportation security, and only to specified bodies (which do not include the RCMP or police, or CSIS).[68] Of note, there is no systematic provision of all API/PNR information to the Minister of Transport under this present API/PNR regime – only provision of information requested upon suspicion.

However, the requirement of the Minister's "belief" in an "imminent threat" to transportation security begs the question, "how does the Transport Minister know of an 'imminent threat' unless he or she already has reviewed the API/PNR information (and determined that the person on a watch list,[69] for example, of suspected terrorists known to be contemplating a hijacking is about to board)?" Although the Minister of Transport could rely upon other sources of intelligence regarding terrorist or other aviation threats, there appears to be no impediment to the Transport Minister being informed about such a threat by another department or agency. This other department or agency could be the RCMP or CSIS, using *Customs Act* API/PNR information, in concert with other law enforcement and national security information, as a basis for informing the Transport Minister to make a decision on an "imminent threat". This is because the new *Aeronautics Act* API/PNR regime does not prohibit the use of *Customs Act*-collected API/PNR information in this fashion.

Now, therefore, airlines must provide API/PNR to the Minister of Transport on request for transportation security reasons and routinely to foreign countries that ask for it under their own legal authority. However, as noted, it is not clear that the *Customs Act* regime for API/PNR disclosure has been wholly replaced by these amendments from the *Public Safety Act, 2002*. This means there are probably two channels of API/PNR information disclosure presently operating in Canada.

This situation will be aggravated when the final amendments (from the *Public Safety Act, 2002*) to the *Aeronautics Act* are in force. These will require airlines and reservation system operators to comply with requests for passenger information from the Canadian Security Intelligence Service (CSIS) or the Royal Canadian Mounted Police (RCMP). The federal government claims that police and national security access to consumers' information will only available "for very restricted purposes" and must be destroyed within seven days[70] "unless it [is] reasonably required for the purposes of transportation security or addressing terrorist threats."[71] The bulk of the disclosure to CSIS and the RCMP under these new amendments will be for the purpose of "transportation security". However, the purposes listed in the new amendments include disclosure to any "peace officer" if the information "would assist in the execution of a warrant".

This is quite simply a dragnet for catching suspected criminals. Likewise, disclosure may be made to a CSIS officer for the purpose of investigation of "threats to Canada". The amendments therefore also create a general-purpose dragnet for those under active CSIS investigation.

---

[68] See s. 4.81(3) and (4) of the *Aeronautics Act*, as am.. The disclosure may be made to: (a) the Minister of Citizenship and Immigration; (b) the Minister of National Revenue; (c) the chief executive officer of the Canadian Air Transport Security Authority; and to persons within their department or agency.

[69] See "Legal concerns delay Canadian version of airline watch list", Canadian Press, November 1, 2004.

[70] See s. 4.82(14) limits retention to 7 days unless required for the security of Canada or for transportation security. Presumably it is not retained for regular criminal investigations beyond 7 days as the warrant will have been executed upon the person involved within 7 days.

[71] Canada, Public Safety and Emergency Preparedness Canada, "Bill C-7 (Public Safety Act): RCMP and CSIS access to airline passenger information," News Release (20 January 2004).

The Office of the Privacy Commissioner of Canada has criticized this checking for outstanding warrants for non-terrorist criminal behaviour. The Privacy Commissioner stated that allowing police and government security agents to access information from private sector corporations without a warrant for criminal offences considerably expands state surveillance and law enforcement powers and threatens the privacy of all citizens and consumers in Canada.[72] She stated to the Senate Committee studying the bill:

> Proposed subsection 4.82(4) allows the RCMP to match the passenger information it receives, even for flights entirely in Canada, with any information under its control. Subsection 4.82 (11) then empowers RCMP officers to notify local authorities or take appropriate steps to effect an arrest if, as a result of this data match, they identify anyone who is wanted on a warrant for any of a wide number of Criminal Code offences.
>
> The list of offences in the proposed regulations is lengthy. It includes arson; it includes procuring; and it includes forgery of a credit card. <u>These are offences that have no connection whatsoever with national security or transportation safety</u>.
>
> <u>One of the basic fair information principles is that information collected for one purpose should be used for that purpose only. This legislation violates that principle.</u> Air carriers collect personal information for the purpose of facilitating travel. This legislation will require them to turn that information over to law enforcement and national security agencies for purposes unrelated to facilitating travel, and largely unrelated even to air transportation. [Emphasis added.]

The Privacy Commissioner called upon the Senate Committee not to allow this amendment due to its apparent violation of privacy principles. The Act was passed without amendment to this power. However, the section allowing disclosure to the RCMP and CSIS remains unproclaimed. Nevertheless, since the information could well be continuing to flow to these agencies under the *Customs Act* regime, it appears possible it is being provided to security agencies in any case.

ATTITUDES OF CANADIANS TOWARDS COLLECTION AND TRANSFER OF API/PNR INFORMATION

Just how much of a problem is the collection, use and disclosure of API/PNR information for Canadians? In the POLLARA Inc. survey, 22% of Canadians were "very concerned" with the gathering and processing of flight information (whether on domestic or international flights) by the Canadian government and 36% were "somewhat concerned". A full forty per cent stated they were not concerned at all. However, this moderate level of concern increases when the question turns to the sharing of this flight information with other countries: in that case 32% were "very concerned" and 27% "somewhat concerned". Nearly forty percent continued to have no qualms. It appears a solid minority of Canadians (40%) simply is unconcerned with any use of personal flight information for any purpose, and its disclosure to anyone, perhaps on the assumption that they have "nothing to hide". It also appears Canadians continue to have an elevated level of trust that their government will not misuse personal flight information. However, concern rises amongst the remaining 60% when they become aware that their movements by aircraft and other details are being provided to the U.S. and other countries. Overall, more Canadians appear to feel sharing flight data with other countries crosses a line that represents for them a privacy violation. This is consistent with their attitudes to outsourcing of personal information cross-border, dealt with below.

---

[72] "Speech to Senate Standing Committee on Transport and Communications: Bill C-7, the *Public Safety Act, 2002*" (Ottawa, 18 March 2004), online: http://www.privcom.gc.ca/speech/2004/sp-d_040318_e.asp .

Finally, it is unclear if Canadians have a good sense of what API/PNR data presently is being collected, how it is used and to whom it is disclosed. Equally, it is unknown if Canadians are aware of the existence of, or scope of, the plans for an increase in the use and disclosure of API/PNR under the unproclaimed *Public Safety Act, 2002* amendments. This research should be undertaken, perhaps by the Office of the Privacy Commissioner of Canada, prior to finalization of this regime to allow Canadians a voice in the size, scale and design of API/PNR data management. Finally, no matter what regime is chosen for API/PNR data, it should be better explained by government to average Canadians, so that they might be in a position to judge the need for such measures and their effectiveness, and to render a political judgment on this and other security matters.

API/PNR, PROFILING AND THE MAHER ARAR INQUIRY

In addition to privacy concerns, the API/PNR regime has the potential to "sort" travelers, possibly by stereotypes. Since September 11, there have been ongoing allegations of discrimination and racial profiling in Canada, particularly amongst Arab and Muslim Canadians, for whom the aftermath of September 11 "has been an interesting time [that] has meant… a sense of psychological internment akin to what our Japanese compatriots felt during World War II in Canada."[73] Results of a recent Ipsos-Reid survey show that more than half of Canadians (52%) believe that our country's security forces unnecessarily target Arab Canadians.[74]

The case of Maher Arar may yet shed light on whether Canada's API/PNR system is prone to the negative effects of profiling.[75] Mr. Arar is a Canadian citizen who, after landing in the U.S. en route to in Canada in 2002, was sent to Syria by American security forces after they had contacted their Canadian counterparts with suspicions that he was involved in terrorist activities. Although not yet proven, it is likely that part of that information was API/PNR. In Syria, Arar was tortured and jailed for ten months before the Canadian government agreed to facilitate his return to Canada. This case has cast doubt in Canadians' minds about the U.S. and our own governments' security forces: "three quarters of Canadians (75%) believe that the United States was unjustified in deporting Maher Arar to the country he was born as opposed to Canada where he lives as a Canadian citizen."[76]

---

[73] Canadian Arab Federation President Raja Khouri, "Impacts on Musli and Arab Community in Canada" in *Anti-Terrorism and the Security Agenda: Impacts on Rights, Freedoms and Democracy*, Report and Recommendations for Policy Direction of a Public Forum organized by the International Civil Liberties Monitoring Group (Ottawa, 17 February 2004) 64 at 64 [*Anti-Terrorism and the Security Agenda*]. See also Rasha Mourtada, "A climate of fear: Some Canadian Muslims say prejudice is affecting their role in the workplace" *Canadian Business* (29 March 2004); Michelle MacAfee and Amy Carmichael, "Muslims endure a year of blame, slights and fear" *Edmonton Journal* (11 September 2002). See also Colin Freeze, "Critics use Arar case to slam detentions" *The Globe and Mail* (13 November 2003); Thomas Walkom, "Canadian citizen let down by his government" *Toronto Star* (5 November 2003); Haroon Siddiqui, "Ottawa must stand up for our democratic traditions: Canada copying America's methods" *Toronto Star* (12 October 2003); Cassandra Szklarski, "Five men held in terrorist probe to sue: Their lawyer says no charges have been laid over allegations the men pose a security threat" *The Hamilton Spectator* (11 October 2003).

[74] Ipsos-Reid, "Three Quarters (75%) Believe U.S. Unjustified In Deporting Maher Arar" *Ipsos News Center* (6 February 2002), online: Ipsos-Reid <http://www.ipsos-na.com/news/pressrelease.cfm?id=2042&content=full>.

[75] See Ottawa, Canada, Public Safety and Emergency Preparedness, *Deputy Prime Minister Issues Terms of Reference for the Public Inquiry into the Maher Arar Matter*, News Release and Backgrounder (5 February 2004); and Canadian Broadcasting Corporation, "Maher Arar: Timeline" *CBC News Online* (21 June 2004), online: Canadian Broadcasting Corporation <http://www.cbc.ca/news/background/arar>.

[76] Ipsos-Reid, *supra* note 75.

It appears from the Arar inquiry thus far that the practice of allowing governments to access airline passengers' personal information as a means of enhancing national security may entail considerable costs to individual privacy, trust in government, and constitutional rights. The *Charter*, s. 1, requires that any Canadian laws and procedures that impair fundamental rights *minimally impair* those rights, including our right to be free from unreasonable search and seizure, arbitrary detention, and delay when stopped or investigated by state officials. If the Arar inquiry concludes his rights were violated through the use of API/PNR, it raises a number of questions.

- Will accessing passenger data actually improve national security?
- How and by whom will the effectiveness of the API/PNR system be measured?
- Why is the Canadian government allowing other governments to spy on Canadian airline passengers?
- Should API/PNR powers be given to CSIS and RCMP and if so, in relation to what (terrorism, regular law enforcement)?
- Why is there no sunset clause on the API/PNR system legislation?
- Does the API/PNR system represent a minimal impairment of Canadians' human and privacy rights?
- How will our government ensure that when agents access or transfer API/PNR data to and from corporate or foreign government agents, Canadians are protected from identity theft and other improper use of their personal information?

As noted, the vigilance of Canadians is required to ask for answers to these and similar questions no matter the eventual outcome of the Arar inquiry nor the actual shape of the API/PNR regime in Canada, provided it continues.

USA PATRIOT Act and Outsourcing of Private Information Processing

In the U.S., the *USA PATRIOT Act* now gives law enforcement and foreign intelligence agents broad powers to covertly and overtly investigate, detain, arrest, imprison, and deport individuals suspected of supporting or engaging in terrorist activity.

Laws in the U.S. also now allow state agents to apply in secret for authorization to collect records, including business, personal and confidential information and "any tangible thing," whether or not "things" seized belong to individuals under investigation. Officials are not obliged to inform individuals of reasons for such searches and/or seizures and, if searches reveal no "relevant" evidence, officials never need to inform individuals of the search.[77] To get approval for similar search warrants before September 11, officials had to meet a relatively high standard of proof by showing "specific and articulable facts" that created a reasonable belief of finding evidence to further an investigation. The *USA PATRIOT Act* amendments reduced that standard to one of "relevance" – officials need only show that they are likely to find "any tangible thing" *relevant* to a foreign intelligence or terrorism investigation.[78]

Section 215 of the *USA PATRIOT Act* amended the *Foreign Intelligence Surveillance Act of 1978*[79] (*FISA*) by expanding the U.S. government's power to secretly investigate foreign organizations, businesses, and individuals. *FISA* also prohibits individuals from revealing that they are subject to such investigations.[80] *FISA* as amended by the *USA PATRIOT Act* now

[77] *USA PATRIOT Act*, § 215.
[78] See Michael Geist & Milana Homsi, *The Long Arm of the USA Patriot Act: A Threat to Canadian Privacy?*, Submission on the USA Patriot Act to the B.C. Information and Privacy Commissioner (July 2004), at 6-7.
[79] 50 U.S.C. § 1801 et seq.
[80] *Ibid*. § 1861.

"empower[s] the US Foreign Intelligence Surveillance Court (FIS Court) to issue secret orders to enable the FBI to obtain records from third parties."[81]

In British Columbia, this issue came to a head when the British Columbia Government and Service Employees' Union (BCGEU) filed a lawsuit against the government of B.C.:

> . . to stop the British Columbia Ministry of Health Services from contracting out the administration of British Columbia's public health insurance program, the Medical Services Plan, to a US-linked private service provider. One of the BCGEU's claims was that the proposed outsourcing would contravene British Columbia's *Freedom of Information and Protection of Privacy Act* (FOIPPA) by making the personal health information of British Columbians accessible to US authorities under section 215 of the USA Patriot Act.[82]

This prompted an investigation by the Office of the Information and Privacy Commissioner of B.C. and a very detailed, comprehensive report on the issue in October 2004 (BC Outsourcing Report).[83] This brought the issue of personal information outsourcing and the national security laws of other countries, specifically the U.S., directly into focus for Canadians.

The B.C. Outsourcing Report's conclusions were that the *USA PATRIOT Act* would indeed allow disclosure of Canadian personal information for U.S, national security purposes where a U.S.-based company had received Canadian personal information for processing. The same result also would likely occur if the information was given to a company in Canada, that had a U.S. parent, although there was a small chance the U.S. FIS Court would not require delivery of that information to the U.S. authorities if there were a clear Canadian law prohibiting such disclosure for U.S. purposes while the information was in Canada.[84]

The POLLARA Inc. survey asked the question of Canadians: "To what extent are you concerned that U.S. firms receiving your personal information from Canadian companies may have to share it with the U.S. government under U.S. security laws?" Forty-six percent (46%) said they were "very concerned". Twenty-seven percent (27%) stated they were "somewhat concerned". Only 25% stated they were "not concerned at all". This indicates there is a high level of elevated concern amongst Canadians regarding the risk of U.S. national security access to their personal information due to outsourcing or other information handling by U.S.-located or U.S.-affiliated companies.

The B.C. Outsourcing Report in its recommendations called for an amendment to B.C. law (called a "blocking statute") that would prohibit companies based in B.C. from disclosing B.C. residents' personal information when requested under the USA PATRIOT Act, and other recommendations, including a recommendation the federal government do a similar audit of outsourcing – which the federal government has indicated it will pursue. However, the B.C. Outsourcing Report stopped short of suggesting an outright ban on all outsourcing to U.S.-affiliated data processing companies.[85] Given the results of the POLLARA Inc. survey indicating Canadians are not at all happy with having their personal information available to U.S. security forces under this law, and the obvious affront to Canadian sovereignty such a law countenances, the authors of this report

---

[81] British Columbia, Office of the Information and Privacy Commissioner, Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing (October 2004). Online: http://www.oipc.bc.ca/sector_public/usa_patriot_act/pdfs/report/privacy-final.pdf (B.C. Outsourcing Report) at 63.

[82] *Ibid.*, at 11.

[83] The B.C. Outsourcing Report was released as this report was going to press. The B.C. Outsourcing Report's discussion of the issue is a model of thoroughness and should be consulted for a full discussion of this issue. For this reason, this report does not duplicate those efforts.

[84] *Ibid.*, p. 18.

[85] *Ibid.*, pp. 111-114.

suggest such a ban (pending negotiation with the U.S. of a comprehensive data "safe harbour" agreement) is the only method for avoiding the subjection of all Canadian consumers to the national security regime not only of Canada, but of the U.S. as well.

US-VISIT

The "U.S. Visitor And Immigrant Status Indicator Technology Program" (US VISIT) is a Department of Homeland Security effort to screen foreign nationals at U.S. borders. US VISIT uses biometric technologies to take a scan of each foreign travelers two index fingers and a digital photograph of each traveler. The biometric information must compare favourably with the biometric information stored in new biometric ready passports that the U.S. has demanded for all persons entering the U.S. The biometric information is used to compare against databases of suspected terrorists.

Since September 30, 2004,[86] US VISIT applies to all foreign visitors to the U.S.,[87] with the exception of Canadian citizens.[88] This exception appears to be an administrative exception or bilateral courtesy of the U.S. that could be withdrawn at any time. It is also crucial to note that US VISIT presently applies to Canadian permanent residents, as they are not Canadian citizens.

Access to and use of US VISIT data is not limited to U.S. immigration but also is available to general U.S. law enforcement. This is because:

> . . . the USA PATRIOT Act requires that US-VISIT be able to interface with law enforcement databases to be used by federal law enforcement to identify and detain individuals who pose a threat to national security. The USA PATRIOT Act also requires that US-VISIT be accessible to all law enforcement and intelligence officers responsible for investigation and identification of aliens. Under the Aviation and Transportation Security Act, the transmission of manifest information may be shared with other federal agencies, upon request, for the purposes of protecting national security. Moreover, the Data Management Improvement Act of 2000 grants the Attorney General discretion to permit other federal, state, and local law enforcement officials to have access to the data contained in the integrated entry and exit data system for law enforcement purposes.[89]

DHS states that: "Personal data will be securely stored and is made available only to authorized officials on a need-to-know basis to help protect the nation against those who intend harm to U.S. citizens or visitors and to ensure integrity in our immigration system."[90] It is not clear if the reference to "those who intend harm" include non-terrorist criminals. However, since there is

---

[86] US VISIT was phased in for countries eligible for the U.S. Visa Waiver program. These countries include the U.K., France, other European countries, as well as Australia and New Zealand. However, since September 30, all nationals from these countries are subject to US VISIT.

[87] US VISIT is a huge administrative undertaking and it is being phased in. According to the DHS "Fact Sheet: U.S. – Canada Land Borders":

> "US-VISIT entry procedures are currently in place at 115 airports and 15 seaports. Exit procedures are being piloted in four airports and one seaport and will be operational in additional airports and seaports within the next few months. By December 31, 2004, US-VISIT entry procedures will be implemented in the secondary inspection areas at the 50 busiest land ports of entry and to all secondary inspection areas at all remaining land ports of entry by December 31, 2005."

Online: < http://www.dhs.gov/interweb/assetlibrary/US-VISIT_Canada_Fact_Sheet-English.pdf>.

[88] See the "Fact Sheet: U.S. – Canada Land Borders" for a full list of the those categories of Canadians who are variously not required and required, to submit to US VISIT.

[89] See Electronic Privacy Information Center, "US-VISIT Page", online: http://www.epic.org/privacy/us-visit/

[90] See the "Fact Sheet: U.S. – Canada Land Borders", *supra*.

explicit legislation allowing US-VISIT data to end up in national security files throughout the U.S. government and in general law enforcement files anywhere in the U.S., it is likely to do so despite these hard-to-decipher DHS assurances. Theoretically, therefore, local U.S. police or the FBI may soon have your fingerprints and photograph.

US VISIT also has none of the usual data protection provisions such as a right of access and correction of data. In addition, there is no limit on the data retention, meaning this information, including biometric identifiers, could be kept indefinitely. This lack of "data rights" has been decried in the U.S. by the Electronic Privacy Information Center[91] and by Privacy International.[92] Privacy International's criticisms are that:

- [US] VISIT employs technology and techniques that are unreliable and unpredictable. The matching of information between a large number of systems generates substantial errors, while the use of biometrics such as finger-printing involves the risk of false accusations on a mass scale because of the inherent frailty of one to many systems.
- [US] VISIT ignores the legal concept of proportionality by creating mass surveillance in order to identify a relatively small number of suspects.
- [US] VISIT redefines due process. Where previously people would be fingerprinted and scrutinised upon suspicion, they are now all suspects until at least temporarily eliminated from suspicion. There is no meaningful oversight. While Europe has several mechanisms, such as the European Court of Human Rights, in North America protections are minimal as National Security interests trumps all rights of data protection.
- [US] VISIT abolishes all principles of privacy. It accumulates personal information indiscriminately, collecting and sharing this information for unforeseen purposes, and retaining it over our lifetimes

As noted, the U.S. presently is not requiring Canadian citizens to submit to US-VISIT. Canadian permanent residents, who are entitled to the benefit of the *Charter*, PIPEDA and related privacy legislation in Canada are, however. As noted, the exemption of Canadian citizens from US VISIT appears to be an administrative courtesy. Newspaper columnists recently have suggested Canadians should "play ball" on U.S. military defence initiatives such as the proposed missile shield in the upcoming NORAD agreement of 2006 or face the prospect of US VISIT applying to them.[93]

The existence of US-VISIT and the prospect of it applying to all Canadians raises the issue of the importance of border security in the national security efforts of both countries. Is biometric information, with its extreme privacy risks, necessary for border security? If so, how far should such sensitive information be disseminated in government? How can we keep borders open for trade but closed to terrorists? It also raises the issue of why the Canadian government thus far has been strangely silent regarding US-VISIT,[94] its likely violation of Canadian privacy principles, and despite its application to permanent residents and its possible application to all Canadians.

---

[91] See Electronic Privacy Information Center, "Comments Of The Electronic Privacy Information Center" to DHS Border and Transportation Security Directorate, Docket No. BTS 03-01, Interim Final Rule and Notice, February 4, 2004. Online: < http://www.epic.org/privacy/us-visit/us-visit_comments.pdf>.

[92] Privacy International, "The enhanced US border surveillance system: an assessment of the implications of US-VISIT", online: http://www.privacyinternational.org/issues/terrorism/rpt/dangers_of_visit.pdf .

[93] John Ibbitson, "A fragile exemption from border restrictions" Globe and Mail, November 16, 2004, p. A4 and "Time to advance the cause of Canada-U.S. relations" Globe and Mail, April 28, 2004, p. A4.

[94] The European Union Working Party on Privacy has not criticized US VISIT. It is suggested in the Privacy International materials that European countries have for some years had similar screening systems,

so are in no position now to complain about this border-control development on privacy grounds. Could Canada be considering extending US VISIT or a similar program to Canadian border entry points?

STATE SECURITY MEASURES INCREASING SURVEILLANCE

A number of national security measures adopted in the wake of 9/11 have significantly increased surveillance of the Canadian public in general and consumers in particular. Increased monitoring of communications, calls for national identification documents with biometrics and state surveillance via closed-circuit television all have become important issues.

Interception of Electronic Communications

Canadian courts have historically recognized the need for strict controls on the ability of law enforcement agents to intercept private communications.[95] This has bred a high expectation of privacy in private communications in Canada.

To intercept cellular or wireline telecommunications, authorities must obtain a wiretap warrant.[96] Judges can authorize such warrants on the basis of evidence and reasonable grounds to believe that a serious crime has been or is about to be committed. Canadian law does not specifically address public surveillance or interception of email or Internet activity. However, authorities can apply for warrants authorizing them to do so under the *Criminal Code*,[97] the *Canadian Security Intelligence Service Act*,[98] or the *Competition Act*.[99] Other Canadian laws express concern for individual privacy and prohibit interception of private communications.[100]

Privacy law statutes, the common law and privacy law consideration restrict and inform the interpretation of the law of surveillance of private communications in Canada. Courts and administrative tribunals throughout Canada have recognized (1) the importance of protecting individuals' reasonable expectation of privacy; (2) that the surveillance and interception of private communications involves balancing competing interests; and (3) that to be demonstrably justifiable, interception and surveillance techniques must: (a) be necessary to achieve a stated purpose; (b) be effective in doing so; (c) not impair privacy and other civil rights and liberties more than other available measures; and (d) be used only for their stated objectives.[101] Further to this, the Federal Court of Canada recently interpreted *PIPEDA* as a "fundamental law of Canada."[102] It also accepted the four-part test introduced by the Privacy Commissioner of Canada to determine "appropriate purposes"[103] in the context of workplace video surveillance.[104] By

---

[95] See generally, R. Hubbard et al., *Wiretapping and other electronic surveillance : law and procedure* (Aurora: Canada Law Book, 2000).
[96] *Criminal Code, supra* note 150, ss. 184-187.
[97] *Ibid*., Part V ("Invasions of Privacy").
[98] Warrants to intercept communications issued under s. 21 of the *Canadian Security Intelligence Service Act*, R.S.C. 1985, c. C-23 [*CSIS Act*] are exempt from the privacy protections in Part VI of the *Criminal Code*.
[99] R.S.C. 1985, c. C-34, ss. 15 and 16.
[100] See *e.g. Radiocommunications Act*, R.S.C. 1985, c. R-2, s. 9(2), which prohibits the unauthorized interception, use, and divulgence of radiocommunication without the sender's or the intended recipient's consent; and *Telecommunications Act*, S.C. 1993, c.38, s. 7(i), which highlights the "essential role" that telecommunications play in "the maintenance of Canada's identity and sovereignty" and "protection of the privacy of persons" as an objective of Canadian telecommunications policy. Federal laws regulating banks and postal services in Canada also include privacy protections.
[101] See *R.* v. *Duarte*, [1990] 1 S.C.R. 30; and *R. v. Weir* (1998), 213 A.R. 285 [*Weir*]. See also *Pacific Northwest Herb v. Thompson*, [1999] B.C.J. No. 2772; *Re Doman Forest Products Ltd*., 13 L.A.C. (4th) 275; *St. Mary's Hospital and H.E.U.*, (1997) 64 L.A.C. 382; and *Brewers Retail Inc. and United Brewers' Warehousing Workers' Provincial Board (Merson)*, (1999) 78 L.A.C. (4th) 394, as cited in Geist, *supra.*
[102] *Eastmond v. Canadian Pacific Railway*, 2004 FCC 852 (T.D.) [*Eastmond*].
[103] *PIPEDA*, s. 5(3).

analogy, a court could apply the same four criteria to determine the legitimacy of intercepting and/or conducting surveillance of communications technology, including e-mail and Internet use.

Much of the response from law enforcement to the challenge of new communications technologies has been through the bias of an international convention known as the Council of Europe's *Cyber-crime Convention*.[105] This international treaty in part seeks to bind signatories to implementing legislation that will aid law enforcement with "lawful access"[106] to electronic communications in whatever form. The treaty was coincidentally timed with September 11: it was somewhat secretly negotiated from 1997 onwards; it finally was publicly acknowledged to exist in May 2001; and was ready for signing in September 2001. Canada signed the treaty with thirty other countries on November 23, 2001. The criticism of the *Cyber-crime Treaty* is that: a) it is not a measured response to real law enforcement problems; and b) it has left open to the signatories the ability to set legal standards for the interception of private communications instead of specifying minimum standards in the body of the treaty.[107] Therefore it is open to the Canadian government to introduce implementing legislation for the treaty that will set a lower legal standard (balancing of privacy and law enforcement rights) for interception than is the case with comparable technologies.[108] This implementing legislation is then passed to amend present Canadian criminal and other laws to accord with the Convention on *Cyber-crime*. This process presently is underway.

"LAWFUL ACCESS" PROPOSAL

The Department of Justice with Industry Canada and the Solicitor General led a debate regarding the implementation of the data interception requirements under the *Cyber-crime Convention* under the rubric of a "Lawful Access – Consultation" (Lawful Access Proposal).[109] The Canadian government claims that the Lawful Access Proposal pre-dated and was not a reaction to the events of September 11, unlike the above anti-terrorism legislation.[110] It is acknowledged by the government, however, that interception of private communications provides law enforcement with

---

[104] In *Eastmond, supra,* the Court held that law enforcement officials must demonstrate that surveillance is necessary to meet a specific need; is likely to be effective in meeting that need; is proportional to the anticipated benefit; and is the least privacy-invasive way to meet that need. The Privacy Commissioner of Canada and others have suggested that the same test apply during consultations about the federal government's *Lawful Access* proposal.

[105] Council of Europe, Committee of Ministers, 109th, *Convention on Cyber-crime*, ETS No. 185. (2001). Online: < http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>.

[106] In the context of the *Cyber-crime Convention*, this means: Search and seizure of stored computer data (Article 19); Real-time collection of traffic data (Article 20); and Interception of content data (Article 21).

[107] In addition, the potential for unauthorized access (hacking via legislated intercept "back doors") raise grave concerns for the privacy rights of consumers of communications technology, further elevating the need for our own and other governments to exercise caution when considering changes to the law in this area.

[108] For example, the CRTC has recently received submissions from the Canadian Association of Chiefs of Police (CACP) for a technological interception capability to be built into VoIP protocols. Nevertheless, these submissions have not committed to maintaining the same legal regime and standard for interception of VoIP calls as already exists for circuit-switched calls, despite their functional equivalence. See CRTC *Public Notice 2004-2 - Regulatory framework for voice communication services using Internet Protocol* (full submissions of all parties available online at: <http://www.crtc.gc.ca/PartVII/eng/2004/8663/c12_200402892.htm>. PIAC opposed this CACP submission in its own submissions, absent a clear commitment from law enforcement to maintain an identical standard for interception of VoIP calls as for circuit-switched calls.

[109] Canada, Dept. of Justice et al., Lawful Access: Consultation Document (Ottawa: Justice, 2002), online: < http://www.canada.justice.gc.ca/en/cons/la_al/>.

[110] Canada, Department of Justice, *Lawful Access FAQ*, online: Department of Justice Canada http://www.canada.justice.gc.ca/en/cons/la_al/summary/faq.html (*Lawful Access FAQ*).

"an essential tool for the investigation of threats to national security."[111] The term "lawful access", when used in this sense is somewhat ambiguous, in that it includes the present legal standard for "the lawful interception of communications and the lawful search and seizure of information, including computer data" -- a power already provided for in Canadian law, but which "can only be used with legal authority, i.e. a warrant or an authorization to intercept private communications, issued by a judge under specific circumstances."[112] However, the lawful access proposal includes a different legal interception standard.

The government's Lawful Access Proposal introduces three key changes to Canadian law that would interfere with their private electronic communications or Internet use. First, the proposal creates a *general production order* that would obligate third parties who have information about individuals to gather and provide that information on request, without the particular consent of the individuals in question. Second, it creates a *specific production order* to gather data about Internet traffic data generally and to gather information about particular Internet subscribers and service providers' data traffic in particular. Third, it creates *data preservation orders* to compel service providers to retain and act as custodians of information about particular subscribers or activities.[113] Such measures would appear to run counter to existing privacy and *Charter* rights protections.[114]. The government justifies them in the as matters of convenience;[115] "less intrusive than a search warrant;"[116] that these communications are worthy of "a lower standard" of privacy protection "in light of the lower expectation of privacy in a telephone number or Internet address;"[117] "a stopgap measure;"[118] and permissible because "a person does not have a reasonable expectation of privacy in personal information that does not tend to reveal intimate details of his or her lifestyle or personal choices."[119]

By introducing the *Lawful Access Proposal*, the government promised to maintain the *status quo* regarding the standards for obtaining "lawful authority" to intercept private communications. Yet the proposal clearly introduces changes to both the means and the standards under which law enforcement agents may access private communications, including consumer records, their e-mail, and Internet records. It makes a number of assumptions that could be characterized as self-serving: First, the definition of "traffic data" is wide and fails to take into account the reality that new information and communications technology dramatically increases the amount and utility of "data traffic" information available to authorities. Traffic data recorded during Internet use, for example, includes particulars of how people use the Internet: what websites they visit and what information they access there, and for how long.[120] This is the stuff of profiling.

---

[111] *Ibid*.

[112] *Ibid*.

[113] This is also known as the issue of "data retention". The European Union has permitted its member nations to have their own local laws on how long companies with Internet and other electronic "traffic data" can be forced to hold onto this data in the event that it is requested by law enforcement. Most of the data retention periods are well beyond that dictated by normal business practice or data retention requirements of privacy and access laws. For an excellent resource on the issue and its implementation in Europe see Electronic Privacy Information Center, "EPIC International Data Retention Page", online: <http://www.epic.org/privacy/intl/data_retention.html>.

[114] Public Interest Advocacy Centre, *Comments on the Federal Government's "Lawful Access" Consultation Document* (16 December 2002), on file with the Public Interest Advocacy Centre. Public Interest Advocacy Centre [Public Interest Advocacy Centre, *Comments on "Lawful Access"*].

[115] *Lawful Access FAQ, supra,* "For practical reasons, the third-party custodian of the documents is often in a better position to produce the documents." (*Ibid*., "General production orders".)

[116] *Ibid*.

[117] *Ibid*., "Specific production orders".

[118] *Ibid*., "Data-preservation orders".

[119] *Ibid*., "Orders to obtain subscriber and/or service provider information".

[120] For an excellent illustration of the problems with the definition of "traffic data" adopted in the *Lawful Access* proposal, see Jason Young, "Digital Traffic Cops: Recommendation for the Canadian Cybercrime Initiative" online: <http://www.anonequity.org/files/cfp2004_jyoung.pdf> at 5-6.

Second, the *Lawful Access Proposal* assumes consumers have a diminished expectation of privacy in new electronic communications technologies. The POLLARA Inc. survey instead shows 86% of Canadians do not think the government should be able to read their e-mail or monitor their web surfing habits without a warrant. This indicates a clear expectation of privacy in Internet communications equal to that for present wireline telephone conversations, contradicting the statement in the *Lawful Access Proposal* that "these communications are worthy of "a lower standard" of privacy protection "in light of the lower expectation of privacy in a telephone number or Internet address".

Third, the *Lawful Access Proposal* also proposes placing the cost of building interception capability of new communications technologies on Internet service providers and possibly on telephone companies offering Voice over Internet Protocol (VoIP) calling.[121] Such intercept capability has been required to be funded by business since 1994 in the United States under the *Communications Assistance to Law Enforcement Act* (CALEA). Anecdotal evidence suggests that these costs will in turn be passed onto consumers, either through increased prices, or that the companies will seek government subsidies or government-approved charges, which will either be indirectly paid from tax revenues, or directly paid as a subscriber charge mandated by the telecom regulator (in Canada the CRTC).[122] Finally, as many diverse commentators in the Lawful Access consultations pointed out, the government has failed to provide empirical evidence of the need to create the invasive, costly, and potentially dangerous "surveillance network" that it is proposing.[123]

Recent developments in the U.S. threaten to further erode or deny individuals' right to privacy when using communications technology. First, regarding e-mail interception, the recent judgment of the U.S. First Circuit Court of Appeals in *United States* v. *Councilman*, No. 03-1382 (29 June 2004), held that wiretap laws do not apply to e-mail service providers who monitor the content of users' incoming messages without their consent. The First Circuit Court of Appeals has agreed to a re-hearing *en banc* of the Councilman decision on the application of several U.S. privacy rights groups on the basis that its effect would be far-reaching and that it essentially ignores the tradition of expectation of privacy in electronic communications in the U.S. Second, the *USA PATRIOT Act* expanded state powers to permit state agents to monitor electronic communications and Internet use.[124] State officials in the U.S. can also obtain "open ended" wiretap warrants without having to specify whose communications will be intercepted for the purpose of furthering an investigation. Third, the FCC has launched a Notice of Proposed Rulemaking to bring all Internet communications under *CALEA*, effectively requiring all ISPs to

---

[121] See Comments of the Canadian Association of Chiefs of Police on CRTC Public Notice PN 2004-2 (VoIP), online: http://www.crtc.gc.ca/PartVII/eng/2004/8663/cac_police/040616.doc>.

[122] Public Interest Advocacy Centre, "Comments on the Federal Government's "Lawful Access" Consultation Document" (December 16, 2002). Online: < http://www.piac.ca/PIAC-Dec16-02.pdf>.

[123] Participants' comments are summarized online in the Government's full report on the Lawful Access proposal and consultation process: Department of Justice Canada <http://www.canada.justice.gc.ca/en/cons/la_al/summary>. One summarized submission notes: "7. The government has failed to present evidence that this massive surveillance infrastructure is necessary. For example, it is unknown how many investigations have actually been seriously hampered by lack of technical capability."

[124] *USA PATRIOT Act*, Public Law 107-56, § 216 and 217 [*USA PATRIOT Act*]. For more detail about how the investigative powers expanded by the *USA PATRIOT Act* may be used by U.S. authorities to obtain personal information, including entire databases of information about Canadians, see B.C. Outsourcing Report, reference *infra*; Canadian Internet Policy and Public Interest Clinic, *Submission on the USA Patriot Act and its impact on the privacy of B.C. citizens' personal information in the context of government outsourcing of data administration*, submitted to the British Columbia Privacy Commissioner (2 August 2004); and Michael Geist & Milana Homsi, *The Long Arm of the USA Patriot Act: A Threat to Canadian Privacy?*, Submission on the USA Patriot Act to the B.C. Information and Privacy Commissioner (July 2004).

make e-mail "monitorable" and other Internet-based communications technologies, such as VoIP, "interceptable."[125]

In Canada meanwhile, in light of the results of the POLLARA Inc. survey, it appears that the government has not provided compelling evidence to establish a lower standard for intercepting Internet and e-mail communications. Canadians do not have a diminished expectation of privacy in Internet and other electronic communications but instead a high expectation of such privacy. Finally, the *Lawful Access* proposal appears to conflict with existing common law, statutory and constitutional privacy expectations for interception of electronic private communications whatever their form.

National Identity Cards And Biometrics

National identity (ID) cards are one means of identifying individuals in society for national security and related purposes. However, there is a constant temptation in producing such cards to add biometrics technology to the cards to make them more accurate, less likely to be forged and to generally authenticate an individual. Therefore, although national ID cards need not use biometrics and biometrics need not be used with identity documents, privacy issues with both tend to be confounded and are best dealt with together.

NATIONAL ID CARDS

The rationale for implementing national ID cards includes not only combating terrorism but reducing identity theft, fraud, abuse of public services, and illegal immigration and employment. Aside from human error and the virtual impossibility of securing the massive databases needed to record and store biometric registries of this scale, opponents say that regardless of what type of card a government chose to implement, an ID card system will cost a fortune, yet fail to do what it promises. ID cards will not significantly improve security or reduce illegal working, immigration, identity theft,[126] or other forms of fraud.[127] It is unclear exactly how a national ID card would target terrorists.

In Canada, then Citizenship and Immigration Minister Denis Coderre promoted plans for a national ID card in 2002 and submitted them for consideration by a House of Commons Committee.[128] Interim Privacy Commissioner of Canada, Robert Marleau, cautioned Canadians about national ID card proposals: "it is highly unlikely that a national identification system could be developed without compulsory participation, serious inaccuracies, and significant disruptions and inconvenience to individuals."[129] In his view, the essential privacy problem with such cards is that

---

[125] See FCC Notice of Proposed Rulemaking, *Communications Assistance for Law Enforcement Act*, Federal Register / Vol. 69, No. 184 / Thursday, September 23, 2004 / Proposed Rules, p. 56976-7. Online: <http://www.cdt.org/digi_tele/20040923nprm.pdf>. [Summary of Notice of Proposed Rule Making, ET Docket No. 04–295, FCC 04–187, adopted August 4, 2004, and released August 9, 2004].

[126] See Submission to the House of Commons Standing Committee on Citizenship and Immigration, "Identity Theft as a Justification for a National Identity Card", Public Interest Advocacy Centre (November 4, 2003), online: < http://www.piac.ca/PIAC_ID_Card_Submissions.pdf>.

[127] For a helpful overview of these concerns, see United Kingdom, Information Commissioner, *Entitlement Cards and Identity Fraud: The Information Commissioner's Response to the Government's Consultation Paper*, Annex A, "Responses to specific questions raised in the consultation paper" (30 January 2003).

[128] Canada, House of Commons, Standing Committee on Citizenship and Immigration, "A National Identity Card for Canada?" News Release (7 October 2003); and Canada, House of Commons, Standing Committee on Citizenship and Immigration, "Deadline – National Identity Card for Canada" News Release (10 October 2003). Some suggest that such plans have since been scrapped (see *e.g.* Maria McClintock, "Grits fold on hi-tech ID card" *Ottawa Sun* (9 April 2004)). At the least, the plans seem to be in limbo.

[129] Canada, Office of the Privacy Commissioner, "Why We Should Resist a National ID Card for Canada," Submission to the Standing Committee on Citizenship and Immigration (18 September 2003), online:

they give government a direct window on our identities and personal lives. In effect, "they allow us to be identified when we have every right to remain anonymous, reveal more information about us than is strictly required to establish our identity or authorization in a particular situation, and allow our various activities to be linked together to form patterns and profiles of our lives."[130]

Making cards compulsory would require the creation of means to enforce policies and procedures for carrying, presenting, and failing to carry or present them. As well as introducing considerable expense, such a move could damage police-public relations and lead to an increase in identity theft and other criminal activity. It also raises further concerns about the likelihood that ID cards would undergo a form of "function creep." Function creep occurs when the original reasons and limited purpose or use for which a measure is created are gradually expanded. In the case of ID cards, this would mean that rather than only needing ID cards to cross borders, individuals would have to present their ID cards for a growing number of functions regulated by government or the private sector. Function creep would require anyone living in Canada to obtain and carry an ID card at all times. The result would be a form of permanent public surveillance.

In addition to "function creep," opponents point out that national ID cards will cost a between $3 and $5 billion[131] and be impractical[132] or even dangerous.[133] According to security expert Bruce Schneier, "a national ID card program will actually make us *less* secure."[134] In his view, what matters is not how a given security measure works, but "how it fails" or can be manipulated into failing and how its failures can be "exploited."[135]

Abroad, despite flagrant opposition from civil society groups and the Home Affairs Select Committee,[136] the U.K. has taken the lead in embracing the concept of a National ID Card. Parliament there introduced draft legislation that will require all individuals living or working there to obtain and carry national ID cards,[137] while the government in Scotland is running a pilot project using volunteers whose biometric information is recorded on "smartcards."[138] The U.S.

Office of the Privacy Commissioner of Canada <http://www.privcom.gc.ca/media/nr-c/2003/submission_nid_030918_e.asp>.

[130] *Ibid*.

[131] Privacy Commissioner Robert Marleau estimated that simply creating a national ID card system would cost between three and five billion dollars, not to mention the "substantial additional ongoing costs" involved in operating such a system. ("Why We Should Resist a National ID Card for Canada", *supra*).

[132] Some critics argue that because national ID cards are prone to errors (as are all forms of technology), involve considerable cost and inconvenience, and must be mandatory in order to be effective, they would not be significantly more reliable than existing forms of identification; see *e.g.* American Civil Liberties Union, "National ID Cards: 5 Reasons Why They Should Be Rejected" (8 September 2003), online: American Civil Liberties Union <http://www.aclu.org/Privacy/Privacy.cfm?ID=13501&c=39>.

[133] Identity cards are also criticized as impractical because they are at least as likely to contribute to identity theft as they are to reduce its occurrence: "The higher the 'integrity' (reliability and accuracy) of a card, the greater is its value to criminals and illegal immigrants. A high-value card attracts substantially larger investment in corruption and counterfeit activity. The equation is simple: higher value ID equals greater criminal activity" (Privacy International, Submission to the Citizenship and Immigration Committee of the Canadian Parliament (4 October 2003), online: Privacy International <http://www.privacyinternational.org/issues/idcard/pi-can-submission-10-03.htm>).

[134] "National ID Cards" *Crypto-Gram Newsletter* (15 April 2004), online: Crypto-Gram <http://www.schneier.com/crypto-gram-0404.html> [emphasis added].

[135] *Ibid*.

[136] See *e.g.* Lucy Sherriff, "ID cards: a bad idea, but we'll do it anyway" *The Register* (30 July 2004).

[137] United Kingdom, Home Office, *Draft Identity Cards Bill*, online: Home Office <http://www.homeoffice.gov.uk/docs3/draft_idbill2604.pdf>.

[138] Lucy Sherriff, "Biometric ID card trial kicks off in Glasgow" *The Register* (21 May 2004), online: The Register <http://www.theregister.co.uk/2004/05/21/biometric_trial_glasgow>. See also British Broadcasting Corporation (BBC), "ID cards: an iCan briefing", online: BBC <http://www.bbc.co.uk/dna/ican/A2319176>.

government also faces considerable public opposition to national ID cards, but has passed a law requiring biometric data in foreign visitor identification documents by October 2004, in order to dovetail with the US VISIT requirements of biometrically-based travel documents.[139] To comply, Canadians seeking to obtain or renew passports or drivers' licences must provide biometric information to the public or private sector agents that issue such documents.

BIOMETRICS

For the most part, police around the world have achieved high rates of success using fingerprints – a form of biometric data – to identify and arrest persons suspected of criminal activity. Yet, even on this limited scale, human and database errors involving biometric data can and do result in mistaken identities. Such errors damage the lives and reputations of individuals who are wrongly accused, detained, imprisoned, and/or threatened with deportation for offences they did not commit; such mistakes also lead to civil lawsuits.[140] The risk of errors and serious implications rises exponentially when we expand the scale on which we use biometric data, including iris scans, fingerprints, facial recognition, etc. In short, the trouble with biometrics is that they "won't identify anyone," instead allowing one only to draw "a strong link between a person and a previously established identity."[141]

By using biometrics and creating a national ID card, "we will be creating a potentially powerful infrastructure" that could easily be adapted to meet much broader objectives and make ID cards much more invasive than originally planned.[142] Although current uses of biometric technology and proposals for a national ID card registry may be for limited purposes, what is to stop police and other government agents or even corporations from demanding to see our biometric identification in the future? Even if an ID card is introduced as a "voluntary" measure, it is likely to "become a *de facto* universal card" in time.[143] Other *de facto* avenues to compulsory use of biometric data are already underway, in keeping with Canada's international obligations and in particular the promises our government made in its *Smart Border Declaration* and *Action Plan* with the U.S.[144]

CANADIANS' ATTITUDES TO NATIONAL ID CARDS

Despite demonstrated privacy risks and considerable costs, Canadians generally support the idea of a national ID card. The POLLARA Inc. survey indicates that 61% of Canadians think the government should require the carrying of a national ID card (only 34% were opposed). At the least, this result shows that there is a serious disjunction between Canadian public perception of

---

[139] *Enhanced Border Security and Visa Entry Reform Act of 2002*, 8 U.S.C. § 302.

[140] See *e.g.* John Lettice, "DHS and UK ID card biometric vendor in false ID lawsuit" *The Register* (11 May 2004), online: The Register < http://www.theregister.co.uk/2004/05/11/identix_false_id_suit>; Benjamin Weiser, "Can Prints Lie? Yes, Man Finds to His Dismay" *The New York Times* (31 May 2004); "The FBI Messes Up" *The New York Times* (26 may 2004); and "Apology is not Enough," Editorial, *The Washington Post* (27 May 2004).

[141] David Heath, "Secure identity in the Big Bad World" *Sydney Morning Herald* (14 April 2004). Online: http://www.smh.com.au/articles/2004/04/13/1081621954002.html

[142] United Kingdom, Information Commissioner, *Entitlement Cards and Identity Fraud: The Information Commissioner's Response to the Government's Consultation Paper* (30 January 2003) at 2.

[143] Colin J. Bennett, "Pick a Card: Surveillance, Smart Identification and the Structure of Advanced Industrial States," Paper presented to the 1997 Canadian Political Science Association Annual Meeting, St. John's, Newfoundland, 8 June 1997) at 13.

[144] See *e.g.* Jim Bronskill, "Canada to introduce biometric passport despite privacy concerns" *canada.com News* (18 July 2004), online: canada.com <http://cnews.canoe.ca/CNEWS/Canada/2004/07/18/548057-cp.html>; and Paul Bobier, "U.S. seeking your biometrics from Ottawa and the provinces" *The CCPA Monitor* 11:2 (June 2004) 19.

national ID cards and privacy advocates' concerns with them. This pattern is repeated with biometrics in U.S. survey research, which indicates 69% of Americans are "open to the concept of biometrics for identity management" with 19% uncertain and only 12% opposed.[145] Of those surveyed in U.S. research favouring biometrics, 88% cited "convenience" as the reason (that is, the avoidance of passwords and other authentication schemes).[146]

This survey research indicates that consumers want the convenience that ID cards and biometrics promise. However, the POLLARA Inc. survey also indicates that consumers wish to retain their personal privacy, even if state security is at issue. 59% stated "No" to the question: "To ensure Canada's national security, are you willing to give up some of your personal privacy?" Only 29% said yes. This indicates that consumers are of a dual mindset: as citizens they see no problem in increasing efficiencies and "doing their part" in national security efforts, even by self-identifying.[147] However, as consumers and individuals, they want privacy in their dealings with the government, in terms of concrete interactions like surveillance and government information holdings. It appears consumers and citizens have grasped the convenience argument behind a national ID card, yet not realized the surveillance possibilities of a single identity card that is required for all meaningful life transactions.

Although the Canadian government's proposal to implement a national ID card stalled when put to the House of Commons for consideration in 2002, it appears possible that it could be resurrected politically, especially in light of national security and terrorism concerns. However, if that debate occurs, government should better inform citizens about the possible ramifications of such a card in terms of data gathering and retention, the likelihood of biometrics being added to a card and the implications of that, the true costs, and the true balance of convenience versus cost to perceived privacy of the complete identification system such an approach would create. The government should also clearly indicate if the private sector could use a national ID card or biometric technology for identification – thus avoiding the uncertainty and industry abuses of the present legal status of the Social Insurance Number.[148]

Closed Circuit Television And Video Surveillance

Video surveillance is an obvious candidate for counter-terrorism measures. However, the resistance to public monitoring by video camera or closed-circuit television (CCTV) has slowed its introduction in Canada and elsewhere in the world. However, this reluctance to embrace video surveillance and CCTV is already under relentless pressure to cede to the goals of counter-terrorism and national security.

CSIS already has authority to conduct surveillance of terrorist suspects or persons who may be a "threat to the security of Canada".[149] This power to conduct surveillance of possible terrorists or spies relates to investigation of individual person, however, and does not extend to general surveillance. However, the RCMP and other police forces are implicated if the investigations of espionage or terrorism "have criminal implications". The RCMP or other forces may also investigate a "terrorism offence" as that phrase now is defined in s. 2 of the *Criminal Code* (added by the *Anti-terrorism Act)*.

---

145 See USA Today, "Steal your face: The dangers of identity theft", November 11, 2004, reporting on an "Identity Management Survey" by the Ponemon Institute. Online: <http://www.usatoday.com/tech/columnist/ericjsinrod/2004-11-10-sinrod_x.htm>.

146 *Ibid.*

147 It may also indicate that consumers are hazy on details of how personal privacy can be compromised by devices like national ID cards and biometrics and the implications of combining biometrics and national ID cards.

148 On the issue of SIN "function creep" see P. Lawson and J. Lawford "Identity Theft: The Need for Better Consumer Protection", PIAC, November 2003. Online: http://www.piac.ca/IDTHEFT.pdf

149 See the *CSIS Act*, s. 2(a),(b),(c) and (d).

Under the *Criminal Code*, Canadian police can obtain permission from judges to use electronic surveillance technologies in particular investigations, if judges find that the police have reasonable and probable grounds to believe that an offence has been or will be committed and that they will obtain information about that offence by using the technology in question.[150] The *Criminal Code* does not, however, expressly regulate general video surveillance. The Criminal Code does not expressly permit the widespread use of surveillance cameras to watch individuals without evidence of particularized suspicion. Neither, however, does it expressly prohibit it. Neither does the federal *Privacy Act*. Indeed, "neither statute prohibits the RCMP's use of general video surveillance that is not continuously recorded the RCMP" according to a legal opinion by the former Supreme Court Justice Gérard La Forest commissioned by the Privacy Commissioner of Canada.[151] However, general video surveillance of the populace, according to this opinion, likely would violate s. 8 of the *Charter*. As such, it may be subject to challenge as well under the *Criminal Code* and the *Privacy Act*.[152]

The legal status of closed circuit television (CCTV) surveillance by the private sector – which allows observers to watch individuals and monitor their activities without recording them – is subject to the *PIPEDA* (and comparable legislation in the territories and provinces) and is a violation of PIPEDA. The very first OPCC decision, #1, involved the monitoring of a public street in Yellowknife by a private security company. The Privacy Commissioner ruled this was not permitted, stating "There is no place in our society for unauthorized surveillance of public places by private sector organizations for commercial reasons".

However, the Privacy Commissioner made a point in OPCC decision #1 to address the issue of state monitoring of public places:

> "There may be instances where it is appropriate for public places to be monitored for public safety reasons. But this must be limited to instances where there is a demonstrable need. It must be done only by lawful public authorities and it must be done only in ways that incorporate all privacy safeguards set out by law."[153] [Emphasis added].

It is not clear from the reasons what "public safety" might encompass, but it likely is the prevention of street crime. It is also unclear if this would include prevention of national security threats or tracking of suspected terrorists.

In 2000, video cameras were installed in Kelowna, B.C. by the RCMP for monitoring a public area. The Privacy Commissioner of Canada, on the complaint of the B.C. Information and Privacy Commissioner under the federal *Privacy Act*, released a "finding letter"[154] that the surveillance of public places by the RCMP without a demonstrable need violated the rights of privacy of Kelowna residents:

> This type of wholesale monitoring or recording certainly runs afoul of the requirement to collect only the minimum amount of personal information required for the intended purpose. Moreover, the broad mandate to prevent or deter crime clearly does not give

---

[150] R.S.C. 1985, c. C-46, s. 487.01.

[151] See OPCC, Opinion by Justice Gérard La Forest, April 5, 2002, re: Video Surveillance, <http://www.privcom.gc.ca/media/nr-c/opinion_020410_e.asp>.

[152] The *Privacy Act*, s. 7 lists the RCMP as a "government institution" covered by the *Act* and s. 3 defines "personal information" protected by the *Act* as "information about an identifiable individual that is recorded in any form" – terms which arguably include video recordings but not unrecorded video surveillance such as CCTV.

[153] See OPCC, PIPED Act Case Summary #1, "Video surveillance activities in a public place", Online: <http://www.privcom.gc.ca/cf-dc/cf-dc_010615_e.asp>.

[154] See OPCC, News Release, "Privacy Commissioner releases finding on video surveillance by RCMP in Kelowna", Ottawa, October 4, 2001. Online: < http://www.privcom.gc.ca/media/nr-c/02_05_b_011004_e.asp>.

> police authorities unlimited power to violate the rights of Canadians. They cannot, for instance, compile detailed dossiers on citizens "just in case." They cannot force people at random to identify themselves on the street. They cannot enter and search homes at will, without proper authorization.
>
> It is equally clear, in my view, that police forces cannot invoke crime prevention or deterrence to justify monitoring and recording on film the activities of large numbers of the general public.
>
> In the normal course of law enforcement, cause (reasonable grounds) is a basic pre-condition for the collection and retention of personal information. In the case of video surveillance, information is recorded regardless of the existence of specific cause. By recording continuously, as opposed to recording only selective incidents related to law enforcement activities, the RCMP was unnecessarily collecting information on thousands of innocent citizens engaged in activities irrelevant to the mandate of the RCMP.

However, the RCMP did not abide by the ruling, citing jurisdictional constraints on the OPCC. During this controversy, the Privacy Commissioner commissioned the La Forest Opinion and others. The Privacy Commissioner then attempted to bring an action in a B.C. court to the effect that the cameras were illegal. However, the court sided with the RCMP that the Commissioner lacked jurisdiction to complain about the cameras. An appeal was abandoned by the OPCC.

The legal debate, therefore, has not conclusively determined that video surveillance of the general public could or should be justified on the basis of state security concerns. While there is a sense that Canada would find general public surveillance for general law enforcement would not be justified, that also is not perfectly clear after the Kelowna debacle.

Police forces in Canada nonetheless have investigated the idea of the use video surveillance and CCTV technology to continuously monitor and/or record the public's daily activities for crime prevention purposes.[155],[156] The question now becomes if the police will bolster their largely unsuccessful arguments to now argue that this general public surveillance will deter not only criminal activity but also assist in national security efforts.

Critics and privacy advocates oppose widespread public surveillance as unduly invasive and a grave violation of our democratic right to freedom; they also point out that it is ultimately ineffective or even counter-productive in reducing criminal activity. The Office of the Information and Privacy Commissioner of Alberta also undertook a literature review that summarized the use of CCTV technology,[157] especially in the United Kingdom, and determined that it the research generally concludes that while surveillance can sometimes assist police, its effectiveness has been overstated.[158]

A key problem with surveillance technology is that its results, at least in relation to crime deterrence, do not justify its potential to "annihilate" Canadians' reasonable expectation of privacy.[159] Research conducted independent of police forces suggests that in the long term

---

[155] Toronto Police Services Board investigated such a public monitoring system in 2002, but dropped the idea due to public outcry. See "Police Defer spy camera plans" Eye Weekly, April 4, 2002. Online: < http://www.eye.net/eye/issue/issue_04.04.02/news/cops.html>.

[156] This initiative did, however, garner some support in strange quarters. See, for example, brief of the Toronto Police Accountability Coalition "Brief on Video Surveillance" January 2002. Online: < http://www.tpac.ca/issues/video.htm>.

[157] Stephen Greenhalgh, "Literature Review on Issues of Privacy and Surveillance Affecting Social Behaviour", for the Office of the Information and Privacy Commissioner of Alberta, August 2003. Online: <http://www.oipc.ab.ca/ims/client/upload/LitReview.pdf>.

[158] *Ibid*.

[159] *R. v. Wong*, [1990] 1 S.C.R. 30 at 47.

cameras do not significantly reduce crime.[160] Instead, cameras "change the way we behave and make us more homogeneous,"[161] and prompt us to avoid public places where we know that we are likely to be watched.

Recently, Jennifer Stoddart, the present Privacy Commissioner of Canada, sought to dispel the legal uncertainty and undertook to provide guidelines on video monitoring/CCTV of the public. These guidelines were described in her 2003-4 Report to Parliament at p. 15:

> Shortly after taking office, the current Commissioner decided on an enhanced approach to this issue, and developed guidelines for the use of video surveillance by public authorities. These guidelines set out principles for evaluating the necessity of resorting to video surveillance and for ensuring that, if it is conducted, it is done so in a way that minimizes the impact on privacy. So, for example, video surveillance should only be a response to a real and pressing problem, where less-privacy invasive methods will not suffice; video surveillance systems should be designed to have the least possible impact on privacy, running for limited periods and avoiding capturing images of areas such as office or apartment interiors where people have an even greater expectation of privacy.

Would general surveillance for the purposes of counter-terrorism be that different from surveillance for crime prevention? Would it be equally ineffective? There is no data on this question although cameras have been installed in some U.S. cities, such as much of New York City, wholly or partly for terrorist watching and deterrence.[162] Certainly the presence of public monitoring for whatever reason would destroy a reasonable expectation of privacy. The question then becomes whether terrorism is such a scourge that the scourge of surveillance would be a lesser evil.

Studies also show that the people who monitor surveillance cameras are often bombarded with too much information and tend to rely on stereotypical characteristics to identify "suspicious" individuals and activity.[163] When it comes to searching out suspected terrorists, the possibility of officials relying on stereotypes and preconceived ideas about who might or might not be a terrorist raises serious concerns about Canada's commitment to openness, diversity, and protecting our individual rights and liberties, given that "one can scarcely imagine a state activity more dangerous to individual privacy than electronic surveillance."[164]

Certainly Canadians want notice of public surveillance. In the POLLARA study, the question: "Should the current law that requires the public to be informed about video surveillance monitoring of public places be enforced?" 78% said yes, and only 19% no. "The law" referred to in the question as requiring notice is the ensemble of the Privacy Commissioner of Canada's guidelines and findings on public surveillance, which make clear that notice of surveillance is a preliminary hurdle to meet in justifying any form of "general" (i.e., not individual investigatory) surveillance).[165] It may be doubtful that such "enforcement" of the principle could take place without a change to PIPEDA.

---

[160] Stephen Greenhalgh, "Literature Review on Issues of Privacy and Surveillance Affecting Social Behaviour", *supra*.

[161] *Ibid*. at 13.

[162] See Surveillance Camera Players, "Nothing has changed" online: < http://www.notbored.org/change.html> The SCP website provides maps of surveillance cameras in NYC.

[163] Stephen Greenhalgh, "Literature Review on Issues of Privacy and Surveillance Affecting Social Behaviour", *supra*.

[164] *R. v. Duarte*, [1990] 3 S.C.R. 36 at 43-44.

[165] See, for example, OPCC Decision #273 (employment context); the *Eastman* decision (in which the company did inform employees of the surveillance), the Kelowna complaint and Commissioner's filings and the OPCC finding #1, which found that without knowledge and consent, the private surveillance of the public violated PIPEDA. It is impossible to obtain consent for surveillance of a public place without

Canada is at a cross-roads regarding surveillance and national security. There is legal uncertainty over the requirements of public surveillance that could be exploited to introduce general surveillance for counter-terrorism purposes. Whether this is justified or not, Canadians intent on holding our government accountable for respecting our right to privacy deserve notice of public surveillance and at least some defensible evidence that the "annihilation" of a reasonable expectation of privacy by surveillance is justified in terms of catching criminal, terrorists, or defending the state.

---

at least a prominently posted notice. The question could also have been worded "Should there be a law requiring notice of public surveillance?".

MARKETPLACE AND BUSINESS-DRIVEN THREATS TO PRIVACY

In addition to initiatives of government, there are several national security developments relevant to business that directly impact consumer privacy. Business is increasingly cooperating with government in national security efforts or building databases of personal information in the guise of "customer information" which are extremely useful to government security forces and which are access targets. The latest Privacy Commissioner of Canada Report to Parliament stated:

> Another matter of concern to our Office, privacy advocates and commissioners is access by law enforcement and national security agencies to personal information collected by private sector organizations. Many people object to the private sector collecting information about them specifically because they worry about it finding its way into governmental hands.
>
> There can be times when this collection is legitimate, but without controls and oversight, it can tip over into what is in effect deputizing private sector organizations as law enforcement agents, and commandeering personal information that they have collected from individuals for entirely different reasons, in violation of the most basic fair information practices. [Emphasis added.]

Canadian businesses are indeed poised to become "agents of the state" in collecting, using and disclosing personal information to government for national security purposes. This fundamentally changes the relationship of consumers and business and risks consumer disenchantment and backlash. The two major innovations that allow business to "help" with national security efforts are data mining of customer databases and radio-frequency identification.

Radio Frequency Identification (RFID)

Radio Frequency Identification (RFID) is a form of technology aimed at identifying objects, animals, and people. An RFID "chip" or "tag" includes an antenna and sends information when activated by a device designed to "read" RFID signals. RFID chips can be affixed to clothing, documents, and other objects, packaging, and transportation materials. They can also be implanted under the skin or secured around the limbs or necks of people or animals.[166] In other words, RFID technology makes it possible "for everything to be essentially monitored all the time."[167]

Industry proponents and observers suggest that RFID technology is "highly accurate – 99.8%"[168] and can perform functions from keeping an eye on senior citizens[169] and locating children[170] to

---

[166] Though distinct from biometrics data, the implanting of RFID chips beneath a person's skin forms a singular identifier analogous to a fingerprint or an iris scan. This raises a host of concerns over individuals' privacy rights, the possibility of technological error or failure, and identity theft or fraud involving RFID technology. Regrettably, an in-depth exploration of these issues is beyond the scope of this report.

[167] Katherine Albrecht, quoted in Lynn Moore, "You're just a number: New technology is tracking you in ways that may be a surprise" *The Montreal Gazette* (20 June 2004).

[168] "Hot Topics in the Mobile Computing Industry" (Thornhill, ON: MobileInfo.com, 2001), online: MobileInfo.com <http://www.mobileinfo.com/Hot_Topics/RFID.htm>.

[169] Celeste Biever, "RFID chips watch Grandma brush teeth" *New Scientist* (17 March 2004), online: New Scientist <http://www.newscientist.com/news/print.jsp?id=ns99994788>.

[170] See *e.g.* Jo Best, "Schoolchildren to be RFID-chipped" *silicon.com* (8 July 2004), online: CNET Networks, Inc. <http://networks.silicon.com/lans/039024663,39122042,00.htm>; and "Kidspotters in LEGOLAND!," Announcement, online: LEGOLAND <http://www.lego.com/legoland/billund/whatsNew/default.asp?locale=2057>.

tracing the origins of infected livestock,[171] reducing theft,[172] and monitoring consumer spending habits.[173] Its supporters liken RFID chips to "a super sized version of the familiar bar code data collection technology"[174] or "bar codes on steroids."[175] In the U.S., the Defense Department and Agriculture Secretary have endorsed the use of RFID technology on manufactured goods and livestock.[176] Libraries use RFID tags to track their materials.[177] Retailers, including two of the world's five largest retailers, Wal-Mart Stores Inc. and Germany's Metro AG, require their suppliers to attach RFID chips to their manufactured goods and transportation materials.[178]

In Canada, provincial privacy commissioners have warned retailers not to violate laws aimed at protecting consumer privacy by using RFID technology to track consumer activity and spending patterns.[179] At a more fundamental level, concerns around RFID technology "are vitally important because they are representative of a larger trend… the seemingly inexorable drift toward a surveillance society."[180]

In addition to the private sector's use of RFID to track the movement and activity of goods, livestock, and people, several countries are considering RFID in relation to their national security

---

[171] Bob Brewin, "Industry and government have plans for nationwide cattle ID system, but funding is lacking" *Computerworld* (29 December 2003), online: Computerworld <http://www.computerworld.com/mobiletopics/mobile/story/0,10801,88625,00.html>.

[172] "RFID May Reduce Electricity Theft" *News* (20 August 2002), online: RFID Journal <http://www.rfidjournal.com/article/articleview/56/1/1>.

[173] Mark Baard, "Lawmakers Alarmed by RFID Spying" *Wired News* (26 February 2004), online: Wired <http://www.wired.com/news/privacy/0,1848,62433,00.html?tw=rss.POL>.

[174] Lindsay Bruce, "RFID becomes a reality" *IT World Canada* (12 March 2004), online: IT World Canada <http://www.itworldcanada.com/Pages/Docbase/ViewArticle.aspx?ID=idgml-c5dbd7d6-b5c2-4b03-8835-5d0c7025d00b>.

[175] Steve Hall, cited in Chris Conrath, "RFID slowly makes headway" *ComputerWorld Canada* (6 February 2004), online: IT World Canada <http://www.itworldcanada.com/Pages/Docbase/ViewArticle.aspx?ID=idgml-e835f0b5-ff21-4ad0-be6b-cae2310dfcf7>. See also Ann Bednarz & Denise Dubie, "RFID helps improve asset visibility" *Network World* (18 July 2003), online: IT World Canada <http://www.itworldcanada.com/Pages/Docbase/ViewArticle.aspx?ID=idgml-e18414c2-385f-4d4d-8fed-a53a4b0188ab>.

[176] Ann Bednarz, "Defense Department goes on offence with RFID" *Network World* (3 November 2003), online: Network World Fusion <http://www.nwfusion.com/news/2003/1103forresterside.html>; and Bob Brewin, "Agriculture secretary backs livestock ID system" *Computerworld (U.S.)* (7 January 2004), online: Computerworld <http://www.computerworld.com/mobiletopics/mobile/technology/story/0,10801,88729,00.html>.

[177] See *e.g.* "Vernon Installs First RFID System in Georgia," News Release (10 June 2003), online: Vernon Library <http://www.vernlib.com/rfidpressrelease1.asp>; and Susan Hildreth, "No reason to fear privacy invasion from library books" *San Francisco Chronicle* (6 May 2004).

[178] Grant Gross, "RFID and privacy: Debate heating up in Washington" *IDG News Service* (28 May 2004), online: Network World Fusion <http://www.nwfusion.com/news/2004/0528rfidpriv.html>; and John Blau, "Germany's Metro plans huge RFID deployment" *IDG News Service* (14 January 2004), online: International Data Group <http://www.idg.com.sg/idgwww.nsf/0/EEFD2AEF7E8CF1D648256E1B000C5D3A?OpenDocument>.

[179] Alberta Office of the Information and Privacy Commissioner, News Release, "Commissioner urges businesses to consider privacy obligations before implementing RFID technology" (April 5, 2004), online: http://www.oipc.ab.ca/ims/client/upload/RFID_NewsRelease_Mar2004.pdf . See also "Tag, You're It: Privacy Implications of Radio Frequency Identification (RFID) Technology" (Toronto: Information and Privacy Commissioner of Ontario, 2004) at 20-22, online: <http://www.ipc.on.ca/docs/rfid.pdf>).

[180] Director of the Technology and Liberty Project of the American Civil Liberties Union, Barry Steinhardt, made this point in his *Statement on RFID Tags Before the Commerce, Trade and Consumer Protection Subcommittee of the House of Representatives Committee on Energy and Commerce* (14 July 2004). Online: < http://www.statewatch.org/news/2004/jul/ACLU-Barry-Steinhardt-RFIDs.pdf >.

plans. For example, the U.S. is considering requiring RFID in passports domestically[181] and from those required to present biometric passports under the US VISIT program.[182] Although the state governments of Utah and California are currently considering legislation to restrict private sector use of the technology in particular,[183] neither Canada nor the U.S. has passed federal legislation that expressly addresses RFID technology. However, the use of RFID technology in Canada may be subject to the privacy protections set out in *PIPEDA,* the *Privacy Act*, or in comparable provincial and territorial privacy laws.

Opponents of RFID technology say that RFID allows corporations and governments to "spy on" individuals, often without their knowledge or consent. Since each RFID tag has a unique identifier and can be read at a distance, corporations, governments or even terrorists – anyone with the appropriate "reader" device – could theoretically track individuals in whose clothing, shoes or under whose skin an RFID chip is implanted. For those concerned with civil liberties and privacy rights, "the problem here is that RFID tags can be read through your wallet, handbag, or clothing" and "could enable an omnipresent police surveillance state" and "erode further what's left of consumer privacy"; it could also "make identity theft even easier than it has already become."[184] Civil libertarians are also concerned about the potential for governments to forego the implementation of national identity card programs by using RFID technology in passports or other identification documents, creating a *de facto* "*global* identity document."[185]

For these reasons, it is essential that governments clearly regulate and set limits on the use of RFID technology. At minimum, unauthorized use of RFID technology – that is, without the consent and awareness of those directly affected by it – must be prohibited and subject to penalty.

Data Mining And Data Aggregation

Corporations and governments in Canada and the U.S. currently maintain extensive databases and use technology to "mine" data – including personal information[186] – about individuals. The term "data mining" has many uses and interpretations.[187] To study how government agencies use it as "a technique for extracting knowledge from large volumes of data," the U.S. General Accounting Office (GAO) consulted industry publications and representatives to develop an operational definition of data mining as "the application of database technology and techniques –

---

[181] See Ryan Singel, "American Passports to Get Chipped" WIRED News, October 21, 2004. Online: http://www.wired.com/news/print/0,1294,65412,00.html.

[182] See "Fact Sheet: U.S. – Canada Land Borders". Online: http://www.dhs.gov/interweb/assetlibrary/US-VISIT_Canada_Fact_Sheet-English.pdf.

[183] See U.S., H.B. 251, *Radio Frequency Identification – Right to Know Act*, 2004, Gen. Sess., Utah, 2004; and U.S., S.B. 1834, *An Act to add Chapter 22.7(commencing with Section 22650) to Division 8 of the Business and Professions Code, relating to business*, 2004, Reg. Sess., 2004. See also Mark Baard, "Lawmakers Alarmed by RFID Spying" *Wired News* (26 February 2004), online: Wired <http://www.wired.com/news/privacy/0,1848,62433,00.html?tw=rss.POL>.

[184] Simson L. Garfinkel, "The Trouble with RFID" *The Nation* (3 February 2004), online: < http://www.thenation.com/docprint.mhtml?i=20040216&s=garfinkel>.

[185] Steinhardt, *supra.* He also notes that "Already, deliberations are underway to encourage governments to include RFID chips in the passport carried by citizens of every nation including the United States."

[186] This can include records of an individual's financial, employment, educational, business, travel, driving, criminal, immigration, and other information.

[187] Data mining can be used to detect and reduce fraud, waste, and abuse; manage human resources; detect criminal activity and patterns; and analyze intelligence information and detect terrorist activity (United States, General Accounting Office, *Data Mining: Federal Efforts Cover a Wide Range of Uses* (Report to the Ranking Minority Member, Subcommittee on Financial Management, the Budget, and International Security, Committee on Governmental Affairs, U.S. Senate) (Washington: United States General Accounting Office, 2004) at 2. (GAO Datamining Report).

such as statistical analysis and modeling – to uncover hidden patterns and subtle relationships in data and to infer rules that allow for the prediction of future results."[188]

Data mining is a growth industry that plays a significant role in national security agendas around the world.[189] Using existing information and surveillance technology, corporations and governments can track our everyday activities. They can also aggregate data, accessing personally identifiable information about individuals from different sources and compiling it into "profiles" or examining it for patterns, for instance. Data aggregators can then store and distribute that information; each replication or transmission multiplies the potential for unauthorized access or to introduce errors or inaccuracies.

The U.S. has long been a user and proponent of data mining technology at various levels of government.[190] Yet, in response to public outcry, it stopped funding the Terrorism Information Awareness program in 2003.[191] Aimed at establishing "a vast surveillance database to track terror suspects," the project alarmed privacy advocates and members of the public concerned about the government's ability to "generate a comprehensive data profile on any U.S. citizen" by allowing government agents to access personal information collected by the private sector, including credit card transactions and other financial information; electronic mail; medical, employment, and telephone records; and travel plans. The Department of Defence is no longer supposed to mine data using personal information about U.S. citizens. However, the Department is authorized to continue mining data about non-citizens in its military and intelligence operations outside the U.S.

Data mining and aggregation raise serious concerns over privacy rights and the creation of a global surveillance culture. When governments can access information from multiple databases – some of which may be inaccurate, outdated, or otherwise subject to information privacy protections[192] – state agents can target individuals for differential treatment.[193] In practical terms, bypassing the "inherent inefficiency of government agencies analyzing paper, rather than aggregated, computer records" eliminates the privacy protection that bureaucratic inefficiency offers.[194] Realizing that we no longer enjoy this limited form of privacy can add to a climate in which "knowledge that the government can collect the data trails that we unknowingly leave behind us every day is as, or more, likely to chill individual behaviour as direct, real-time government surveillance."[195]

---

[188] *Ibid*. at 1. In simpler terms, the U.S. Technology and Privacy Advisory Committee (TAPAC) in its Safeguarding Privacy in the Fight Against Terrorism Report of March 2004 (TAPAC Report), at p. viii defined "data mining" as "searches of one or more electronic databases of information concerning U.S. persons, by or on behalf of an agency or employee of the government." Online: <http://www.sainc.com/tapac/TAPAC_Report_Final_5-10-04.pdf>.

[189] This is especially true of the U.S., where the GAO Data Mining Report, at 4 characterizes "data mining and related technologies" as "key tools in Department of Homeland Security initiatives."

[190] See GAO Datamining Report.

[191] *Department of Defense Appropriations Act, 2004*, Pub. L. No. 108-84 (25 September 2003), § 8131. The program was initially introduced under the name "Total Information Awareness" but was later changed (TAPAC Report, *supra*, at p. vii).

[192] See TAPAC Report at 36: "Data aggregation creates the risk that the resulting profile provides the government with substitutes for information it is otherwise not allowed to access or act upon."

[193] For example, an individual identified by data aggregation technology might be singled out when they travel and apply for jobs or services. These "life chances" can be significantly affected by the "social sorting" made possible by data aggregation and datamining. See David Lyon, "Terrorism and Surveillance: Security, Freedom, and Justice After September 11, 2001" Paper given at the Privacy Lecture Series <http://privacy.openflows.org> on November 12, 2001. Online: <http://privacy.openflows.org/pdf/lyon_paper.pdf>.

[194] TAPAC Report, supra, at p. 6. See also at 36: "Data mining can… diminish informational privacy by eliminating the practical obscurity that currently results from data being difficult to locate and access."

[195] *Ibid*. at 36.

Other concerns about data mining include the potential for inaccurate information that is publicly available via the Internet or stored in government or corporate databases to be mined and compiled into "profiles" of individuals about whom governments have no reasonable cause to be suspicious; the possibility of individuals' personal information being accessed, used or misused, modified, or disclosed without their consent, without appropriate authorization, or for purposes other than those for which it was originally obtained; the denial of individuals' right to know how, when, and for what reason information about them is being collected, distributed, and used; and their right to access that information and request any necessary corrections.[196] The U.S. Technology and Privacy Advisory Committee warns that data mining and especially data aggregation threaten not only individual privacy rights, but also civil society as a whole.[197] These risks are multiplied when we consider the real possibility of mined data being outdated or inaccurate and the further possibility of human error and practical difficulties creating integrating and relying on large volumes of data.[198] In this way, the threats posed by using aggregated data extend beyond privacy to jeopardize our constitutional rights, including *Charter* rights to freedom of expression, religion, and association.

"Corporate Spying" on Canadians

Canadians may be under the impression that most of the abusive data mining (to produce profiles of identifiable individuals) is prohibited either by the *Privacy Act* (in relation to mining government databases) or *PIPEDA* (regarding private sector databases). However, neither of these acts is really of any use in halting this process, and indeed, PIPEDA now explicitly allows it.

The *Public Safety Act, 2002* amendment (s. 98) to PIPEDA allows not only the collection and disclosure of personal information by private industry (either at the behest of government or on their own initiative) to the government for national security purposes, but also allows companies to "use" it for these purposes.[199] Datamining is quite simply data processing. It seems quite clearly a "use" of the data under PIPEDA. Therefore this amendment has given companies, either at the urging of government, or simply on their own "good corporate citizen" initiative, the right, if not the duty, to apply any data mining technique to their entire personal information holdings. It quite simply allows profiling of Canadians for national security purposes from private sector information holdings and the provision of these profiles to the government.[200] In effect, the government now has access to massive personal information holdings of business that it can mine and that it does not have to pay to maintain or to search.

Regarding the possible data mining efforts of the Canadian federal government, the Privacy Commissioner of Canada has acknowledged that the *Privacy Act* is badly out of date and in need of amendment. The *Privacy Act* does not directly address the "use" of data question. Effectively, it would be a difficult argument that the *Privacy Act* in and of itself controls government data mining or that it prohibits use of information obtained from business that had been data mined. Add to this the data sharing allowed under the *Customs Act* in relation to API/PNR data (and note that the *Privacy Act* does not apply to information sent by airlines to U.S. authorities that returns to the Canadian government from the U.S. government[201]) and there is no effective mechanism

---

[196] *Ibid*. See also Organization for Economic Co-operation and Development (OECD), *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Paris: OECD, 1980).

[197] TAPAC Report, *supra*, at 36: "The risk of chilling individuals' behavior is especially great when the government is aggregating data from across our lives."

[198] *Ibid*. at 37-39 provides an instructive list of practical problems associated with data integration and individual identification when using data mining and aggregation technology.

[199] See Appendix C for the text of the *Public Safety Act, 2002* amendment affecting PIPEDA.

[200] Geist & Homsi, *supra* at 24-25 suggest that given CSIS's role in redrafting *PIPEDA*, this exemption *may also apply to U.S. and other foreign investigative agencies.*

[201] See s. 4.83(2) of the *Aeronautics Act*, as amended by s. 6 of the *Public Safety Act, 2002*.

for controlling Canadian government data mining efforts and the realization of individual profiles for national security purposes.[202]

It is questionable as well whether our privacy laws protect individuals in Canada from data mining and aggregation performed by non-Canadian agencies and corporations, as permitted by existing U.S. law. Under present mutual legal assistance treaties, it may be possible for this foreign data mining profile information to be transferred to the Canadian government from a foreign government that accessed it under its own national security laws.

A majority of Canadian consumers do not want the government to have the power to create profiles on them by obtaining their consumer information in the name of "national security". The POLLARA Inc. poll indicated that 56% said "No" to the question: "If the government thinks you are a security threat, should the government be permitted to monitor your purchasing habits, without a warrant?" Forty-one per cent, however, indicated the government should have this power. When it comes to business taking it upon themselves on their own initiative to "flag" customers as national security threats, the response was 57% "No" and 39% "Yes". Canadians do not want profiling. They do not want either government or private sector data mining.

And yet the amendments to PIPEDA allow just this profiling and information sharing. The amendments effectively make businesses "agents of the state" and fundamentally change the consumer-business relationship. This could lead to a serious loss of consumer confidence.

In the B.C. Outsourcing Report, Commissioner Loukidelis said this about data mining in general and in Canada specifically:

> A recent audit by the US Government Accountability Office has studied the extent of data mining by US federal agencies. It confirmed that this practice is increasingly common and that many of the data mining efforts involve the use of personal information. *The extent of data mining by governments in Canada has not been the subject of sufficient or transparent study and documentation and, in our view, since the privacy implications of data mining can be significant, this needs to be remedied.* [Emphasis added.][203]

Commissioner Loukidelis went on to make two recommendations in regard to data mining by the B.C. government, but indicated the Canadian government also should consider them. First, he recommended the government of British Columbia should undertake "a comprehensive and independent audit of data mining efforts by all public bodies" and second, that the B.C. government "use the audit to identify and describe operational and planned data mining activities, including in each case: the kinds of personal information involved, the purposes of the data mining, and the authority and conditions for doing so" and make the audit public.[204]

Given that "national security" now is permitted under Canadian federal privacy laws, and that Canadians are not in accord with the principle of data mining, we recommend that the audit at the federal level start with a study of data mining in relation to national security efforts.

Business should commit to not voluntarily providing information to the government for national security purposes, even though they have the legal ability to do so. They should await a warrant. They should advise their customers of this policy. And they should never voluntarily mine their customer data for "suspicious" profiles to provide to national security forces.

---

202 Note that the *Anti-terrorism Act* made clear that information collected under the authority of the following Acts is in the "Exempt Personal Information Bank Order, No. 25 (RCMP)" category: *Criminal Code*, the *Security of Information Act*, the *Security Offences Act*, the *Royal Canadian Mounted Police Act* and the *Canadian Security Intelligence Service Act*. See the *Privacy Act*, s. 18, as amended by the *Anti-terrorism Act*, s. 40.

203 B.C. Outsourcing Report, p. 14.

204 B.C. Outsourcing Report, p. 20.

CONCLUSIONS AND RECOMMENDATIONS

Canada's National Security Policy tells us that "[t]he world is a dangerous place, even if the relative safety of life in Canada sometimes obscures just how dangerous it is." Ontario's Information and Privacy Commissioner Ann Cavoukian dismisses "anonymity" – including our freedom not to give governments and corporations access to information about ourselves or our activities – as "a thing of the past."[205] How do people in Canada view privacy in our "new reality" of "national security" and "public safety"?

Conclusions

Canadians, it seems, want both security and personal privacy. Perhaps they are right: that more can be done by all parties to balance the tension between privacy and state security. However, there may be areas that are not possible to balance, where tough decisions will have to be made.

The polling results clearly show this seeming contradiction: Canadians will assist in efforts to aid authorities with national security but do not see why this must change the legal regime for access to their personal information. They trust government and business but react poorly when confronted with concrete examples of present balancing of privacy and security. Finally, they appear to want to keep national security at home, and not go as far as compromising their personal privacy to aid other nations, specifically the U.S., in their national security efforts.

The law, including both *Charter* rights and the more recent privacy legislation such as PIPEDA, appears to be of little help in balancing privacy rights and state security issues. Short of a constitutional amendment,[206] it is unlikely that the courts will impose any serious restrictions on state security measures that trim privacy rights. In addition, where statutory privacy rights would appear to be inconvenient, the track record thus far has shown Parliament is willing to amend those inconveniences right out of the privacy debate – despite the opposition of various Privacy Commissioners.

This report demonstrates that privacy issues are rarely considered alongside the development of new security laws, policies, and procedures. Issues, such as the outsourcing and USA PATRIOT Act controversy in B.C. only come about when one party holds its ground and demands an answer. This after-the-fact method of balancing does not appear to do much more than polarize the population and require decision-makers in government to choose between privacy and security (and usually the decision is for increased security). A more open discussion is required, with an emphasis on accountability of decision-makers.

Recommendations

There is scope for improvement in the balancing of privacy and state security in Canada. The following recommendations are grouped by issue and occasionally made with reference to specific legislation. This report calls on government and business to make changes and consumers and citizens to hold them to account.

---

[205] "Tag, You're It: Privacy Implications of Radio Frequency Identification (RFID) Technology" (Toronto: Information and Privacy Commissioner of Ontario, 2004) at 1 (online: http://www.ipc.on.ca/docs/rfid.pdf accessed September 28, 2004).

[206] Possible models for the enshrinement of privacy as a constitutional right are Article 8 of the *European Convention on Human Rights* and Article 7 and 8 of the *Charter of Fundamental Rights of the European Union*.

For Government and Business

The recommendations for government and business are contained in the following recommendations:

RECOMMENDATION 1 – OPCC PRIVACY REVIEWS OF PROPOSED LEGISLATION

That the Office of the Privacy Commissioner be asked for a privacy assessment of all new federal "national security" legislation in advance of its introduction in Parliament. This report should be tabled in Parliament. The OPCC's recommendations would not be binding, however, absent extreme circumstances, Parliament should await the report before voting through such legislation. The public and business should be invited to participate in OPCC reviews of national security legislation. A public education campaign should be undertaken by the OPCC based on these reviews.

RECOMMENDATION 2 – SUNSET CLAUSES

All "national security" amendments affecting privacy rights should be "temporary" in the sense of expiring on a set date unless justified by the government of the day in Parliament. These sunset clauses could be coordinated to come up for renewal simultaneously to coincide with an OPCC review and report to Parliament on the provisions. The results of these reports should be communicated effectively to the public.

RECOMMENDATION 3 – REPEAL "CORPORATE SPY" AMENDMENTS TO PIPEDA

The amendment to PIPEDA introduced in s. 98 of the *Public Safety Act, 2002* should be repealed. Business should commit to not providing person customer information for national security purposes either at the "request" of a "government institution" *without a warrant or other judicial or mandatory legislative authority* nor, especially of its own volition. Business has no business in spying on consumers absent a warrant or a clear law forcing disclosure.

RECOMMENDATION 4 – COSTS OF NATIONAL SECURITY - DIRECT TAXATION

All costs of national security measures should be borne by government and raised by taxes. Business should actively resist all government efforts to "download" national security costs to business.

RECOMMENDATION 5 – API/PNR – CLARITY AND LIMITS

Advance Passenger Information/Passenger Name Record Information collection, use and disclosure should be clarified under one statute, with an accountable department. Passengers should be clearly informed as to what information will be collected and why, in advance. The level of detail required in API/PNR should be restricted to the essentials necessary for terrorism investigations only. API/PNR information should not be used for criminal records checking or other law enforcement (or other) purposes.

RECOMMENDATION 6 – INTERCEPTION OF INTERNET COMMUNICATIONS WITH A WARRANT

The "Lawful Access" process underway should conclude that a warrant is required to intercept Canadians' Internet-based and other electronic communications, with a legal standard identical to that for interception of circuit-switched telephone calls. Business should keep electronic transaction information only as long as required by law and for appropriate business usage.

RECOMMENDATION 7 – SURVEILLANCE OF THE PUBLIC FOR NATIONAL SECURITY PURPOSES

Canada should clearly confirm in legislation that police and national security forces may not use general surveillance as a method of terrorist deterrence (or any other general crime prevention).

RECOMMENDATION 8 – NATIONAL ID CARDS & BIOMETRICS

The OPCC should conduct a thorough review of national ID cards and their effectiveness in reducing terrorism as well as the potential cost in terms of surveillance and profiling of citizens. A related study (perhaps combined with the National ID Card study) should focus on use of biometrics to enhance state security and document integrity. Both reports or a combined report should be presented to Parliament, and a public education campaign undertaken by the OPCC with government funding, prior to any legislation on the matter being passed by Parliament.

RECOMMENDATION 9 - RFID

Consumer consent should be required to sell RFID tagged merchandise or to require these devices in documents. The RFID chips should be deactivatable by the consumer, without penalty or lack of ability to access government services. A clear federal law on the use of RFID, in national security efforts and otherwise, is required. In the meantime, business should voluntarily adopt such guidelines and self-identify as being compliant with these fair information practices.

RECOMMENDATION 10 – AUDIT OF DATA MINING EFFORTS IN NAME OF NATIONAL SECURITY

That the federal government complete an audit of all federal data mining efforts, led by the OPCC, commencing with those data mining efforts in support of national security. This audit should extend to business cooperation with government in data mining efforts.

RECOMMENDATION 11 – OUTSOURCING AND USA PATRIOT ACT

That all data processing of Canadian personal information by U.S.-based or U.S. linked corporations be banned (at the provincial and the federal level) pending conclusion of a treaty or other agreement with the U.S. regarding privacy and security matters that adequately protects Canadian personal information from wholesale use by the U.S. for national security purposes. Business should voluntarily impose the ban as soon as practicable.

For Consumers

The recommendations of what consumer can do to reverse the trend towards reduced privacy in the name of national security are grouped by the themes of accountability, integrity and resistance.

First, consumers and citizens should insist on clear authority, adequately explained and justified, for national security-based reductions of consumer and personal privacy. Consumers should demand clear accounting for such measures. They should insist national security measures only be imposed by democratic institutions and any funds required to run these programs should be raised through taxes.

Consumers and citizens should be more proactive in guarding the integrity of their own personal privacy. This means informing themselves of both their privacy rights under PIPEDA and other privacy legislation and being aware of national security concerns and how the government is attempting to address these concerns, often curtailing privacy rights in the process.

Finally, consumers can take concrete measures to counter what they may see as excessive reduction of privacy rights. First, regarding government, consumers and citizens can speak out on privacy issues by writing their MPs, by commenting upon legislative proposals and by raising these issues in political meetings and pass judgment upon such issues in elections. Consumers can demand businesses they frequent do not "accommodate" government information requests in the name of national security. They can provide less personal information to business and use their rights under PIPEDA to see it is appropriately limited to only that necessary and destroyed promptly after the required business use. They can choose to travel in ways that are not as heavily monitored for information as air travel.

Most of all, however, consumers must be aware that their personal information and to some extent their personal lives are at risk in the vast shift to a security-based society. This awareness may lead them to seek appropriate shelter for and stronger (constitutional) protection for their personal information – so as not to have it become collateral damage in this "information war".

APPENDIX A: POLLARA INC. SURVEY – UNWEIGHTED FREQUENCIES

		Percentage	Frequency
Q1: To ensure Canada's national security, are you willing to give up some of your personal privacy?			
	Yes	31%	389
	No	58%	725
	Don't Know	11%	139
	Refused	1%	7
	TOTAL	100%	1260
Q2: Should the government be able to read your e-mail or monitor your Internet use without a warrant?			
	Yes	11%	141
	No	86%	1078
	Don't Know	3%	38
	Refused	0%	3
	TOTAL	100%	1260
Q3: If the government thinks you are a security threat, should the government be permitted to monitor your purchasing habits, without a warrant?			
	Yes	41%	516
	No	56%	701
	Don't Know	3%	39
	Refused	0%	4
	TOTAL	100%	1260
Q4: If a business thinks you are a security threat, should that business be permitted to report your purchasing behaviour to the government, without a warrant?			
	Yes	40%	506
	No	55%	696
	Don't Know	4%	54
	Refused	0%	4
	TOTAL	100%	1260

Q5: Should the current law that requires the public to be informed about video surveillance monitoring of public places be enforced?

	Yes	78%
985		
	No	18%
225		
	Don't Know	4%
47		
	Refused	0%
3		
	TOTAL	100%
1260		

Q6: Do you think the government should require everyone in Canada to carry a national identity card?

	Yes	62%
783		
	No	34%
426		
	Don't Know	4%
50		
	Refused	0%
1		
	TOTAL	100%
1260		

Q7: Are you aware that the government released Canada’s first National Security Policy this past April?

	Yes	22%
276		
	No	77%
964		
	Don't Know	2%
19		
	Refused	0%
1		
	TOTAL	100%
1260		

Q8: To what extent are you concerned about the Canadian government accessing and saving your personal information when you fly (within Canada or from Canada to another country) for up to seven years?

	Not Concerned At All	40%
506		
	Somewhat Concerned	36%
459		
	Very Concerned	22%
281		
	Don't Know	1%
13		
	Refused	0%
1		
	TOTAL	100%
1260		

Q9: To what extent are you concerned about the Canadian government sharing your flight information with other countries?

	Not Concerned At All	39%
491		
	Somewhat Concerned	27%
343		
	Very Concerned	32%
407		
	Don't Know	1%
17		
	Refused	0%
2		
	TOTAL	100%
1260		

Q10: To what extent are you concerned that U.S. firms receiving your personal information from Canadian companies may have to share it with the U.S. government under U.S. security laws?

	Not Concerned At All	25%
314		
	Somewhat Concerned	27%
336		
	Very Concerned	47%
590		
	Don't Know	1%
17		
	Refused	0%
3		
	TOTAL	100%
1260		
	Q11 AGE GROUP	
	18-24	11%
137		
	25-34	17%
209		
	35-44	22%
282		
	45-54	23%
285		
	55-64	15%
183		
	65+	12%
151		
	Refused	1%
13		
	TOTAL	100%
1260		
	Q12 PEOPLE IN HOUSEHOLD	
	1	18%
224		
	2	34%
424		
	3	18%
226		
	4	18%
226		
	5	8%
102		
	6+	3%
42		

	Refused	1%
16		
	TOTAL	100%
1260		
	Q13 HOW MANY ARE UNDER 10 YEARS OF AGE	
	None	74%
769		
	One	12%
124		
	Two	10%
101		
	Three	2%
21		
	Four Or More	1%
6		
	Refused	1%
15		
	TOTAL	100%
1036		
	Q14 HOW MANY BETWEEN 10-17 YEARS OF AGE	
	None	74%
770		
	One	14%
150		
	Two	8%
83		
	Three	1%
14		
	Four Or More	0%
4		
	Refused	1%
15		
	TOTAL	100%
1036		
	Q15 EDUCATION	
	Elementary School	5%
67		
	High School	33%
415		
	Community College	25%
315		
	University	25%
309		
	Post-Graduate/Professional	10%
132		
	Don't Know/Refused	2%
22		
	TOTAL	100%
1260		
	Q16 HOUSEHOLD INCOME	
	Less Than $25,000	13%
160		
	$25,000 to Less Than $50,000	24%
304		
	$50,000 to Less Than $75,000	19%
241		
	$75,000 And Over	22%
279		
	Don't Know/Refused	22%
276		
	TOTAL	100%
1260		

	Q17 GENDER	
	Male	49%
613		
	Female	51%
647		
	TOTAL	100%
1260		
	Q18 GENDERATION	
	Male - 18 To 34	14%
170		
	Male - 35 To 54	23%
281		
	Male - 55+	13%
156		
	Female - 18 To 34	14%
176		
	Female - 35 To 54	23%
286		
	Female - 55+	14%
178		
	TOTAL	100%
1247		
	Q19 REGION	
	Nova Scotia	8%
102		
	New Brunswick	7%
84		
	Prince Edward Island	1%
8		
	Newfoundland	4%
56		
	Montreal CMA	9%
117		
	Rest Of Quebec	10%
132		
	Toronto CMA	8%
107		
	Rest Of Ontario	12%
149		
	Manitoba	3%
44		
	Saskatchewan	4%
53		
	Alberta	13%
158		
	Vancouver CMA	10%
127		
	Rest Of BC	10%
123		
	TOTAL	100%
1260		
	Q20 REGION	
	Atlantic	20%
250		
	Quebec	20%
249		
	Ontario	20%
256		
	Prairies	20%
255		
	British Columbia	20%
250		

	TOTAL	100%
1260		
	Q21 LANGUAGE	
	English	82%
1030		
	French	18%
230		
	TOTAL	100%
1260		