National Identity Cards, Biometrics And the Consumer: Displacing the Personal from the Person

Written by Hasini Palihapitya
Research by Lisa Joly
Edited by John Lawford
Public Interest Advocacy Centre
1204 – ONE Nicholas St.
Ottawa, Ontario
K1N 7B7

February 2006

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

Palihapitiya, Hasini

National Identity Cards, Biometrics and the Consumer:
Displacing the Personal from the Person

ISBN 1-895-060-74-5

EXECUTIVE SUMMARY

As Canada continues to bolster national security post September 11th, and consumer commerce becomes increasingly jeopardized by identity theft, a National Identity Card scheme has been discussed as a potential solution. However, critics charge that National Identity Cards could turn into "de facto internal passports" which would be required to access almost all government or business services. Additionally, this new Card could lead to serious breaches to personal privacy. First, this report focuses on the security solutions offered by a National Identity Card, in terms of (a) National Security, (b) Identity Theft. Second, the privacy implications of a National Identity Card program will be identified, including a discussion of the effect of *The Personal Information Protection and Electronic Documents Act* (*PIPEDA*) in enabling infringement of personal privacy in the context of a National Identity Card scheme.

A National ID Card may likely be an inadequate solution to bolster national security because it fails to achieve the three broad goals set in Canada's *National Security Policy*. National Identity Cards would link names with faces, and possibly even with biometric data, but would not, on its own, identify those persons harboring malicious intentions. Additionally, National Identity Cards would likely not help to curb identity theft, as identity theft has many causes. Even those for which a National ID Card might directly apply, there are weaknesses and dangers in its use. This report examines the reasons behind these shortcoming in terms of (1) Easy Credit, (2) Consumer Control of Credit Bureau Files and (3) Function Creep.

A National Identity Card program will also face technological and practical shortcomings. (1) They will be prone to fraud and counterfeit, just like other forms of identification. (2) Specifying who will be issued a Card, and who will not, includes the potential for social exclusion. And, (3) because of serious concerns about its accuracy and reliability, biometric indicators may in fact make National Identity Cards less secure. Given the pitfalls associated with a National Identity Card program, consumers are justified to be concerned about fraud, the implications of misidentification, as well as the cost of implementation.

A National Identity Card will also involve a vast accumulation of consumer information, which is cause for concern from a privacy standpoint. The major privacy implications stem from function creep, the threat posed by use of collected information for purposes other than that for which it was originally collected. Further, protecting the databases holding personal information is not only costly, but difficult to assure. Finally, exceptions under *PIPEDA* permit information to be exchanged between and within government, as well as between businesses and government for the protection of national security.

This report concludes that the use of National Identity Cards, with or without biometrics, in interactions between individuals and the state or commercial entities, in a context of inadequate legal and technological safeguards, would introduce new ways of violating individual privacy and integrity. It would also be unacceptably costly given the expected, poor, results. However, should the Canadian federal government pursue the idea of a National Identity Card, recommendations have been supplied to reduce the risk of harm to consumers and citizens with respect to privacy and civil rights.

TABLE OF CONTENTS

INTRODUCTION

As Canada continues to bolster national security post September 11th, and consumer commerce becomes increasingly jeopardized by identity theft and other fraud, a National Identity Card scheme has been discussed. Such a card, with or without the use of biometrics, intends to make authentication of identity more certain. However, critics charge that National Identity Cards could turn into "internal passports" which would be required to access almost all government or business services. Furthermore, a National Identity Card scheme would produce vast quantities of information which, if collected by private industry and government, could be used for data-matching and secondary marketing (targeted to the individual and his or her spending or borrowing habits). Thus, the new Card would lead to serious breaches to personal privacy. This report will focus on the security solutions promised by National Identity Cards and biometrics and discuss their effectiveness in terms of limiting consumer and identity fraud. This report will also comment on the privacy risks inherent in such strategies.

This report is divided into two parts, and will answer the following questions:

1. Security Solutions:
    a. Will a National Identity Card benefit a society that is concerned about national security, and identity theft?
    b. What are the technological and practical shortcomings of such a system?
    c. What are consumer concerns arise as a result from a National Identity Card scheme?

2. Privacy Implications:
    a. What are the privacy implications of a National Identity Cards program?
    b. What effect does *PIPEDA* have in enabling infringement of personal privacy in the context of a National Identity Card scheme?

This report concludes that the use of National Identity Cards, with or without biometrics, in interactions between individuals and the state or commercial entities, in a context of inadequate legal and technological safeguards, would introduce new ways of violating individual privacy and integrity. It would also be unacceptably costly given the expected, poor, results. However, should the Canadian federal government pursue the idea of a National Identity Card, recommendations have been supplied to reduce the risk of harm to consumers and citizens with respect to privacy and civil rights.

National Identity Cards

National Identity Cards can be broadly defined as a nationwide, all purpose identification document.[1] It could be issued by either the federal, or provincial governments and could contain relevant personal information, such as name, address, date of birth, and perhaps even additional information relating to physical characteristics such as eye colour and height. They may also be designed to exploit Radio Frequency Identification (RFID) technology.[2] One of the main goals of introducing a National Identity Card is to replace multiple identification documents with one all encompassing piece of ID. Thus, National ID cards could be used in a number of different settings, ranging from border control and immigration, to authentication of a person's entitlements to government services. Furthermore, National ID cards could be used to replace other forms of identification, such as drivers' licenses and birth certificates, in commercial contexts. Yet, National ID Cards are qualitatively different than other forms of identification currently used. Some have argued that they may essentially become "internal passports".[3] However, it is important to note the government has not yet outlined specific design details, or issued a draft policy statement regarding the practical implementation of the card once it is introduced. Consequently, the present discussion is limited by the fact that a proposal has not yet been drafted for a National Identity Card.

Many countries in the world have already implemented National ID Card systems. Examples include Kenya, Jordan, and South Korea.[4] Although the scheme is not as popular among common law countries,[5] the U.K. and Australia

---

[1] CIPPIC, "National ID Cards, FAQs & Resources", online: http://www.cippic.ca/en/faqs-resources/national-id-cards/.

[2] Originally intended as a more functional replacement for bar codes in the retail sector, RFID chips (a type of low-end microchip) can store large amounts on information despite their minuscule size. There are a number of privacy and surveillance concerns associated with this technology that are relevant to their use in National Identity Cards. Refer to PIAC's RFID paper for a thorough analysis of technology and related privacy implications. George Hariton et al., "Radio Frequency Identification and Privacy: Shopping into Surveillance", Public Interest Advocacy Centre, February 2006.

[3] Richard Rosenberg, "National Identity Cards", Appearance before the Standing Committee on Citizenship and Immigration (Canada), February 19, 2003, online: http://www.cs.ubc.ca/~trevor/writings/NationalIDCard-presentation.pdf.

[4] For a survey of the National ID Documents in other countries, refer to Appendix B of the Interim Report issued by the House of Commons Standing Committee on Citizenship and Immigration. House of Commons, Canada, "A National Identity Card for Canada?" Interim Report of the Standing Committee on Citizenship and Immigration, Joe Fontana M.P., Chair, October 2003, [***Standing Committee Interim Report***], online: http://192.197.82.11/infocomdoc/Documents/37/2/parlbus/commbus/house/reports/cimmrp06/cimmrp06-e.pdf.

[5] As Peter Lilley, noted opponent of British Identity Cards, points out, "No common law country has ever introduced compulsory ID cards successfully in peacetime". Peter Lilley, MP, "Identity Crisis: The Case Against ID Cards", The Bow Group, 2005, [***Lilley, Identity Crisis***], at Chapter 5, online: http://www.bowgroup.org/harriercollectionitems/IDCards.pdf.

have discussed introducing a new form of national identification in recent years.[6] In fact, a National Identity Card program continues to progress through the U.K legislature. In May of 2005, the U.K. Identity Cards Bill was introduced to Parliament in the Queen's Speech,[7] and at the time this report was published, the House of Lords voted to support the proposed national identity card scheme, overturning several amendments.[8] If finally implemented, the first identity cards carrying unique biometric information will be issued in the U.K. in 2008.[9]

Domestically, Denis Coderre, former Minister of Citizenship and Immigration, proposed the possibility of creating a National Identity Card in November of 2002. Coderre cited terrorism and identity theft as pivotal concerns in the discourse on a "positive proof of identity". He further suggested that the House of Commons Standing Committee on Citizenship and Immigration (House Committee on Citizenship) study the matter.[10] The results of this investigation were published in an Interim Report entitled, "A National Identity Card for Canada?" in October of 2003, just before the second session of the 37th Parliament ended.[11] The issue was pushed aside during the third and final session of Parliament, which was dissolved in May of 2004, and remained dormant for some time.

As recently as mid-February 2006 the issue of National Identity Cards resurfaced when Stockwell Day, Minister of Public Safety, expressed interest in breathing new life in the project, or one similar to it.[12] Although it remains unclear what the present government intends to do on this front, there is mounting pressure from the international community to increase security of travel documents.[13] This logic

---

[6] A few common law countries have issued National Identity Cards, including: Singapore, Hong Kong, Malaysia and Cyprus.

[7] Compulsory identification cards have been issued in the U.K. in the past. ID cards were first issued during WWI, but abandoned in 1919, and later re-introduced during WWII (in 1939), but again abandoned in 1952.

[8] "UK Government Wins Narrow Majorities on ID Card Bill", Privacy International, February 14, 2006, online: http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-523776&als[theme]=National%20ID%20Cards.

[9] These cards will be issued to legal residents of the U.K.(of 3 or more months), including foreign nationals, who are over the age of 16. For more information see online: http://www.homeoffice.gov.uk/passports-and-immigration/id-cards/, and http://www.identitycards.gov.uk/

[10] News Release, "A National Identity Card for Canada", Standing Committee on Citizenship and Immigration, Ottawa: October 07, 2003.

[11] Standing Committee Interim Report, *supra* note 4.

[12] Canadian Press, "Day Proposes National ID Card", February 17, 2006, GlobeandMail.com, [***Cdn Press Article***] online: http://www.theglobeandmail.com/servlet/story/RTGAM.20060217.wstockwell0217/BNStory/National.

[13] Take, for example, the US Visit Program, which was announced in January of 2004. US Visit makes concrete the need for certain countries to have in place a biometrics program for travel documents in order to continue participation in the Visa Waiver program. This requirement took effect in October of 2004, and included 27 countries. Canada is exempt from these requirements. Canada is, however, involved in the US-Canada Smart Border program. Passport Canada, "Backgrounder: Biometrics in the International Travel Context", [***Passport Canada, Backgrounder***], online: http://www.pptc.gc.ca/newsroom/news20040201_e.asp.

seems to be at the heart of Day's interest in providing Canadians with a "smooth and quick access at all border points", both within North American and internationally.[14] Day agrees that there are many ways in which this goal may be achieved. Either a new form of identification could be issued, or technological enhancements of existing identification could be implemented, as is the case in the U.S.

The United States Congress recently passed the highly controversial Real ID Act in May of 2005, which will standardize state issued drivers' licenses to meet federal ID standards established by the Department of Homeland Security.[15] Significantly, the Real ID Act will require states to link their databases with one another, and eventually with Canada and Mexico.[16] There are, of course, numerous jurisdictional concerns that need to be addressed before the Act involves all three nations.[17] Many have argued that the sum of the required enhancements to existing identification will amount to an American National ID Card.[18] While it is possible that a similar program will be developed in Canada, especially in light of these recent developments in the US and rekindled interest in the topic, this report will treat National Identity Cards as separate and distinct from other government issued identification, such as provincially issued drivers' licenses.

---

[14] Cdn Press Article, *supra* note 12.

[15] Declan McCullagh, "FAQ: How Real ID Will Affect You", May 6, 2005, News.Com, [***McCullagh, Real ID FAQ***] online: http://news.com.com/2102-1028_3-5697111.html?tag=st.util.print.

[16] Privacy International, "Real ID Act Passes by Congress", May 11, 2005, online: http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-210373&als[theme]=ID%20Around%20the%20World.

[17] The American Association of Motor Vehicle Administrators (AAMVA) has completed a survey of 50 states and 9 Canadian provinces on implementation of Driver's License and Identification Card Reform. The American Association of Motor Vehicle Administrators (AAMVA), "Survey of the States on Implementation of Driver's License and Identification Card Reform", August 2005, [***AAMVA Survey***], online: http://www.epic.org/privacy/id-cards/aamva_survey_report.pdf.

[18] According to Barry Steinhardt, director of the American Civil Liberties Union's technology and liberty program, "[The Real ID Act] is going to result in everyone, from the 7-Eleven store to the bank and airlines, demanding to see the ID Card. They're going to scan it in… It's going to be not just a national ID card but a national database". McCullagh, Real ID FAQ, *supra* note 15. See too, for example, Dawn Kawamoto, "Driver's License or National ID Card?", (February 16, 2006), News.Com, online: http://news.com.com/Drivers+license+or+national+ID+card/2100-7348_3-6040655.html.

Biometrics

Biometrics is the use of biological properties such as fingerprints, iris scans, facial recognition to identify individuals. Biometrics has many public and private sector uses, [19] including applications in credit, debit and health cards, drivers' licenses, and voice identification in banking systems.

Former Minister of Citizenship and Immigration Denis Coderre placed biometrics at the centre of the debate over National Identity Cards in 2003 with the bold assertion that, "[t]he biometric train has left the station. We have to ask ourselves where do we want to sit on that train"?[20] His comments speak to the building reputation of biometric indicators in enhancing the security of identity documents.[21] However, there are many pitfalls in the technology, which is still immature.

However, the technology is gaining acceptance. Biometrics will likely be added to Canadian passports in the future.[22] Already, Canada is complying with recommendations of the International Civil Aviation Organization, the United Nations agency responsible for aviation issues, which stipulate that Canadians must port "neutral" expressions in their passport photos.[23] This measure is one step towards introducing standardized biometrics in airports around the world.[24]

There are three kinds of biometrics that are being explored for wide spread use in travel documents:[25]

1. **Fingerprints**: Fingerprints are the oldest and most widely recognized biometric.

---

[19] Examples in the U.S. include the use of finger geometry by Disney World with its season passes, and the introduction of a Smarttouch digital fingerprint system by VeriStar Corporation for optional use in fast food restaurants. Paul de Hert, "Biometrics: legal issues and implications", Background paper for the Institute of Prospective Technological Studies, DG JRC, European Commission (January 2005), [***de Hert***], online: http://cybersecurity.jrc.es/docs/LIBE%20Biometrics%20March%2005/LegalImplications_Paul_de_Hert.pdf

[20] Denis Coderre, Address to Forum on Biometrics: Applications and Implications for Citizenship and Immigration (Ottawa, Ontario) October 8, 2003.

[21] See also European Commission, Joint Research Centre, Institute for Prospective Technological Studies, "Biometrics at the Frontiers: Assessing the Impact on Society", EUR 21585 EN, European Communities, 2005, online: http://europa.eu.int/comm/justice_home/doc_centre/freetravel/doc/biometrics_eur21585_en.pdf

[22] The implementation date for this program has not yet been defined. See generally, Passport Canada Backgrounder, *supra* note 13.

[23] Shawn McCarthy, "No Smiling! We're Canadian", Globe and Mail, (August 27, 2003).

[24] *Ibid*.

[25] Passport Canada, "Biometrics: FAQ", online: http://www.pptc.gc.ca/faq/index_e.asp#700.

2. **Iris Scans**: Acquisition, analysis, and comparison of the unique details contained in the intricate patterns of the furrows and ridges of the iris are used in this form of identification. This information is captured in a manner similar to taking a normal photograph.

3. **Facial Recognition**: Distinctive features of the human face are captured and compared in order to perform the biometrics match. Again, this involves use of technology similar to photography.

Biometric systems not only measure and record biometric characteristics of a person, but match the obtained biometric data to a database containing additional information about the individual in question. There are two ways in which data may be 'matched' with an individual. In **one-to-one matching**, biometric data obtained by an on-the-spot scan is matched to only one sample stored in a database or card chip. Whereas, in **one-to-many matching**, biometric data obtained by the on-the-spot scanner is matched to a multitude of stored samples. The system then sorts though the data to find the right match, or the best match. However, the objective in both cases is to establish a connection between a person in real time with additional identification information, such as her stored biometric sample, name, membership number or SIN.

Canada already employs biometrics in its CANPASS Air Program, which enables pre-approved travelers to clear customs and immigration by simply looking into a camera that completes an iris scan as proof of identity.[26] One-to-one matching is employed in this program and participants must successfully pass a screening process to qualify.[27] Biometric indicators have also been discussed in relation to other, non-travel, forms of identification such as the "Maple Leaf" card for permanent Canadian residents.[28] By extension, it may also be added to National Identity Cards when the scheme is rolled out, and is thus relevant to our discussion of the issue.

Despite the excitement surrounding the potential uses and conveniences proposed by biometric identification, there are serious concerns about its accuracy. The reliability of biometric systems depends on a number of factors, including the scale of operation and the purpose of the system. It depends on what biometric identifier is used and whether more reliable one-to-one identification techniques are used, versus one-to-many identification, which produces more errors. A thorough discussion of this issue occurs later in this report.[29] Thus, it is sufficient to state at this point out that issues concerning its

---

[26] The CANPASS Air program is currently available at 7 Canadian airports including: Calgary International Airport, Pearson International Airport, Toronto, and Pierre Elliot Trudeau International Airport, Montreal. Canada Border Services Agency, "CANPASS Air Fact Sheet", July 2005, online: http://www.cbsa-asfc.gc.ca/newsroom/factsheets/2005/0419-e.html.

[27] *Ibid.*

[28] Standing Committee Interim Report, *supra* note 4 at pp. 4.

[29] Refer to "Technological and Practical Shortcomings", below.

accuracy and reliability plague the use of biometrics, and also raises many privacy issues that may outweigh the potential benefits of the technology.

PART A: SECURITY SOLUTIONS

There are many forces pushing Canada to bolster national security, and prevent identity theft. Meanwhile, innovative technologies continue to arise and offer novel means of addressing these harms. The debate over the adoption of a National Identity Card finds its footing firmly in this environment of technological determinism.[30] However the effectiveness of a National Identity Card scheme is yet to be established. It is necessary to identify the actual benefits and dangers to consumers and citizens elicited by introducing this new form of identification before the government proceeds to allocate significant amounts of the public purse to such an involved project. Specifically, consumers need to understand how a National Identity Card will address concerns about national security, identity theft, and fraud? What are the technological shortcomings of such a system? And, what are the implications for consumers stemming from a National Identity Card scheme? This portion of the report will answer these questions and demonstrate that a National Identity Card is likely an inadequate solution.

TWO PROBLEMS, ONE INADEQUATE SOLUTION

(1) National Security Post September 11

The 'war on terrorism', and the need to control the flow of people over borders, is often cited as the primary reason for the adoption of a National Identity Card with biometric technology.[31] Although a detailed analysis of the political and historical context motivating the push to bolster national security is beyond the scope of this report, it is accurate to note that both internal pressures from various branches of the Canadian government, as well as external pressures stemming from the international community, particularly the United States, have greatly influenced Canada's interest in introducing National Identity Cards.

---

[30] Technological Determinism is the belief that technology develops by its own laws, that it realizes its own potential, limited only by the material resources available, and must therefore be regarded as an autonomous system controlling and ultimately permeating all other subsystems of society. See Bruce Bimber, "Three Faces of Technological Determinism", in "Does Technology Drive History, edited by Merrit Roe Smith and Leo Marx, Cambridge, MA, MIT Press, 1994.

[31] Lilley, Identity Crisis, *supra* note 5.

Many legislative responses were initiated in the hopes of reinforcing Canada's national security following the events of September 11th.[32] Most importantly, A *National Security Policy* was introduced in April 2004 by the federal government,[33] which encompasses three broad goals: [34]

(1) Protection of the physical safety and security of Canadians at home and abroad;

(2) Securing Canada against use by terrorists as a base for threats to our allies; and

(3) Contribute to the development of a more effective international security system.[35]

The plan is "very much a Canadian approach", that tries to balance Canadian values,[36] safeguards and liberties while also acknowledging global realities.[37] It is also "a living document",[38] that provides space to generate new ideas and respond to changes in the threat environment. As previously mentioned, former Minister of Citizenship and Immigration Denis Coderre proposed a National Identity Card scheme in 2002, with the bulk of discussion on the matter occurring in 2003, before the National Security Policy was introduced. In light of these new developments, it is advisable to analyze the National Identity Card with respect to the goals enumerated above.

---

[32] Canada's "Anti-Terrorism Plan" was introduced in the months following 9-11 and included: *The Anti-Terrorism Act* (S.C. 2001, c.41), and the *Public Safety Act, 2002* (S.C. 2004, c.15), as well as amendments to other pieces of Canadian legislation. For a thorough discussion of the counter-terrorism legislative changes and their effect on consumer privacy, refer to PIAC's paper on the issue. John Lawford and Sharon Roberts, "Consumer Privacy and State Security: Losing our Balance", PIAC, November 2004 [***Consumer Privacy and State Security, PIAC***].

[33] This is Canada's first comprehensive statement on national security. 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.

[34] Speech delivered by The Honorable Anne McLellan, then Deputy Prime Minister and Minister of PSEPC, National Press Theatre, Ottawa, Ontario, "Securing an Open Society: Building a National Security Policy for Canada", April 27, 2004, [***McLellan Speech***] online: http://www.psepc-sppcc.gc.ca/media/sp/2004/sp20040407-en.asp.

[35] Canada's National Security Policy focused on six key areas, including: strengthening our intelligence gathering capabilities, developing a national emergency management system, creation of a Public Health Agency, reinforcing transportation security, enhancing border security and international dimensions. National Security Policy, *supra* note 33.

[36] The U.S. has repeatedly criticized Canada's emphasis on the protection of civil liberties to the apparent detriment of the war against terrorism. See "Nations Hospitable to Organized Crime and Terrorism", Oct 2003, U.S. Federal Research Division of the Library of Congress at 145, 147, online: http://www.loc.gov/rr/frd/pdf-files/Nats_Hospitable.pdf.

[37] McLellan Speech, *supra* note 34.

[38] *Ibid.*

Firstly, how will a National Identity Card serve to protect the physical safety and security of Canadians at home and abroad? Although introducing a National Identity Card may seem to be a magic bullet that would go far in achieving this goal, the reality falls far short of the ideal. Many critics have flatly argued that National ID Cards would be ineffective in protecting the nation from acts of terrorism. As Privacy International (PI) notes, "a link between identity cards and anti-terrorism is frequently suggested [but], the connection appears to be largely intuitive."[39] In fact, as PI argues, while the connection is often made through rhetoric, there is no evidence to suggest that stronger identity documentation would be an effective tool to counter terrorism.[40] The consensus among privacy advocates is that identity documentation is not an effective means of bolstering national security when considered against the staggering cost of implanting such a plan. Using this cost, benefit analysis implementing a National Identity Card program doesn't make logical sense.[41] As Bruce Schneier explains, [42]

> What good would it have been to know the names of Timothy McVeigh, the Unabomber, or the D.C. snipers before they were arrested? Palestinian suicide bombers generally have no history or terrorism. The goal here is to know someone's intentions, and their identity has very little to do with that.

National Identity Cards would link names with faces, and possibly even with biometric data, but they would not be able to prevent terrorism, either in Canada or elsewhere. Therefore, a National Identity Card program would likely fail to achieve the first objective and prove ineffective in protecting the physical safety and security of Canadians either at home or abroad.

Second, how will a National Identity Card secure Canada against use by terrorists as a base for threats to our allies? The world's experience with terrorism has demonstrated that it is almost impossible to catch a terrorist before the damage is done, despite sophisticated surveillance and top-secret intelligence. Take for example the July 7th 2005 bombings in London that targeted the public transport system during rush hour. The group of four men suspected of carrying out the devastating attack, which killed 56 people and injured over 700, were unknown to authorities prior to the bombing.[43] A National Identity Card would be ineffective in identifying terrorists before they commit acts

---

[39] Privacy International, "Mistaken Identity; Exploring the Relationship Between National Identity Cards & Prevention of Terrorism", April 2004, [***Privacy International, Mistaken Identity***] online: www.privacyinternational.org/issues/idcard/uk/id-terrorism.pdf.

[40] *Ibid*.

[41] For more discussion on the cost of implementing a National Identity Card in Canada, refer to "Consumer Concerns: Who's Going to Pay for this?", below.

[42] Bruce Schneier, "National Insecurity Cards", Posted May 11, 2005, Schneier.com, [***Schneier***] online: http://www.alternet.org/module/printversion/21977.

[43] BBC News, "7 July Bombings: London Attacks In Depth", online: http://news.bbc.co.uk/1/shared/spl/hi/uk/05/london_blasts/what_happened/html/default.stm

of terrorism. Rather, resources would be more effectively allocated to crime prevention strategies, and strengthening intelligence gathering capabilities.

Some reports have even gone so far as to argue that the adoption of a National ID Card would make the state more susceptible to acts of terrorism. As argued in the London School of Economics assessment of the British Identity Cards Bill: [44]

> The [British proposal] unnecessarily introduces, at a national level, a new tier of technological and organizational infrastructure that will carry associated risks of failure. A fully integrated national system of this complexity and importance will be technologically precarious and could itself become a target for attacks by terrorists or others.

Thus, a National Identity Card program may be ineffective in achieving the second goal of securing Canada against use by terrorists.

Third, how will a National Identity Card contribute to the development of a more effective international security system? As previously mentioned, National Identity Cards have been issued in numerous countries throughout the world, but many argue that they have done little to improve security either at the national or at the international level. Many countries in Europe currently employ National Identity Cards.[45] Examples include: Germany, Italy, Spain, and Poland.[46] Despite the popularity of implementing national identity cards, many critics warn that this trend should not be interpreted to mean that the cards are effective. For example, PI argues that the assumptions underlying endorsement of national identity card schemes are flawed. Indeed, target terrorists will apply for identity cards, and will be entitled to obtain them, and worst of all, will do so using their true identity.[47] As PI notes, "there is no known correlation between the extent of terrorism and the presence of an identity system".[48] As noted critic of National Identity Cards in the U.K., Peter Lilley, points out: [49]

> The worst terrorist atrocity in Europe – the Madrid bombing – was carried out in one of the few countries which make it compulsory to carry an ID card at all times. They likewise failed to stop the

---

[44] London School of Economics, "The Identity Project: an assessment of the UK Identity Cards Bill and its implications", 21 March 2005, [***LSE***], at pp.6 online: www.lse.ac.uk/collections/pressAndInformationOffice/PDF/IDreport.pdf .

[45] For a comprehensive review of many European Countries experiences with National Identity Cards, refer to the Interim Report of the Standing Committee on Citizenship and Immigration. Standing Committee Interim Report, *supra* note 4.

[46] Some critics of National ID cards have pointed out that some countries, such as Germany and Spain, introduced National ID cards under fascist regimes in the 1930s, and have not withdrawn them. Lilley, Identity Crisis, *supra* note 5, at Chapter 5.

[47] Privacy International, Mistaken Identity, *supra* note 39.

[48] *Ibid.*

[49] Lilley, Identity Crisis, *supra* note 5.

> bombings in Istanbul. And those who planned the 9/11 attacks chose to do so from Germany, which requires its citizens to have an ID card though not to carry it. […] The perpetrators of 9/11 then traveled to the USA under their true identities.

Despite the widespread use of National Identity Cards, terrorists continue to travel from country to country. Thus, a National Identity Card program may fail to achieve the third and final objective, and may not contribute to the development of a more effective international security system.

In sum, a National Identity Card program would likely be ineffective in reaching the objectives outlined in the National Security Policy. To reduce the reasons for this failure to one argument: identification aids very little in preventing or dealing with terrorism. Many have advised the government to invest the funds it would allocate to a National Identity Card program to funding other, proven manners of fighting crime, such as hiring additional security personnel, and high level intelligence gathering operations.

(2) Identity Theft and Fraud

Protection from identity theft is often listed as another benefit attributable to the implementation of a National Identity Card program. As Minister Denis Coderre suggested, "While the new focus on a positive proof of identity is partially rooted in the aftermath of the terrorist attacks, other forces are at play. Identity theft is seen as a serious and growing problem in Canada."[50] While it is indisputable that incidents of identity theft continue to rise, National Identity Cards may prove to be ineffective in addressing the problem.

Identity theft is the unauthorized collection and fraudulent use of someone else's personal information. Victims of identity theft regularly suffer financial loss, damaged reputations, and are left with the complicated and arduous task of clearing their name.[51] The most common purpose of identity theft is financial gain. Identity thieves typically use personally-identifying information of others, such as stolen Social Insurance Numbers, credit cards, debit cards and PINs, to open bank accounts, obtain loans, or run up utility, cell phone or other bills. Another reason for stealing personal information includes ruining the reputation of another person, starting a new life under a new identity, and avoiding criminal prosecution. Criminals of all kinds, including, but not limited to, terrorists, use

---

[50] Minister Coderre before House of Commons Standing Committee on Citizenship and Immigration, 6 February 2002.

[51] For a thorough discussion of Identity Theft from a consumer perspective, see PIAC's paper on the issue. Philippa Lawson & John Lawford, "Identity Theft: The Need for Better Consumer Protection", Public Interest Advocacy Centre, November 2003, [***PIAC, Identity Theft***], online: http://www.piac.ca/financial/identity_theft_the_need_for_better_consumer_protection/.

false identification to escape detection by law enforcement officials, both before and after committing crimes.[52]

Identity theft is financially burdensome to society. [53] In 2003, the latest year for which statistics are available, PhoneBusters National Call Centre recorded losses reported by victims at $21.6 million.[54] In addition to these financial losses, victims of identity theft are left with damaged credit ratings and disrupted personal and financial records. In a 2003 survey, the U.S. Federal Trade Commission reported that identity theft victims spent an average of $500 US to recover lost identities and clear credit ratings.[55]

Thus, it is indisputable that identity theft is worthy of concern, and that action should be taken to curb this harmful activity and protect consumers. However, additional identity documentation in the form of a National Identity Card is likely the wrong approach to achieve these ends. PIAC criticized use of National Identity Cards to curb identity theft in its November 2003 submission the House of Commons Standing Committee on Citizenship and Immigration. [56] These submissions noted there were several problems with relying upon a National Identity Card to combat identity theft. In fact, there is little evidence to prove that a National ID Card would appreciably limit identity theft in a manner that justifies the potential threat such a scheme poses to personal privacy.

PIAC completed an extensive report on identity theft in Canada with assistance from Industry Canada in 2003. The report concludes that there are eight main causes of identity theft in Canada:[57]

1. Pre-approved Credit offers and Credit Card "Cheques",
2. Easy Credit.
3. Electronic Access to Personal Information,
4. Sloppy Government and Business Information Practices,
5. Lack of consumer control of their credit bureau files,
6. Function Creep: Abuse of Social Insurance Numbers, Drivers' License numbers,
7. Weak ID theft laws and uncoordinated law enforcement,
8. Inadequate protection by privacy laws.

---

[52] PIAC, Identity Theft, *supra* note 51.

[53] Criminal Intelligence Service Canada, "2005 Annual Report on Organized Crime in Canada", at pp.28-30, "Identity Theft", [***CISC***] online: http://www.cisc.gc.ca/annual_reports/annualreport2005/document/annual_report_2005_e.pdf.

[54] PhoneBusters, "Statistics on Phone Fraud: Identity Theft Complaints", Canada, 2003, online: http://www.phonebusters.com/english/statistics_E03.html.

[55] CISC, *supra* note 53.

[56] Public Interest Advocacy Centre, "Identity Theft as a Justification for a National Identity Card", Submission to House of Commons Standing Committee on Citizenship and Immigration, [***PIAC Submissions***] November 4, 2003.

[57] PIAC, Identity Theft, *supra* note 51.

While all of these causes of identity theft can be tied back to the issue of improper identification to a certain extent, (2) Easy Credit, (5) Consumer Control of Credit Bureau Files, and (6) Function Creep, are the only causes that may be *directly* effected by a National Identity Card program. The following discussion will focus on these issues exclusively, and the likely failure of a National Identity Card program to reduce the concern in either domain.

Easy Credit

Credit is too easily obtained in today's marketplace. While checking photo ID is obviously a way of verifying a debtor's identity, the question remains, should a National ID card become the default form of identification used fur such a purpose?[58] If it were made mandatory to check National ID Cards to conduct financial transactions, financial institutions and business would keep records of ID checks. In so doing, they would amass a huge amount of National ID card information, which could potentially be linked to every financial transaction of that customer.

As PIAC argued strenuously in its Identity Theft Report, verification of individual identity should not involve the *collection* of additional personal information, but rather simple verification. The rationale is clear: the more personal information is recorded and retained, the more susceptible it is to abuse. In fact, a major factor in the phenomenon of ID theft is controlling electronic access to personal information. A National ID Card would do nothing to prevent such abuses,[59] while the value of obtaining the sensitive data they will contain makes them particularly vulnerable to abuse.[60] As PIAC argued before the Commons Standing Committee on Citizenship and Immigration:[61]

> [B]ased on past experience of function creep of key government identifiers and private credit information such as credit card numbers, [PIAC] finds it extremely unlikely that effective legislation could be enacted to forbid electronic storage or linking of National ID card information.

Finally, business could also create consumer profiles based on National ID Card information they compile and use it for marketing purposes, which is yet another potential breach of personal privacy.[62]

---

[58] Note that if financial institutions and creditors were required to check National ID Cards, legislation would have to be passed at both the federal and provincial level to make it mandatory.

[59] In situations where lenders do not actually check identification, having a National ID Card will not assist.

[60] Refer to "One Card, One Database: Increased Vulnerability", below.

[61] PIAC Submissions, *supra* note 56.

[62] Another concern stemming from business collecting this sort of information is what would happen to that information if the government were to ask for it? Under *PIPEDA* s.7.3(d)(ii)

Credit Bureau

Closely related to the concern of "Easy Credit" is the lack of control that consumers have over their credit bureau files. As mentioned, another way that identity theft occurs is through creation of fraudulent credit accounts, and stealing credit information. Credit information is regularly communicated to and from credit bureaus by credit grantors without the knowledge of the individual subject. Consumers have notoriously little control over their credit reports, but once identity thieves have gained access to open credit accounts, they are quickly victimized. Thus, credit bureaus stand at the cross roads of ID theft. As was argued before the Commons Standing Committee on Citizenship and Immigration, credit bureaus need to do more on behalf of consumers to combat identity theft.[63]

Although some credit bureaus have advocated for a National ID Card program, implementation of such a system does nothing to combat the actual problems with the present system. In fact, consumers may suffer if credit bureaus were to have access to even more personal information than they already have, and particularly the sensitive information contained on National Identity Cards. There are a number of measures which could counter ID theft, that would not require implementation of a National Identity Card program, and would better address the situation. For instance, credit "freezes" of a customer's credit file, notification of unusual patterns of credit applications, notification of significant inaccuracies in a credit file are just three suggestions. Credit bureaus could do more to help consumers catch identity theft at the outset and minimize the damage it causes.

Function Creep

The danger of function creep associated with a National Identity Card program is real and presents considerable concern from an identity theft perspective.[64] The reason for this is quite simple. A National Identity Card would sit on top of the hierarchical list of identity documents. It would, presumably, have multiple uses and would be demanded in multiple contexts, and would therefore become the most "powerful" form of identification. Consequently, it would also become an ideal target for identity thieves, and those wishing to do harm. Indeed, "a single

---

business could volunteer information if they are suspicious of wrongdoing related to a national security issue. Also see "Inadequate Privacy Legislation: *PIPEDA*", below.

[63] PIAC Submissions, *supra* note 56.

[64] Function creep is the term that has been given to the use of a unique identifier, often government-issued, for purposes other than those for which it was issued. Also refer to "Function Creep", below.

document that would provide supposedly definitive proof of identity could actually increase counterfeiting and identity theft".[65]

As a witness brought to the attention of the House of Commons Standing Committee on Citizenship and Immigration, a report issued by the United States National Research Council from 2002 states:[66]

> It is likely that the existence of a single, distinct source of identity would create a single point of failure that could facilitate identity theft. The theft or counterfeiting of an ID would allow an individual to "become" the person described in the card, in very strong terms, especially if the nationwide identity system were to be used for many purposes other than those required by the government… The economic incentive to counterfeit these cards could turn out to be much greater than the economic incentive to counterfeit U.S. currency.

This idea of a "single point of failure" is extremely problematic, both from the consumers' perspective, as well as from the government's perspective. Given the potential ubiquitous use of a National Identity Card if issued,[67]

> [T]he failure of the card could be very problematic, both for the individual concerned, who might become, in essence, a non-entity, and for any system that places great reliance on the card's effectiveness. Currently, if the Employment Insurance database experiences technical problems or a person loses their health card, there might be some inconvenience, but witnesses suggested it would be minimal compared to the possible disruption caused by the loss or failure of a multi-purpose card.

Thus, the potential for harm stemming from a single, multi-purpose card appears to outweigh any potential convenience or claimed security it may offer.

---

65 Standing Committee Interim Report, *supra* note 4, at pp.11.

66 *Ibid*. at pp.11-12.

67 *Ibid.* at pp.11-12.

TECHNOLOGICAL AND PRACTICAL SHORTCOMINGS

A national ID card, with or without biometrics, is unlikely to provide increased security by authenticating identity for either the purpose of bolstering national security, or preventing identity fraud. While the policy arguments underlying this failure have been outlined above, this section will address the technological and practical shortcomings of the National Identity Card scheme. In fact, a National Identity Card program may be incredibly vulnerable to exploitation and misuse. Noted critic Bruce Schneier flatly argues, "a National ID card program will actually make us less secure". He argues that in order to measure the effectiveness of the cards, we should focus on how they fail, rather than how they may succeed. As he explains, [68]

> What matters is how the system might fail when used by someone intent on subverting that system: how it fails naturally, how it can be made to fail, and how failures might be exploited.[69]

National Identity Cards can be criticized in three respects: firstly, they will be prone to the same abuses that other forms of identification suffer, secondly, designing an implementation scheme specifying who will be issued a Card, and who will not, includes the potential for social exclusion; and finally, the addition of biometric indicators will not make National Identity Cards more secure, but potentially even less secure.

Issuance of a New Card, The Same Problems

Identity cards in general are susceptible to various forms of technical abuse and insecurity.[70] Firstly, no matter how sophisticated the design, they remain vulnerable to those who invest great time and energy in producing forged versions. National Identity Cards, no matter how clever the design, will be forged by those who are sufficiently determined to do so.[71] Further, a related issue rests in the fact that National Identity Cards can only be as secure as the identity documents used to issue them.[72] Like any other piece of official identification, the point of issuance presents a great opportunity for fraud to occur. Because

---

68 Schneier, *supra* note 42.

69 Schneier has even gone so far as to label them "National Insecurity Cards". *Ibid*.

70 *Ibid*.

71 *Ibid*.

72 There are two main types of identity documents used by Canadians. The first are often referred to as "foundation" documents, and include birth certificates and immigration records. These primary documents are used to obtain documents of the second type, "entitlement" documents, such as passports, drivers' licenses and social insurance numbers. Standing Committee Interim Report, *supra* note 4.

other pieces of identification, like drivers licenses and birth certificates for example, which may well be much easier to forge, may be used to issue the National Identity Card, fraudsters may still be able to obtain fraudulent cards if they go to the trouble of forging other pieces of identification first. This loophole negates the security rationale for issuing the new card in the first place.[73] National Identity Cards may not be any less prone to fraud than any other piece of identification currently available.

Second, people lose their identification all the time, and wallets and purses often get stolen. National Identity Cards would remain vulnerable to loss and damage just like other pieces of identification. However, because of the greater value that these cards will have, a method of dealing with loss will have to be developed, and this new protocol may itself be vulnerable to abuse.[74]

Third, National Identity Cards will still be susceptible to human error in terms of sloppy ID verification. There is no way to assure that the cards will be diligently verified by those hired to do so.[75] To err is human, and mistakes will inevitably occur. Notably, the addition of biometric indicators does not offer a solution to this problem, as they are themselves highly prone to error.[76] Additionally, even a recorded biometrics, as noted by digital rights group Electronic Frontier Foundation, is no more safeguarded than the identification utilized to acquire it. Thus, where biometric data has not been previously recorded, and one's actions have not attracted suspicion, it is still possible to use phony documentation together with a genuine biometric and have both listed on a National Identity Card. Therefore, the quality of the initial enrolment or registration of biometric identification is pivotal.[77]

As previously mentioned, if introduced, National Identity Cards would be the most powerful form of identification available to Canadians. Given the importance that the government and the public will attach to the new card, determined fraudsters are more likely to take the risk in obtaining cards, whether it be through theft or fraud. Thus, black market dealings for National Identity Cards may be intense. Ultimately, there are security benefits from having a variety of different ID documents, and avoiding the pitfalls of making one especially important.[78]

---

[73] According to the House Standing Committee on Citizenship and Immigration Interim Report: at both the federal and provincial levels, reforms are either proceeding or are being contemplated to ensure that foundation documents are more reliable and are only issued to their rightful bearer. However […] the risk of fraudulently obtained foundation documents is real and could jeopardize a multi-billion dollar national identity card system". Standing Committee Interim Report, *supra* note 4, at pp.12.

[74] Schneier, *supra* note 42.

[75] *Ibid*.

[76] Refer to "Biometrics:Failing and Failing Badly", below.

[77] Electronic Freedom Frontier, "Biometrics: Who's Watching You?", [***EFF Biometrics***], online: http://www.eff.org/Privacy/Surveillance/biometrics/

[78] Schneier, *supra* note 42.

Social Exclusion and National Identity Cards

Perhaps the most practical question concerning implementation of a National Identity Card rests in deciding who will be issued a National Identity Card, and who will not? [79] Being denied possession of a National Identity Card could effectively marginalize individuals, barring them from an assortment of activities if Card use becomes ubiquitous. In short, "ID cards are, by definition, markers of membership".[80] Critics have hypothesized the creation of a social ranking system arising from a National ID Card program, and argued that social exclusion could occur.[81] As Dr. David Lyon, Director of the Surveillance Project at Queen's University, and Professor of Sociology, argues:[82]

> With the use of biometric ID cards, the codes that determine the status of those who hold (or do not hold) the cards are increasingly related to bodily and behavioural characteristics. This further abstracts from the narratives of ordinary life and struggle experienced by those who are most vulnerable. As Didier Bigo suggests, biometric ID cards produce not so much a *pan*opticon as a *ban*opticon. In other words, they are not meant to put all under scrutiny, but to single out the exceptions as quickly as possible. Profiling to discover differences, the banopticon channels flows of information in order to control at a distance any who deviate from the coded norms. Skin colour, accent, attitude – these may all be used to assign worth or risk, such that 'hazards' may be removed swiftly. The multiplication of stories of those who have been wrongfully apprehended, detained and even tortured since 9/11 only serves to underscore the dangers of automating such processes.
>
> […] States are likely to see ID Card systems as intrinsically attractive. They can keep out unwanted foreigners in an economical way and also help to stimulate technology-dependent economies. Far from being a means of ensuring greater social cohesion, however, the evidence presented here suggests that ID cards will aid the processes of profiling and classifying, thus accentuating difference.

---

[79] Under the U.K. scheme, for example, cards will be issued to legal residents of the U.K. (of 3 or more months), including foreign nationals, who are over the age of 16. U.K. Home Office, online: http://www.homeoffice.gov.uk/passports-and-immigration/id-cards/

[80] David Lyon, "Identity Cards: Social Sorting by Database", Oxford Internet Institute, Internet Issue Brief No. 3, November 2004, [***Lyon***] at pp.3, online: http://www.oii.ox.ac.uk/resources/publications/IB3all.pdf.

[81] See for example, James B. Rule, "Time to Ask Questions About the Paths Opened by ID Cards", Oxford Internet Institute, Internet Brief No. 3.2, January 2005, online: http://www.oii.ox.ac.uk/resources/publications/IB3all.pdf.

[82] Lyon, *supra* note 80 at pp.8.

This concern is far from theoretical. Inevitably there will be individuals who will not be able to get Cards, and will be negatively impacted by virtue of their exclusion. This is especially problematic given that the most vulnerable members of our society, like refugees for example, may be further marginalized. The question, therefore, for proponents of the National ID Card scheme will be how to address the potential inequities in implementing such a Card.[83]

Biometrics: Failing and Failing Badly

As mentioned above, biometrics may not solve the many failures of a National Identity Card scheme. Biometric identifiers are unreliable and may do more to exacerbate the issue of misidentification than they do to remedy it. The reason for this is simple: biometrics of all kinds, even the more popularly used face recognition,[84] iris scanning or fingerprinting forms of biometrics, remain technologically unreliable and thus ineffective as identifiers.[85] Privacy advocates have emphasized that any arguments in favor of their accuracy are generated by the biometric technology industry itself, which is not only biased, but also capable of manipulating the results of biometric testing.[86]

Biometrics experts measure the reliability of biometric systems by considering two measurements: **false accept rates** and **false reject rates**. False accepts, or false matches, are cases where the system grants access although the person presenting the card does not actually match the embedded biometric feature (i.e. to a person that should have been rejected). False reject rates, or false non-match, measure instances where the system rejects identification despite the fact that it is presented by the legitimate cardholder (i.e. to a person that should have been accepted). At present, biometric systems with false accept rates and false

---

[83] Note that s.15 (1) of the Canadian Charter of Rights and Freedoms proclaims: "Every individual is equal before and under the law and has the right to the equal protection of the law without discrimination" and, specifically bars discrimination based on race, national or ethnic origin, colour, and religion among others. Thus, the Charter offers a means of attacking any potentially discriminatory implementation standards of a National ID Card scheme. See generally, Mary C. Hurley, "Charter Equality Rights: Interpretation of Section 15 in Supreme Court of Canada Decisions", Parliamentary Information and Research Service, Library of Parliament, January 2005, online: http://www.parl.gc.ca/information/library/PRBpubs/bp402-e.htm.

[84] Accounts of facial recognition in electronic identification chips in U.S. passport show that this biometric is highly prone to error, with a failure rate of between 10% and 40%. See Jonathan Krim, "Passport ID Technology Has High Error Rate" (6 Aug 2004) The Washington Post, online: http://www.itl.nist.gov/iad/Articles/Facial-Passports.html.

[85] Fingerprinting has been seen as a more promising science at 0.4%, yet can be equally ineffective. See Krim, *Ibid*.; John Lettice, "Are Fingerprints Really Infallible, Unique ID?" *The Register* (6 April 2004), online: http://www.theregister.co.uk/2004/04/06/identity/. Fingerprint machines have been cited as ineffective: see Ian Austen, "Latest fingerprint scanners go beyond skin deep" New York Times News Service (18 Oct 2004), online: http://www.lumidigm.com/press/Documents/NYTimes_10_14_04.pdf.

[86] EFF Biometrics, *supra* note 77.

reject rates of 1% are considered reliable. Applying this statistic, if 1000 individuals were scanned, about 10 would be mistakenly denied access, and another 10 mistakenly granted access.[87] In fact, for a card to be highly secure, there would have to be a lot of false rejects. In other words, the system would have to reject a high number of legitimate cardholders based on the sheer number of individuals registered by the system (i.e. the inherent margin of error).[88] As the House of Commons Standing Committee on Citizenship and Immigration noted regarding high failure rates, [89]

> [L]egitimate National Identity Card holders could be subject to suspicion and accusations when the technology fails.[90] […] to lower the false reject rate would result in raising the false accept rate. Of course, a high false accept rate would undermine the purpose of creating a National Identity Card.[91]

As explained above, biometric systems measure and record biometric characteristics of a person and match the obtained biometric data to a database containing additional information about the individual in question. There are two ways in which data may be 'matched' with an individual: either through one-to-one matching, where the on-the-spot biometric scan is matched to only one sample stored in a database or card chip, or through one-to-many matching, where the on-the-spot biometric scan is matched to a multitude of stored samples (e.g. with a database of individuals who are highly suspicious). Thus, there exists yet another manner of describing biometric failure.

Biometric systems either fail in one-to-one matching, where subjects are matched with their own reference samples (*false non-match*), or else they fail in one-to-many matching, where they falsely match a class of subjects with the reference samples of others (*false match*). In the first case, little can be done if a biometric system has incorrectly matched a person with his or her own biometric. Because a failed biometric cannot be retrieved or reproduced, the cost of failure is borne by the individual. In the second case, a certain proportion of persons suffer the potential fallout of being falsely identified. This has already occurred in a number of cases in the U.S. where fingerprinting, for instance, incorrectly

---

87 CIPPIC, "Biometrics: FAQ", [***CIPPIC Biometrics***], online: http://www.cippic.ca/en/faqs-resources/biometrics/

88 It is significant to mention the enormous scale of the National Identity Card plan here. For example, the United States Immigration and Naturalization Service (INS) (now called the Bureau of Customs and Border Patrol of the Department of Homeland Security) for example, handles some 1 billion entries and exits per year. If the error rate were even 0.1%, 1 million person visits would be subject to the inconvenience of investigation, not to mention the enormous burden of allocating resources to track false leads.

89 Standing Committee Interim Report, *supra* note 4 at pp.14.

90 Also see "Consumer Concerns: Consequences of Misidentification", below.

91 Biometric technology experts suggested that using two or more biometric identifiers on the card could ensure greater security. Facial recognition logarithms coupled with fingerprint or iris data could address this concern. Standing Committee Interim Report, *supra* note 4 at pp. 14.

matched persons' identities with those of criminals.[92] In such cases, the cost of failure is extremely high and, again, borne by innocent individuals.

An example of the harm that can arise via misidentification can be found in a product liability and slander case was brought forward in 2004 against Biometrics Company Identix and the states of California and Oregon. Here, two plaintiffs sought restitution for the damage inflicted by duplication in police records, which gave them other people's criminal records.[93] In this case, misattributed fingerprint scans and duplicate record ID numbers lead to the unfortunate situation arising. As John Lettice explained, "fallibility in software and human input can produce extremely serious errors in systems which are intended to provide virtually infallible identification".[94]

The trial run of the British National Identification Card in early 2004 revealed numerous problems with an ID card kit to be offered to the public. Such problems included "hardware, software and ergonomic problems" or calibration problems.[95] British scientists found that facial recognition is increasingly difficult with populations over 1000; fingerprints did not register correctly; and iris scanning was ineffective due to inconsistent lighting and ergonomic conditions, and potentially undetectable problems with machines that would distort results.[96] As Charles C. Mann states, when biometric systems fail, they "fail badly".[97]

Putting aside concerns over the accuracy of data collection and matching, biometrics is controversial for many other reasons.[98] Firstly, many consider the collection of biometric data to be intrusive. Secondly, because digital information is easily copied, transmitted, altered and searched, it is particularly vulnerable to privacy breaches. Thirdly, biometric data cannot easily be substituted. While credit card cards and passports can be invalidated and replaced if necessary, the same cannot be said of biometric identifiers. Once a biometric identifier is compromised, it stays compromised, as the physical characteristics used in

---

92 Fingerprinting has lead to extended detentions of innocent individuals in such cases. See Benjamin Weiser, "Can Prints Lie? Yes, Man Finds to His Dismay" *The New York Times* (31 May 2004), online: http://www.nytimes.com/2004/05/31/nyregion/31IDEN.html?ei=5007&en=6fc3c22e435936e1&ex=1401336000&partner=USERLAND&pagewanted=all&position=; "The FBI Messes Up" *The New York Times* (26 May 2004), online: http://www.nytimes.com/2004/05/26/opinion/26WED2.html?ex=1400904000&en=2eaeb0a5fbb0e411&ei=5007&partner=USERLAND.

93 John Lettice, "DHS and UK ID Card Biometric Vendor in False ID Lawsuit", The Register, (May 11, 2004) [***Lettice, False ID Lawsuit***] online: http://www.theregister.co.uk/2004/05/11/identix_false_id_suit/print.html.

94 *Ibid*.

95 John Lettice, "Glitches in ID Card Kit Frustrate Blunkett's Pod People", *The Register* (5 May 2004) online: http://www.theregister.co.uk/2004/05/05/id_pilot_glitches/print.html.

96 *Ibid*.

97 Charles C. Mann, "Homeland Insecurity", September 2002, The Atlantic Online, online: http://www.theatlantic.com/doc/200209/mann. Also, Schneier, *supra* note 42.

98 CIPPIC Biometrics, *supra* note 87.

biometric identification have not been altered. Fourth, biometrics does not work well on certain individuals, [99] such as those with certain disabilities, [100] or those with "unreadable" biometric characteristics. [101] Finally, as use of biometrics entails automation of identification processes, it is particularly vulnerable to technological failure. It is difficult for human substitutes to manually execute iris scans, for example, if computerized scans fail for some reason. Further, substituting identity documents in such a situation would compromise the rationale driving National ID Cards.

CONSUMER CONCERNS

Fraud

A primary concern with a National ID Card from a consumer perspective is that of fraud. Many aspects of this issue have been discussed in other portions of the report, and so to summarize, National Identity Cards may be highly susceptible to fraudulent activity in the following ways:

- National Identity Cards may be obtained using other pieces of fraudulent identification, foundation documents, which are themselves easier to counterfeit. Thus, National Identity Cards would inevitably be wrongly issued to individuals who should not possess them.

- The risk of fraud is heightened because of the relative strength of a National Identity Card as a form of identification in comparison to other pieces of identification.

- The card itself may be counterfeited, no matter how sophisticated the design.

---

[99] Labourers and many others do not fingerprint well. A report by Privacy International anticipated that the biometrics to be potentially used in a UK national ID card would fail in a large number of similar cases. "UK Identity Cards and Social Exclusion" (30 May 2005), online: http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-228833.

[100] More than four million disabled persons alone would encounter problems when using a combination of biometric techniques, from mild to very serious obstacles in accessing public or private services. See 'Resources Related to Biometrics and People with Disabilities' *The International Center for Disability Resources on the Internet*, online: http://www.icdri.org/biometrics/biometrics.htm

[101] Aniridia a genetic defect that usually results in both eyes developing without an iris. People with aniridia would thus be prevented from using iris recognition technology. While anirida is rare (1 in 64,000 live births), it serves as a useful example of biometric technology operating in a way that makes society inaccessible to disabled persons. "Aniridia", eMedicine.com, online: http://www.emedicine.com/OPH/topic43.htm.

The addition of biometrics would fail to ease this concerns. Fraud is a multi-faceted issue, and requires multiple safeguards, rather than just one solution, such as biometric indicators, which are themselves prone to fraud. Once an individual's signature, fingerprint or voice is captured, there is little to prevent others from using it in contexts where the specific individual does not even need to be present to give their biometric information. Persons who allow their biometric to be scanned risk enabling that captured information to be used in unauthorized contexts. Vendors and scanner operators may state that they have technologically protected this information, yet there is no way for the consumer to verify whether such protections are properly implemented and fully functional.[102] Also, as mentioned above, a valid biometric may also be attached to a fraudulent identity, and would therefore serve as a completely ineffective safeguard.

Consequences of Misidentification

Although consumers may fear fraud more than misidentification, they will be most affected and inconvenienced by misidentification. No system is infallible. This may be especially true of a National ID Card, which will likely require a vast infrastructure to make it function. As this report has already highlighted, the Card may be plagued by the statistical weaknesses of biometrics, and will compensate by employing high false reject rates. However, the practical consequences of this safeguard may inevitably lead to long lines and delays. Such delays in flight plans, for example, can be costly and extremely inconvenient. Additionally, this creates practical problems for security staff and others hired to verify identification. Mistakes in checking ID are unavoidable, especially given the repetitive and boring nature of the task.[103] However, high false reject rates may serve to confound the problem, by making the verification process more onerous, yet less reliable.

Furthermore, the embarrassment of being singled out, or "caught" so to speak, can cause distress. Further, additional background checks may lead to even more serious consequences, such as interrogation, which will obviously necessitate additional staff and resources. As Ann Cavoukian, Information and Privacy Commissioner of Ontario, noted in her statement to the House of Commons Standing Committee on Citizenship and Immigration in regards to National Identity Cards and biometric technology:[104]

---

102 EFF Biometrics, *supra* note 77.

103 Schneier, *supra* note 42.

104 Ann Cavoukian, Information and Privacy Commissioner, Ontario, "Statement to the House of Commons Standing Committee on Citizenship and Immigration regarding Privacy Implications of a National Identity Card and Biometric Technology", November 4, 2003, [***Cavoukian***] online: www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=14793&N_ID=1&PT_ID=11457&U_ID=0.

> We must recognize the difficulty of convincing security staff that the biometric match is incorrect and that you have been falsely accused. This is a legitimate risk, especially in any public safety or national security context where secrecy is the operative paradigm.

This will be especially true of the National ID Card's impact on international travel and commerce. Cross-border travel and trade is vitally important to the Canadian economy. Consequently, [105]

> The confusion and congestion caused by thousands of individuals being falsely identified on a daily basis as security risks would threaten to bring our travel and trade with other countries, particularly the United States, to a grinding halt.

Finally, as the National Identity Card will likely require a massively complex system that is itself prone to human error, not to mention technological bugs and even worms and viruses that may also lead to misidentification. This is especially problematic given the potency of the Card, the perceived utility of which may outweigh all other pieces of identification.

Public Perception

Two polls were conducted on the issue of National Identity Cards. The first, a COMPAS/National Post poll from December of 2002 asked respondents to compare the possible security benefit and the possible risk to freedom of issuing a high-tech identity card for all residents of Canada. Although 57% of those polled said it was a good idea and 30% said it was a bad idea, it has been noted, "the context in which the question was asked, however, raised doubts about the usefulness of the response".[106] EKOS Research Associates conducted a second poll, dated March 31, 2003 entitled "Canadians' Views Towards a National ID Card and Biometrics", at the direction of Citizenship and Immigration Canada. This poll also demonstrated significant public support for a national identity card. 67% supported a voluntary ID card, while 65% supported a mandatory ID card. Significantly, this poll went on to demonstrate that most Canadians do not understand the term 'biometrics'.[107]

---

105 *Ibid*.

106 Standing Committee Interim Report, *supra* note 4 at pp.6.

107 EKOS Research Associates, "Canadians' Views Towards a National ID Card and Biometrics", March 31, 2003, as quoted in Standing Committee Interim Report, *supra* note 4 at pp.8 [***EKOS Research***].

However, it is possible that public support for a National ID Card has declined since the polls were conducted. Furthermore, as noted by EKOS Research itself:[108]

> While overall results suggest solid support for the adoption of a new National ID Card and the use of biometrics by governments and the private sector, the possibility that these results represent a peak of support exists. […] It is certainly plausible that a public debate on the issues could erode support. […] Adding to this challenge, we find that the strongest arguments for adoption of these technologies are based on those that point to the inadequacies of current documents, systems and procedures, leading to fraud and abuse.

While on the surface it may seem that public support for National ID Cards is high, this support may be based on inadequate information and discussion. Thus, in order for consumers to properly weigh in on the debate, they must be educated about every aspect of the scheme.

Government authorities may interpret this bias as a lack of preparedness for the potential for terrorism in Canada,[109] but it may indicate that Canadians recognize the value of protecting their own individual despite the culture of fear that permeates society. Alternatively, it may suggest that the public does not see National Identity Cards or biometrics as effective in preventing threats against national security. And, if the evidence is correct, the public is justified in this belief. Indeed additional security personal, dogs, etc. are more effective in combating terrorism than are identification documents.[110]

Who's going to pay for this?

Given the scope of a National Identity Card project, it will without a doubt be very expensive. Estimates have ranged from $2 billion to $5 billion.[111] Given the government's past handling of large expenditures such as this one, it is likely that the cost will tilt toward the upper limit. The official word at this point is that it is impossible to predict the future cost of rolling out a new Card scheme without a proposal for a specific type of card and data management system.[112] However, many critics have made reference to the cost of the national gun registry that far exceeded projected cost estimates, and has cost over a billion dollars to register

---

108 *Ibid*.

109 "Canadians should brace for transit attacks, McLellan warns" CBC News (11 July 2005) online: http://www.cbc.ca/story/canada/national/2005/07/11/mclellan-attacks-050711.html.

110 Paul Elias and Brian Bergstein, "Dogs, people best at securing mass transit" (12 July 2005), Globe and Mail, online: http://abcnews.go.com/Technology/print?id=929989.

111 Standing Committee Interim Report, supra note 4 at pp.13

112 *Ibid*.

a minority of Canadians. Consider that when the province of Ontario debated introducing an entitlement smart card, start-up costs were estimated at $500 million.[113] Also, a proposal to replace the Social Insurance Number with a National Identity Card was discussed in the 1990s and was rejected by the government due, in part, to a projected cost of as much as $3.6 billion. The new permanent resident, or "Maple Leaf" card, which has cost over $120 million by 2005 to register 1.5 million permanent residents, despite the $50 cost recovery fee charged to each applicant. [114]

Given the enormous financial burden of introducing a National Identity Card, the government will have to decide, what cost, if any, will be borne by the consumer? As individuals currently have to pay for their own passports and other government licenses, it is not a far-fetched idea that a fee would be charged for the National Identity Card. While it may be reasonable to levy a replacement fee, it is not reasonable to charge an initial enrollment fee.

PART B: PRIVACY IMPLICATIONS

A National Identity Card will involve a vast accumulation of consumer information, which is cause for concern from a privacy standpoint. The major privacy implications stem from function creep, the threat posed by use of collected information for purposes other than that for which it was originally collected. Further, protecting the databases holding personal information is not only costly, but also incredibly burdensome to execute and difficult to assure. Finally, exceptions under *PIPEDA* permit information to be exchanged between and within government, as well as between businesses and government that may ultimately be worrisome for persons wishing to protect all aspects of their identities from improper or intrusive use and disclosure.

FUNCTION CREEP

Function creep is the term that has been given to the use of a unique identifier, often government-issued, for purposes other than those for which it was issued. Misuse of Social Insurance Numbers is a good example of how function creep can lead to the over extended use of an identifier into novel domains. Legislation regulating use of Social Insurance Numbers forbids a business or government from requiring an individual to share his or her SIN for a purpose other than taxation or employment. The law does, however, permit other entities to *ask* for

---

113 *Ibid*.

114 *Ibid.* at pp.13-14.

Social Insurance Numbers. Most consumers comply, and provide their SIN for various authentication purposes in the course of routine financial transactions.

In 1998, the Auditor General of Canada stated that the SIN had become a "de facto national identifier for income-related transactions, contrary to the government's intent".[115] A similar fate likely awaits the National ID Card. It will likely be regarded as an ideal unique identifier – without the stigma and sensitivity of a SIN. However, as PIAC argued before the Commons Standing Committee on Citizenship and Immigration, unique identifiers in the hands of identity thieves are powerful tools.[116] As argued above in relation to identity theft, unless businesses are forbidden from relying upon National ID Cards to identify individuals and qualify them for services, National ID Card information, once stolen by an identity thief, could immediately be used to initiate any number of electronic transactions, or other transactions that can be completed remotely (i.e. not in person).

Thus, legislation must outline the uses and abuses of National Identity Cards to contain function creep. Unless businesses are forbidden from asking for the National ID card information, it will enter the stream of commerce and, like all other personal information, be vulnerable to theft or disclosure through negligence or inadvertence. Additionally, if this information were collected then the range of harm possible would continue to expand. It would then be necessary to mandate businesses to properly secure this information, and also prevent them from compiling information to form consumer profiles.[117]

Additionally, the projected cost of a National Identity Card system would only encourage the expanded use of its functions. However, as witnesses have argued before the House Standing Committee,[118]

> When [citizens] provide information to government, we are normally promised that it will only be used for the purpose for which it was collected. If the state and its enforcement agencies are able to access that information for other purposes, it was suggested that a fundamental promise would be broken.

Finally, many have argued that National ID Cards may be used in so many contexts that they would earn the title of "internal passport".[119] For example, as George Radwanski, former Privacy Commissioner of Canada commented:[120]

---

115 It was also noted that "Existing SIN application procedures are insufficient to guard against fraud and abuse", and that "minimal effort is dedicated to investigations of SIN fraud and abuse, and penalties are minimal, with no real impact on deterrence." 1998 Report of the Auditor General of Canada, Chapter 16, online: http://www.oag-bvg.gc.ca/domino/reports.nsf/html/9816ce.html

116 PIAC, Identity Theft, *supra* note 51.

117 Please refer to "One Card, One Database: Increased Vulnerability", below.

118 Standing Committee Interim Report, supra note 4 at pp.11.

119 *Ibid*. at pp.9.

> In Canada, agents of the state have no right to require us to identify ourselves in our day-to-day lives unless we are being arrested or we are carrying out a licensed activity such as driving. The police cannot stop people on the street and demand, "Your papers, please."
>
> The creation of a *de facto* internal passport would inevitably change that.

While this may be an extreme example, the unimpeded progress of function creep should illicit proper safeguards and barriers to prevent this sort of worst-case scenario from occurring.

VOLUNTARY VERSUS MANDATORY CARD SYSTEMS

Robert Marleau, the Interim Privacy Commissioner of Canada, commented:[121]

> Complete and absolute authentication of identity would be impossible if only a segment of the Canadian population were to register with the national system. […] If the national identification system is to have the advantages claimed for it, it would have to be mandatory.

While Marleau makes a valid point, much of the discussion regarding a National Identity Card scheme has indicated that the Card would be implemented on a voluntary basis, at least at first.

As mentioned above, survey results indicate that Canadians would prefer a voluntary card system as opposed to a mandatory card scheme.[122] Yet, as Ontario's Information and Privacy Commissioner Ann Cavoukian and others have argued, once the National Identity Card system is implemented, their use will gradually become normalized rather than voluntary.[123] This phenomenon is yet another effect of function creep. As it has been noted, "[v]oluntary schemes have

---

120 George Radwanski, Privacy Commissioner of Canada, "Statement before the House of Commons Standing Committee on Citizenship and Immigration regarding a National Identity Card", March 18, 2003, Ottawa, ON, [***Radwanski***] online: http://www.privcom.gc.ca/speech/2003/02_05_a_030318_e.asp.

121 Robert Marleau, "Why We Should Resist a National ID Card for Canada", Submission of the Office of the Privacy Commissioner of Canada to the Standing Committee on Citizenship and Immgration, September 18, 2003, [***Marleau***] online: http://www.privcom.gc.ca/media/nr-c/2003/submission_nid_030918_e.pdf.

122 EKOS Research, *supra* note 107.

123 Cavoukian, *supra* note 104.

a funny way of turning into compulsory ones in all but name".[124] This is due in large part to expansion of a card's uses into domains not originally anticipated at the time the Card was implemented. The more it is requested in order to verify identity, the more individuals will feel that they (a) need to possess it, and (b) need to produce it upon request. If public or private agents began defaulting to the card as the most legitimate form of identification, individuals may be asked to produce a card on request whether or not they have enrolled for one. The gradual requirement of the card for identification by both government and commercial entities will likely have the effect of restricting access or service to groups who choose not to obtain a card. Thus, National Identity Cards will become *de facto* mandatory, despite legislation to the contrary.

The planned adoption of a similar card in Australia in the 1980s was halted by widespread concerns over function creep.[125] These concerns arose, partially, after the public discovered the government's secret plans to intentionally trigger function creep, and by so doing, transform the card from voluntary to mandatory:[126]

> It will be important to minimize any adverse public reaction to implementation of the system. One possibility would be to use a staged approach for implementation, whereby only less sensitive data are held in the system initially with the facility to input additional data at a later stage when public acceptance may be forthcoming more readily.

This disturbing revelation suggests that the same may be possible in Canada, as we already categorize personal information as 'more sensitive' and 'less sensitive'.[127] For example, publicly available information, such as that listed in the telephone directory, is considered low on the sensitivity scale while employee data (other than name, title, etc.) qualifies as highly sensitive.[128] This categorization scheme begs the question, where would National Identity Card information rank in terms of 'sensitivity', for the purposes of *PIPEDA*? In the commercial realm too, just as SIN cards are often requested by businesses to the point that Canadians feel compelled to provide it, National Identity Cards will likely become the gold standard for commercial transactions. As previously described, SIN cards are used for numerous purposes unintended by

---

124 *Charter*88, *l.c.*, 4 cited in De Hert, *supra* note 19 at pp.27.

125 Privacy International "On Campaigns of Opposition to ID Card Schemes", 1 January 1996, online: http://www.privacyinternational.org.

126 Health Insurance Commission, Planning Report of the Health Insurance Commission, Feb 26, 1986 cited at fn. 21 of Privacy International discussion of Australian Card scheme of the 1980s, online: http://wearcam.org/envirotech/simon_davies_opposition_to_id_card_schemes.htm.

127 For example, see *PIPEDA* Principles 4.3.4, and 4.7.2.

128 Murry Long, Suzanne Morin, "The Canadian Privacy Law Handbook: Applying Canada's New Private Sector Privacy Law", Centrum Information and Conferencing, Inc., First Edition, June, 2000, at pp.174.

legislation.[129] Indeed, if "both government and businesses started asking people to produce such a card, the pressure to conform would be enormous. People who didn't have one would increasingly be open to suspicion".[130]

The loss of privacy and social integrity that would arise through a voluntary card would arise in other respects as well. First, voluntary cards would not necessarily attract the legislative protections that mandatory cards would necessitate. This is particularly true of legislative protection extending to database security, and legislation outlining proper and improper use of personal information.

One Card, One Database: Increased Vulnerability

Possibly the most pressing danger associated with a multi-purpose National Identity Card is that detailed personal information would be compiled in a single database. From a technological standpoint, compiling data on one database is the simplest, most economical, and most efficient approach to keeping data. As the U.S. Supreme Court noted almost three decades ago, the "threat to privacy [is] implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files."[131] This threat takes several potential forms. First, there is a risk associated with matching and linking personal data. This data, once compiled, could lend itself to unauthorized and undesired use. However, information must be linked in order for the program to work as it is intended. There is also the related fear that the database may be "hacked", and personal information shared with unauthorized parties. The government officials authorized to run the system could even abuse these databases. Second, data contained within cards, such as biometric identifiers, could be harvested and or exploited. Such abuses by commercial or government authorities, another example of *function creep*, could be conducted contrary to the individual authorization for use of personal data.

Mass data losses and "data spills" of personal information are becoming more common and widespread. These breaches generally occur when unsecured computers with unencrypted personal information are stolen from businesses or government. The ChoicePoint,[132] Equifax Canada,[133] and Visa/Mastercard

---

129 Refer to discussion on SIN cards above, at pp. 30-31.

130 Radwanski, *supra* note 120.

131 *Whalen v. Roe*, U.S. Supreme Court Reports, 1977, Vol. 429, 589.

132 Individual posing as legitimate businesses purchased personal information from ChoicePoint for fraudulent purposes. The breach, discovered in October of 2004, was not made public until February 2005. For a chronology of news on this breach and others by data aggregators, see The Virtual Chase, online: http://www.virtualchase.com/tvcalert/choicepoint.html For similar incidents since ChoicePoint, see Privacy Rights Clearinghouse, online: http://www.privacyrights.org/ar/ChronDataBreaches.htm.

breaches,[134] for example, demonstrate how single incidents can affect millions of consumers. However, the security of personal digital information is also threatened by unauthorized access from outside an organization (hacking), or from within the organization. These concerns are particularly pressing when valuable information, as will be the case of National Identity Cards, is contained in databases. If these databases are violated, then a great deal of damage could be caused.

In order to protect against this harm, it is necessary to design a data protection framework. This may include both electronic security measures, as well as physical security measures to protect the government's databases, as is the case in Spain.[135] As noted by the House of Commons Standing Committee,[136]

> Data protection laws exist and could be expanded if a National Identity Card were introduced, [but] some suggested that for such laws to be of any value, a massive bureaucracy would be needed to administer the law and protect personal data.

This would be achieved at a great cost to taxpayers. The financial burden of implementing a top-level security system for the database could propel the Card scheme into uncharted financial territory, and would perhaps make it less likely to be implemented with stringent security measures. Ultimately, priorities will be set according to which features of the plan are worth the monetary investment, and which are not. However, securing databases should be at the top of the list of priorities if National ID Cards are introduced.

Secondly, the danger of function creep will be compounded by the increasing technological interaction between state and commercial sectors. Cards will find their way into private sector use in countries such as the U.S. and Canada.[137] Thus, risk of function creep will be reproduced in the commercial context, where the use of a single card identifying one's every movement, purchase and behavior in all areas leaves a more identifiable digital trail.

Consumer privacy is in particular danger when businesses, which have increasing technological access to numerous consumer details, make unethical,

---

133 Files were accessed by criminals posing as legitimate credit grantors. See "Hackers hit Canadian Credit Bureau" Globe and Mail, Canadian Press (16 June 2005).

134 A security breach experienced by the operations centre for a credit card processing firm exposed clients of Visa and MasterCard and other companies to fraud. See Brian Bergstein, "Theft indicates hackers' increasing power" Globe and Mail (21 June 2005).

135 Spain's databases are housed in a "fortified building on the outskirts of Madrid that resembles a maximum-security prison", assuring protection from external physical attack. However, Spanish officials were reluctant to clarify how the data itself was protected from misuse by officials and state security. Standing Committee Interim Report, supra note 4 at pp.25.

136 *Ibid*. at pp.10.

137 Colin Bennett, "Rules of the Road and Level Playing-Fields: the Politics of Data Protection in Canada's Private Sector", *International Review of Administrative Sciences* Vol 62, No. 4, December 1996 at pp.479.

illegal – and often undetectable - uses of data for financial gain. As previously noted, financial institutions and other private entities will feel compelled or else entitled to keep records of information collected about consumers.[138]

By maintaining these detailed consumer records, businesses contribute to the risk of misuse or theft of data internally, through employee misconduct. While external sources of hacking have been reduced, through security initiatives implemented by these large corporations, poor security training and awareness at the employee level have been primary contributors to problems of fraud and theft. Employees with access to large singular databases of information may actively use or disclose information to illegitimate sources for their own financial advancement. [139]

Another misuse of collected data is data mining. Data mining is the search for useful information or "hidden patterns in large, pre-existing collections of data, […] such as the fact that a specific commercial transaction is more common at certain times of the month or year".[140] Data mining ideally occurs when data is captured from a large segment of the population and patterns are uncovered. Compiling consumer information for data mining purposes is certainly not the purpose of issuing National Identity Cards, but it is a possible side effect. Again, legislative barriers could be helpful in preventing this issue from arising in the first place.

As PIAC argued before the Commons Standing Committee on Citizenship and Immigration, the aggregation of personal data, often cross-referenced to financial information or key identifiers like SINs, create a real threat of sudden, massive identity theft.[141] Furthermore, It remains difficult to imagine how a National ID Card could curtail the damage from such a data spill. In all likelihood, the unique identifier on the National ID Card would be linked to the information in databases that would remain vulnerable to loss. Thus, both businesses and government should take security measures commensurate with the sensitivity of the information they hold. Finally, there should be immediate, mandatory disclosure of security breaches to individuals.

---

138 Also see section on Identity Theft above. See also, PIAC Submissions, *supra* note 56.

139 Indeed, employees constitute the largest threat to the world's largest financial institutions according to a 2005 Global Security Survey conducted by Deloitte Touche Tohmatsu (Deloitte Touche Tohmatsu, online: http://www.deloitte.com). On one hand, employees are highly susceptible to *phishing* (Phishing constitutes sending emails from well-known sources, such as banks or utilities companies, and requesting confirmation of personal details. See 14, 39 of Deloitte Survey, ibid.) and *pharming* (Pharming is the exploitation of a vulnerability in the DNS server software that allows a hacker to acquire the Domain Name for a site, and to redirect traffic from that website to another web site.

140 Jay Stanley and Barry Steinhardt, "Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society", American Civil Liberties Union, January 2003, at note 6, online: http://www.aclu.org/FilesPDFs/aclu_report_bigger_monster_weaker_chains.pdf.

141 PIAC Submissions, *supra* note 56.

INADEQUATE PRIVACY LEGISLATION: *PIPEDA*

Canada's personal privacy laws, provincially and federally (especially the *Personal Information Protection and Electronic Documents Act* or *PIPEDA*[142]) require safe information practices by businesses and government. However, these acts typically do not provide real economic sanctions for non-compliance. As a result, *PIPEDA* does not have the bite that it needs to properly and effectively protect the personal privacy of Canadians with respect to the implementation of the National Identity Card scheme. As a result, organizations are left with space to maneuver and resist steps to make their personal information handling more secure.

PIPEDA is unfortunately weak in respect of demands by companies for personal information that is not strictly necessary for the requested service or transaction.[143] Consumers continue to receive better service in exchange for this superfluous data collection. Indeed, if National Identity Cards are introduced to Canadian society, businesses will face tremendous pressure to collect National ID Card information because of the assumed reliability of the personal information it will contain. As mentioned above, this collection may become a routine part of consumer transactions thereby exposing consumers to the risk of data spills, internal fraud, compiling and linking this data with other consumer data to create profiles, and ultimately, unsolicited target marketing.

Openings exist between government and private actors for information disclosures that risk violating individual privacy. Under *PIPEDA,* personal information may cross the commercial-government boundary in circumstances where national security is perceived or suspected to be at stake. Two provisions of *PIPEDA* are of particular concern in this respect. Specifically, s. 7(3)(c.1)(i) enables businesses to disclose personal information without an individual's knowledge or consent when it is suspected that said information relates to national security.[144] And s.7(3)(d)(ii) stipulates that the business may initiate disclosure of personal information if it is suspected that said information relates to national security.

Even biometric information may be provided to the federal government by vendors who permit or require a biometric payment option, when it is requested under *PIPEDA*. This poses a big threat to privacy, as information stored by biometric companies is potentially more valuable than information that does not

---

142 S.C. 2000, c. 5. [***PIPEDA***].

143 PIAC Submissions, *supra* note 56.

144 Alberta and British Columbia have enacted similar provisions in their privacy legislation: see *Personal Information Protection Act*, S.B.C. 2003 C.63, s. 18, and *Personal Information Protection Act*, S.A. 2003, c. P-6.5.

identify the physical body. The high value of this information translates to great cost to individual victims where it is abused or mistakenly disclosed.[145]

The problem lies in the fact that businesses are not well placed to balance the privacy interests of their customers or clients with broad national security concerns. The Canadian Privacy Commissioner has stated that "personal information" is to be broadly interpreted,[146] such that potentially any information given to a company may be available for disclosure. Schedule I, Principle 8 (Openness) of *PIPEDA* requires companies to provide consumers with a statement of their policies in respect of consumer privacy. However, it is unlikely that individuals take the time to research these policies and are aware of the precise uses and disclosures that can be made of their own personal data. Thus, the excessive discretion allotted to companies in using and disclosing personal information, whether or not consent is acquired, leaves personal information vulnerable to abuse both domestically and across the border.

---

[145] See De Hert, *supra* note 19 at 6 citing the clandestine use of facial recognition at the 2001 Super Bowl by the Tampa police.

[146] Privacy Commissioner of Canada, Annual Report to Parliament 2001-2002, Part 2: Report on the Personal Information Protection and Electronic Documents Act online: http://www.privcom.gc.ca/information/ar/02_04_10_02_e.asp#002.

Security Measures Associated with a National ID Card

If a National Identity card system is implemented, it will most likely carry electronic information, which necessitates implementation of an authentication system associated with the card to ensure that the bearer is the person represented. This objective could be achieved either through passwords and PINs, or through biometrics. Both schemes produce privacy concerns that warrant further discussion.

Ubiquitous use of passwords and PINs as a system of authentication ignores the inherent limits on an individual's ability to remember multiple passwords and PINs. Many individuals opt to record passwords and PINs along with their associated services, which benefits ID thieves. It is common for individuals to use the same password for multiple purposes, or record the different passwords with their associated uses, in order to remember them. Reliance on such a method of authentication, while helpful, is therefore of limited assistance in guaranteeing the security of any National ID card.

The use of biometrics is commonly discussed in relation to National Identity Cards because of their utility in authenticating identity. While the technological unreliability of biometrics has been discussed earlier in this report, there are also many privacy concerns stemming from use of biometrics in authentication.[147] Ann Cavoukian outlined 6 principles to support the introduction of biometrics in her presentation to the House of Commons Standing Committee on Citizenship and Immigration. These principles include: [148]

(1) Government clearly outlining the problem to be solved by biometrics;

(2) Broad consultation with the public;

(3) Legislation that defines a limited purpose for the introduction of biometrics, and sets limits for the collection, use and disclosure of biometric information;

(4) Effective and independent oversight, perhaps through the office of the Federal Privacy Commissioner, who should also have investigative powers to address complaints;

(5) Completion of comprehensive Privacy Impact Assessments for each stage of the project;

(6) Evaluation of the system to test its privacy strengths and weaknesses using international standards

147 Radwanski, *supra* note 120.

148 Cavoukian, *supra* note 104 at pp. 7.

Implementing the National Identity Card scheme without making protecting personal privacy a priority, would "pose a potentially lasting corrosive effect on our society".[149]

CONCLUSIONS AND RECOMMENDATIONS

National Identity Cards have been discussed as a means to bolster national security and as a tool to combat identity theft. However, a National Identity Card program will be an ineffective security solution to either problem. It will not benefit a society that is concerned about national security and identity theft, and is fraught with technological and practical shortcomings. Additionally, it produces a number of consumer concerns including fraud, misidentification, and the sheer cost of implementing the program. It also raises a number of privacy concerns that could potentially lead to violations of personal privacy if the program is not well contained. Indeed, information collected in relation to a National ID Card may be highly susceptible to function creep, and become widely used in the private sector. In conclusion, the use of National Identity Cards, with or without biometrics, in interactions between individuals and the state or commercial entities, in a context of inadequate legal and technological safeguards, would introduce new ways of violating individual privacy and integrity. It would also be unacceptably costly given the expected, poor, results. However, should the Canadian federal government pursue the idea of a National Identity Card, the following recommendations have been supplied to reduce the risk of harm to consumers and citizens with respect to privacy and civil rights.

Recommendations

1. Legislation must outline the uses and abuses of National Identity Cards to contain function creep.

2. Use of biometrics should be limited to one-to-one matching, as opposed to one-to-many matching standards.

3. Biometric data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.

4. Any biometric system must be structured toward impeccable levels of data security. This includes transmission that prevents interception,

[149] Cavoukian, supra note 104 at pp.8.

storage that prevents theft, and with very limited and supervised access by internal agents.

5. Verification of individual identity should not involve the *collection* of additional personal information, but rather simple verification of identity documentation.

6. Details contained on cards should be encrypted such that only those who possess card readers and software can read them.

7. Legislative privacy protections assuring consumers that as the holders of cards they are the owners of stored information and have the right to know what data and functions are on the card, to exclude certain data, and to reveal at their discretion specific data on the card.

8. Prohibition against the use or disclosure of personal information between businesses except with the express consent of consumers in every instance absent a court order.

9. Ensure that where data is outsourced to American companies, assurances will be sought and other measures taken to prevent information from being disclosed to third parties. Likewise, where Canadian companies contract in the U.S. protections against their forced disclosure of information under American Law.

10. An independent commission should be created to ensure that the use of the information is *supervised* and *secure* (similar to the Commission d'accès à l'information du Québec).

11. A strong audit and oversight program is required to provide the necessary checks and balances of conducting the program.

12. The cost associated of issuing a National Identity Card should be borne by the government, and not by individuals. While it may be reasonable to levy a replacement fee, it is not reasonable to charge an initial enrollment fee.