CAN ID?

VISIONS FOR CANADA'S IDENTITY POLICY

Understanding Identity Policy and Policy Alternatives

WRITTEN BY

Krista Boa, Andrew Clement, Simon Davies, Gus Hosein

Information Policy Research Program, Faculty of Information Studies, UofT

in partnership with

Policy Engagement Network, LSE

Faculty of Information Studies
University of Toronto

THE LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE

PEN paper 1

Summary

Whether intended or not, Canada is approaching the point of no return on a national identity policy. There is nothing simple or trivial about developing national policies for managing the identities of millions of citizens. Such policies are highly complex socio-technical interventions into the functioning of a nation, requiring significant investments of time and resources, with the potential of reshaping the relationship between the individual and the state. They must be carefully designed and deployed so as to avoid or balance an array of costs, risks and challenges. There are few opportunities for 'second chances' for getting it right.

This report maps, analyses and makes recommendations about the current identity policy landscape in Canada. Prepared by a team of independent researchers from the University of Toronto and the London School of Economics, with the support of a Contributions Program grant from the federal Office of the Privacy Commissioner of Canada, it draws upon experiences in other national jurisdictions as well as a review of selected cases of identity scheme development in Canada. To solicit further experiences, insights and feedback, the team also conducted two research workshops with government officials, academic, civil society organizations and private sectors firms who are active in the identity arena.

We begin by enumerating the main policy dynamics surrounding national identity schemes. The most significant of these are the political risks they inevitably incur. We also show how considerations of the various driving forces, feasibility and effectiveness issues, high implementation costs, ownership tensions and civil liberty challenges further interact to complicate the policy development process. The turbulent experience in the UK with its ID Card legislation and current struggles with implementation of the world's most ambitious national ID scheme provide abundant evidence for the fraught social, financial, political, and technical complexities of identity policy. We further illustrate these dynamics with the cautionary analysis of the current major identity development initiative in the U.S., REAL ID, which despite relatively swift passage into law is now facing of a host of problems that have emerged as its practical implications are considered more closely, and it may yet flounder.

At the same time however, there are undoubtedly significant benefits that can be derived from the development of a sound national identity policy framework. The needs for reliable and convenient forms of identity assurance are already widespread throughout society, and growing with the spread of digitally networked mediations for many forms of everyday transactions. A policy framework that tackled the recurring issues of identity authentication based on a firm understanding of the practical contingencies as well as the social dimensions could be an economic boon to commerce and re-invigorate citizen-state relations. Experience in other jurisdictions, notably France, Sweden, Hong Kong and Malaysia, while not exemplary in all aspects of their recent identity initiatives, do offer

valuable positive lessons for the Canadian context. In particular, they suggest that Canada would do well to avoid developing a single, monolithic identity scheme based on the enterprise-wide models that have emerged in corporate environments, such as a single, multi-purpose ID card, but rather develop a more flexible framework allowing for 'federated' ID schemes.

This danger in taking an 'all ID eggs in one basket' approach was strongly endorsed in the two multi-stakeholder research workshops we conducted in Vancouver and Ottawa. The discussions contributed insights into both the strategic challenges of a Canadian identity policy as well as the many practical issues it would face. There was a clear sense that Canada was not ready for a 'big bang' policy or another national ID card initiative. However, participants saw good prospects for making progress on the issues if based on clearly established objectives, a transparent development process, reinforced privacy protections and a 'pull' rather than 'push' approach that effectively demonstrated to Canadians the value they would derive from improving identity infrastructures and practices.

We also review a variety of identity programs, activities, actors and interests in Canada. As examples, we investigate current or recent identity initiatives in four provinces as well as several at the national level. In particular, we discuss in detail the major components of the current 'Smart Border' policy, as well as three identity related projects within the federal government. Unfortunately, we were not able to report on the pending development of the biometrically enabled e-Passport, now in development, because the Passport Office did not respond to our repeated enquiries about it.

We further analysed the various policy drivers, legal requirements, and specific implementations. Based on the examples we studied, generally we can see that the main overt drivers are more efficient access to government services, immigration and border management, and credential management. Some schemes are even looking to increase user autonomy and control. Interestingly, terrorism prevention seems to be less of a driving concern, at least explicitly. Similarly, law enforcement's goals seem to playing a driving role at interdepartmental level and in some of the work at the border. This may because the public is becoming less responsive to simple appeals to 'national security'. While privacy protection is many cases a prominently featured concern being taken into consideration, there are signs that this is more as lip-service, with the drive for other goals, such as efficiency and effective identity management, playing the greater role.

In analysing these Canadian identity initiatives for recurring themes, we find there is an over-reliance on technological optimism, often revealing a naive understanding of the limitations of new technologies as well as the challenges involved in turning technological possibility into well functioning systems. Perceived international obligations also play an exaggerated role, in some cases amounting to 'policy laundering', illegitimately forestalling adequate discussion of their appropriate application in Canada under the pretext that we have no choice in the matter. Furthermore, we find a tendency to pursue a 'one size fits all' approach that makes it harder to focus

on the specific problems at hand and think innovatively about simpler, more effective local solutions. Finally, considering the broad and significant changes in identity policy and practice already underway, we were shocked and alarmed at how little consultation with stakeholders has taken place to date. This situation must be corrected as a matter of urgency. Public consultation and participating in policy making with respect to identity systems too often appears to be treated as threatening and to be avoided if at all possible. Rather it is essential, not only because it allows the public to express their positions in these important debates, but it also improves the quality of decision-making. Canadian policy-makers need to avoid making the same mistakes as other countries, some of which have attempted to implement widespread use of biometrics without first better understanding the effectiveness and constraints of these techniques.

While we highlight many of the flaws and dangers in the current Canadian approaches to ID technology, policy and practice, we also explore the promising options that are worth pursing. We show how federated identity schemes in particular can accomplish legitimate identity policy goals while avoiding many of the pitfalls of the schemes underway. By drawing upon multiple credentialing agencies and a more fine-grained operationalization of identity assurance, federated identity allows for greater personal control by identity subjects as well as a more nuanced range of policy choices to accommodate the contending democratic, civil liberty and administrative requirements. When carefully considered, biometric can play a useful role in such approaches where high levels of identity assurance are necessary.

Turning many of the critiques and challenges raised in this study into positive alternatives, the report offers a variety of concepts, precepts and principles to better guide the development of identity policy and systems in Canada. We enlarge the definition of identity currently being developed with the Government of Canada to incorporate client and citizen perspectives on everyday identity transactions. Instead of focussing exclusively on the narrow preoccupation of a government agency asking if it is 'dealing with the right person', we argue that from the point of view of the citizen, the crucial identity question is about personal status and entitlement. With this premise, we then articulate several sets of principles, each based on a different but relevant perspective. From a legal/constitutional perspective and drawing upon the Charter of Rights and Freedoms, we postulate 'identity integrity' and related rights as fundamental to citizen identity. With a more organizational focus we extend the 10 fair information practice principles found in PIPEDA, first by incorporating explicit reference to identity in their wording and then by adding several more that address specific identity issues. Two of these draw directly on Microsoft's '7 Laws of Identity' as re-interpreted by Ontario's Information and Privacy Commissioner. We also offer desiderata for the properties of an identity system as well as how it is developed.

The report closes by highlighting five key tests aimed at ensuring that a Canadian identity policy framework will produce systems that are secure, cost effective, robust, trusted and fit for purpose.

These include a careful consideration of: Clarity of Purpose; Capability; Alternative measures; Consultation, and Respect for Rights.

Despite the need for Canada to address identity policy issues, this report does not call for an identity card policy. Identity cards entail large complex systems, and Canada needs proportionate and more specific solutions, framed by a national initiative to deal with identity policy in an integrative, but not monolithic fashion.

A successful policy can be celebrated as a revolutionary renewal of the social contract, but an unsuccessful policy risks being dismissed as the government showing its lack of respect towards its citizens. It is not a policy environment to be taken lightly and there is little room for simple logics of 'balancing rights and responsibilities', ‘technological breakthrough’, 'international obligations', and imperatives to combat fraud and terrorism. Instead it is probably best approached with great care and respect for what has gone before, both within Canada and from experiences abroad

We have shown that there are many paths forward for Canada, both dangerous and benign, and have sketched a map of the opportunities currently in our midst. We hope this can provide a basis for establishing good legislation and sound policy programs. Not all identity systems are designed equally. We can and must find a way of achieving our policy goals, satisfying the varied driving principles and actors’ interests, and promoting privacy protection, all the while honouring the relationship between the citizen and the state appropriate to a free and democratic society.

Table of Contents

1. Introduction

The Importance of Identity Policy 8

2. Dynamics of Identity Policy

1. Political risks 12
2. Drivers 15
3. Feasibility of Goals and Realities 17
4. Effectiveness of the Choices 19
5. Costs 21
6. Who decides the policy and owns the system? 24
7. How does the system regard privacy and civil liberties? 25

Case: REAL ID 26

3. Benefits of a National Identity Policy Framework

Why identity assurance is important 29
Uses for Identity Assurance in Various Sectors 31
Economic Benefits of Leading a National Discussion 34
Lessons from Abroad 36
Conclusions 39

4. Research Workshops and Consultations

Strategic Issues 41
Practical Issues 50
Summary 53

5. What's Happening in Canada

Ontario Smart Card Project 55
Identity documents in Quebec 56
Alberta's Drivers Licence 60
BC Ministry of Health 60
Smart Borders 62
Treasury Board Secretariat Identity Management Initiatives 69
Industry Canada 74
Statistics Canada's National Routing System 75
Synthesis 76

6. Analysis of Drivers: Key Challenges for Canada

Technological Optimism 77
International Obligations 80
Innovative Thinking 82
Consent and Consultation 84
Conclusions 88

7. Identity System Strategies

Components of Effective Identity Systems 90

8. Identity Policy Principles

A Citizen-Centred Definition of Identity 97
Guiding precept 97
Some fundamental rights in relation to Identity 98
Fair Identity Practice principles? 99
Identity system desiderata 102
Reflections on Identity Principles 105

9. Conclusions

The Five Tests 107
Importance of Process 108
Testing Canada 109
Concluding Remarks 114
About this project 115
About the FIS research team 116
About the LSE research team 117

Appendix A: Privacy Protection in Canadian Charter Jurisprudence

Section 8 Cases 122
Non-Section 8 Cases 127
Conclusions 129

Appendix B: Sources for Identity Principles

1. Introduction

Whether intended or not, Canada is approaching the point of no return on a national identity policy. Such policies are significant investments of time and resources and may reshape the relationship between the individual and the state. Yet some policies are fraught with complexities, risks, and significant challenges. There are few opportunities for 'second chances' at establishing such a policy.

This research maps out the Canadian policy landscape by identifying the policy dynamics: the variety of programs, activities, actors and their interests. As examples, we investigate in the current Smart Border Agreement, plans for the Western Hemisphere Travel Initiative, and the stated policy plans for biometric travel documents; while also looking at the plans for drivers' licences in various provinces; and consider the discussion paper from the Treasury Board. It is essential that we better understand these programs and analyse the nature of the projects, the organisations committing to the projects, and the objectives. This mapping is by no means comprehensive, as we can never know all the plans, programs, and schemes across Canada. But it will provide a snapshot to better understand the principal drivers and oft-stated policy goals.

After we have highlighted principles, programs and policies we then scrutinize the details and plans to consider their effectiveness and ramifications. We conduct analyses of the policy drivers, legal requirements, and the specific implementations. We review the technologies of biometrics so as to better understand their effectiveness; we will also review the perceived and real benefits for these programs and their implications. Most importantly we will be able to identify the key questions that remain unanswered, such as the extent of the problems that an identity policy is trying to solve.

Finally, we conclude that there are many paths forward for Canada, whether through policy or technology design. Not all identity systems are designed equally and there may be a way of achieving our policy goals, satisfying the driving principles and the actors interests, while minimizing the harm to the relationship between the citizen and the state, whilst applying, preserving, and enhancing privacy.

The Importance of Identity Policy

It is highly likely that the Government of Canada will have to consider establishing an identity policy. But identity policies are also emerging on provincial and local scales, and even in the voluntary and private sectors. Developing a policy regime to recognize, standardize, and create coherence amongst these policies is not trivial. In fact, it may require considering a policy framework for managing multiple identity policies.

A comprehensive identity policy involves creating or adapting a program for the collection and processing of individual-specific data that will be shared across services, both within and beyond government, often for a variety of purposes. Taking this broad definition of an identity policy, it is increasingly apparent that there are a number of programs in development across Canada that will amount to the core components of a national identity policy framework.

Some emerging components of a national identity policy include:

- e-Passport: In accordance with international standards emerging from the International Civil Aviation Organisation (ICAO), Canada is implementing new passport standards to incorporate facial biometrics.
- Western Hemisphere Travel Initiative and Smart Border Agreement: These two initiatives are both part of a larger program to secure our borders. These initiatives involve the development of greater data-sharing capabilities between border agencies in Canada and the United States.
- Treasury Board Identity Policy Discussion: The Treasury Board of Canada is preparing a discussion paper on the need to establish a national identity policy for Canada. The Treasury Board is clear that they do not intend to reintroduce the debate on national identity cards but there are likely to be proposals for increased data-sharing of authentication information.
- Principles of Authentication: For years Industry Canada has been leading debates within Canada on the definitions and uses of authentication, through its working group on authentication. As this work progresses it is likely to shape government and private sector implementations of identification and verification.
- Changes to Existing Identity Programs: Alongside changes to the passport, we are likely to see a number of calls for changes to the existing identification programs across Canada to cater for new policy drivers (e.g. combating terrorism) and new technologies (e.g. biometrics). We have already seen announcements from a number of provinces.[1] Even something as mild as requiring photographs for health insurance cards will involve significant changes in enrolment, issuance, and renewal processes.

Indeed, there are serious policy choices to be made and these must be made with great care. Every shift in design and decision over specification will have significant ramifications. Identity policies, as with all sophisticated and complex technology policies, have contentious components:

- technological (e.g. will the program be centralized and on-line; or decentralized and off-line; permitting one-to-one verifications or one-to-many verifications?)

1 e.g. 'B.C. drivers' licences could soon use biometrics for security', Ian Bailey, CanWest News service, October 16, 2006.

- legal (e.g. will there be an increasing duty to carry or a duty to be identified?)
- political (e.g. who is responsible for the policy? how will it be decided? who will (not) be involved in deciding?)
- social (e.g. will people trust and appropriate this technology because it is designed for their interests and enhances privacy or will it be seen as another mechanism for the state to collect more information on its citizens?)

Each of the policy choices carries significant risks. But the greatest risk is that the decisions we make (or choose not to make) may transform the relationship between the citizen and the state. This point was noted previously by the 2003 report from the Parliamentary Standing committee that was charged to look into the case for a national identity card for Canada. When they questioned, as is often asked, why so few countries do not have identity cards, they found that it hinged on the relationship between the citizen and the state.

> "The relationship between the individual and the state in Canada, the U.S., the U.K. and Australia was also discussed as a commonality that distinguishes our countries from those with a long-standing tradition of national identity card systems."[2]

We are now a few years removed from the last time there was a proposal on a national identity card in Canada. Back in 2002 the then-Minister for Citizenship and Immigration, Denis Coderre, called for a national debate on identity cards. He saw a Canadian national identity card as something that was inevitable and merely a response to the fact that 'hundreds' of other countries have ID cards.

When the Coderre case for a card was rejected the debate reduced to a mere simmer. Now, we can only hope that the rising number of other identity policy initiatives would bring the debate back to a boil. The debate that was held in 2002 and 2003 focused narrowly on the sheer existence of a card. As we have seen in other countries the card itself is merely one component of a national identity policy.

As Coderre was noted in February 2006, the need to consider these issues has not gone away:

> "We have to have a real debate on this . . . we cannot bury our head in the sand any-more. Something is going on worldwide and we have to have that debate. Three years ago we were in the avant-garde, but right now we're trailing."[3]

Indeed there is a need for a debate, but we must better understand the implications of our actions. Instead what we have are a number of initiatives taking place without any broader consideration of

2 Interim Report: A National Identity Card for Canada?, Report of the Standing Committee on Citizenship and Immigration, October 2003.

3 Denis Coderre, 'Day Proposes National ID Card', Canadian Press, February 17, 2006.

the challenges that exist. This not only gives rise to concerns about democratic process, but also because the appropriate policy alternatives may not be considered.

2. Dynamics of Identity Policy

Like most policies that involve advanced social, legal, technological, and economic issues, identity policies are complex. In this section we identify some of the challenges that are likely to emerge as identity policies are decided upon. The following overview builds on the research conducted by the Parliamentary Standing Committee as well as our own research to date into identity policies and programs in a number of countries.[4]

1. Political risks

The greatest risk run by any identity policy is political. That is, as with all policies involving personal data collection and processing, an identity policy hinges on public trust.

In almost every country when a national identity policy is first introduced, as with the Australia card in the 1980s and the UK Identity Card in recent years, public support is originally quite high. In both Australia and the UK public support was above 80%. As time goes on and problems with the policy are identified and the political and media process follows, support eventually begins to fall away.

Even in countries with national identity schemes public trust remains a strong factor and restricts change. Recent plans to 'modernize' the French identity card scheme to mimic the British plans were set on hold after consultation and numerous problems were identified by the non-governmental organization 'Le Forum des droits sur l'internet' that questioned the plans on numerous grounds and in particular how the new scheme would create a new social contract between the citizen and the state.[5] To this day that project is still on hold. Nor are all countries with identity cards equal: the UK scheme is the only one to propose a central on-line register with multiple biometrics as such a design would be considered politically unpalatable elsewhere. For instance, in Germany such a scheme would be illegal due to laws passed there in 2002 that prevent the establishment of biometric databases.

One way governments seek to avoid this political risk is through the claim that the new policies are due to international obligations or obligations established beyond the jurisdiction of the government that is introducing the policy. This is a common strategy that uses the introduction of biometric travel and border documentation as a platform for introducing changes to identity policies even in those countries with existing national schemes. This strategy is also being used in the U.S. with the REAL ID Act where states have reduced powers to question the federal statute. These strategies are only successful to a point. We have already seen controversies arise in the United States as some states have considered legislating against the REAL ID Act's implementation in their jurisdictions. With

4 c.f. 'Identity Project Report', the London School of Economics and Political Science, June 2005, http://identityproject.lse.ac.uk.

5 'Project de carte nationale d'identite electronique', un rapport part Le Forum des droits sur l'internet', 16 juin, 2005.

biometric passports governments are now realizing the political problems that are emerging from a poorly-debated policies of fingerprinting (e.g. how do we secure fingerprint data? does fingerprinting work?), and new enrolment strategies (e.g. how does the mass registration of the population actually work?). All these activities will likely give rise to significant political risks as the realities of the schemes set in.

Prime Minister Tony Blair conceded this in a speech he gave to News Corp in July 2006. Despite having successfully passed the legislation through the UK Parliament, though after a near-constitutional crisis brought upon the government by the recalcitrant House of Lords, he admitted:

> "It is, to me at least, almost incredible that the proposal to introduce an identity register in the UK should be so extraordinarily controversial. But it is."[6]

Even to this day support for the card hovers around 50% even before a single card has been paid for and issued, and there is an even more significant lack in confidence that the government can successfully deploy the scheme.

The political risks in Canada would be substantial. Research from Queen's University[7] in 2006 found that support for identity policies varied considerably around the world. For instance, 78% of French respondents agreed that everyone should have a government-issued ID card that must be carried with them at all times (with China falling behind at 77%). In Canada support was significantly lower, at 53%. In Quebec support was at 62% over. These results are not promising for a Canadian identity card policy because as we mention above, for countries without identity cards the support tends to start quite high but then falls significantly as more is learned about the details of the plans. Unlike in Australia and the UK, Canada is starting at a relatively low level of support, rendering any potential policy as being politically risky.

Another reason that strong surveyed support should be treated with caution is how the relationship between the citizen and the state may be altered, even years later. Though France has a strong acceptance rate for its ID card, it remains a source of tension. Racial disquiet and tensions between minority communities and the police lead to the riots in 2005 in the suburbs of French cities. With a national election approaching, the police union, Alliance, revealed that officers were under orders to perform fewer identity checks to avoid raising tensions.[8] There are many reports around the world of minorities being disproportionately targeted by police using their stop-and-search powers for identity checks, leading to further political troubles.

---

6 Speech to News Corps', Tony Blair, Pebble Beach, California, July 30, 2006.

7 David Lyon, Elia Zureik, and Yolande Chan, 'The Surveillance Project and the Globalization of Personal Data, available at http://www.queensu.ca/sociology/Surveillance/

8 'Battle of Gare du Nord rocks Paris', Henry Samuel, Daily Telegraph, March 29, 2007. One of the leading candidates for the election is the former minister of the interior.

Another key political issue is the confidence that citizens have in their governments to manage their personal information. The Queens University research found that less than one-third of Canadians felt that they have a lot or complete say in what happens to their personal information, compared to 60% of the French, and 67% for the Chinese. In Quebec the results were slightly higher, with over a third having confidence while less than 30% for the rest of Canada. When asked whether their own government will protect their personal information, only 48% of Canadians agreed. One conclusion that may be drawn is that Canadians are not aware of or confident in the laws that are there to protect their personal information. These numbers would likely fall, therefore, if Canadians' faith in their personal privacy were to be tested through an identity policy initiative involving significant data collection.

Similar to situations elsewhere in the world, however, the claim of 'international obligations' are still leading to changes in existing identity policies across Canada. Passports Canada is indeed planning on implementing a biometric passport, but we have been unable to find the necessary information to analyse the changes, systems, and policies.

A number of provinces have announced initiatives to 'secure' their drivers' licences to compete against the Canadian passport to provide adherence to the U.S. Government's initiatives and programs to raise the level of identity assurance at the border. For instance, the Ontario government announced in March 2007 that it would introduce security changes "guided by [the] Western Hemisphere Travel Initiative"[9] in order to maintain the ability for Ontarians to use their licences at the U.S. and Canadian border checkpoints. The announcement, and many similar announcements that have been emerging across Canada, contained no mention of privacy safeguards, however. Nor did the announcement make clear that the U.S. is requiring citizenship status to be included in any identity credential being used to travel across borders.[10] This would require the collection of new and additional information by the Transport Ministries across Canada. Meanwhile, the U.S. officials involved in the border policies remain sceptical that such a system would even comply with U.S. requirements.[11]

Even though these changes are being introduced with unlikely benefits in meeting the international obligations, none of these initiatives have been deliberated upon and debated by the Canadian publics. Plans for information sharing will likely face opposition in Canada as well. Again according to the research at Queens University, only 30% of Canadians believe that government departments should share information provided that they have given their prior consent, which is a relatively difficult task. The number of Canadian respondents who were fundamentally opposed to information

9 Ministry of Transportation, 'McGuinty Government to Introduce New Driver's Licence Card', March 9, 2007, www.mto.gov.on.ca."

10 'Pilot project in B.C., new Ont. ID offer hope for relaxed U.S. passport rules', Canadian Press, February 22, 2007.

11 'Ontario cautioned on drivers' licences: Security features might not negate U.S. demand for passports at border', Rob Ferguson, Robert Benzie and Tim Harper, The Toronto Star, February 23, 2007.

sharing was lower in Canada, however, at 15%. But when it comes to sharing information with other countries, only 4% of respondents were willing to accept 'carte blanche' information sharing, and 25% of Canadian respondents rejected outright information sharing with foreign governments.

It is possible that through these backdoor mechanisms the policies will slowly become adopted and accepted by Canadians, as they grow to be a part of the daily lives of citizens in countries with extensive identity systems. Concern may also rise about mounting identity policy gaps, such as when the Ontario Health Ministry had to admit that it was unable to identify how many of the province's 12.6 million residents are ineligible for free medical care.[12] This followed a report from the provincial Auditor General that indicated there were approximately 300,000 more health cards in circulation than the estimated population of Ontario.[13] But a policy initiative that relies on complacency as an adoption strategy is inadvisable, and potentially politically dangerous. Citizens are often adept at noticing initiatives that are ambitious and wide-ranging, particularly when they apply to the entire population.

2. Drivers

As identity policies are often introduced as an inevitable outcome of the spread of e-government, international obligations, needs to combat fraud and terrorism, and other such drivers we eventually need to scratch beneath the surface to better consider why we're introducing changes to identity and information management.

When the Parliament Standing Committee was considering the Coderre proposal they were forced to ask whether a national policy was actually required. The drivers at the time were in fact poorly considered. As with many modern identity policy proposals they seem to hinge on a number of arguments from proponents, including amongst others:

- the need to combat terrorism (e.g. the UK government argued that a third of all terrorists use multiple identities)
- the need to combat fraud (e.g. to ensure that only those who are entitled to government services may actually receive them)
- the need to combat identity theft (e.g. the growing concern about fraudulent use of identities to open accounts in other people's names)
- the need to manage borders (e.g. the implementation of biometric visa schemes and to combat illegal working)

12 'Ontario seeking excess OHIP cards', Karen Howlett, Globe and Mail, December 7, 2007.

13 Office of the Auditor General, 2006 Report: Chapter 3, section 3.08 Ontario Health Insurance Plan', p.179.

- the need to support the private sector with an adequate regime of identification (e.g. the Industry Canada principles of authentication to guide industry adoption of identification services, while also aiding industry in meeting legal requirements to identify new accounts and existing rights such as legal residence)
- the need to aid the development of electronic government services (e.g. to enable citizens to gain access to government services on-line will require some form of authentication in order to file taxes, etc.)

One growing reason for establishing identity policy is the requirement to show identity documentation in order to vote. This has become controversial as it was noted that this would exclude significant sectors of the population including the homeless, transient populations such as students[14] and tenants, or even religious communities.[15] This is despite the fact that there are no clear problems with voting fraud.[16] According to reports in the U.S., at least 11 percent of voting-age Americans, disproportionately elderly and minority voters, lack the necessary papers.[17]

These are all valid reasons to reconsider existing policies, though it is daunting to consider them all within a single policy. An open and deliberative policy process requires additional information to inform decision-making so as to best understand the type of system(s) to develop. For instance, if the over-riding goal is to adhere to international obligations then this will have deterministic effects on the form of the policy: it will involve the use of biometrics and contactless chips that contain specific and limited information regarding the individual, in accordance to international standards from United Nations bodies.

But if the purpose is to combat fraud and identity theft the nature of the policy solutions differ significantly. We first need to establish the extent of these problems to better contemplate if these drivers should be the primary consideration for the design strategy. Similarly we need to better understand the nature of benefits fraud such as health tourism to understand which government (e.g. provincial?) and which department (e.g. health ministries?) should be responsible for a proposed system. This will also go some way to shaping the political risks because traditionally the medical sector has been relatively reluctant to require too much information from applicants for fear of turning away those who are in need.

We also tend to have images of benefit fraudsters as being foreigners from far abroad, flying to Canada to expensive operations. In fact the Ontario Auditor General found that the majority of the

14 'Thousands won't have IDs to vote, MPs told: New law would leave homeless, students off list, advocates say', Tim Naumetz, Ottawa Citizen, December 6, 2006.

15 'People must identify themselves to vote: Boisclair', Tu Thanh Ha, Bertrand Marotte, and Rheal Seguin, Globe and Mail, March 22, 2007.

16 'Voter-ID law would go too far', Murray Mollard, Globe and Mail, December 13, 2006.

17 'The myth of voter fraud', Michael Waldman and Justin Levitt, Washington Post, March 29, 2007.

'extra' health cards in circulation were focused around the Toronto region, but also in regions close to the United States border.[18] Moreover there are other mechanisms that could be considered. While Ontario moved to implement photo-identity health cards in 1995, the Ministry waited until 1998 to establish a Fraud Program Branch, staffed with police inspectors and fraud examiners. This branch was never given a mandate to conduct fraud audits, nor access to files and records that would allow for monitoring, and no fraud cases have ever been referred to the Branch. It was also discovered that the Ministry had not verified the citizenship documents for 70% of all existing health-card holders. This problem was not fixed by the issuance of the new photo cards, however, as only 54% of the new card holders had their citizenship documents verified.

If we are to prioritize the drivers and their design implications we need to be certain that they stand up to scrutiny. Is health tourism in truth a serious problem or is this merely a public response to concerns about insecure borders? Do we understand the risks of identity fraud and can we understand the key areas that need to be addressed? Again these will all have different effects on the shape and form of the scheme.

Identity systems are not all built equally and they must be designed for specific purposes. We have seen a number of policy processes where the driving principles of the scheme have shifted in mid-course and this has raised the political risks of the entire scheme particularly as information is released to the public and they begin to feel as though they have been duped into believing the policy is necessary only to later find out that this may not be the case. The drop of support in the United Kingdom emerged as the UK government shifted its arguments from terrorism to identity fraud, and supporting their case through 'evidence' of the extent of identity fraud that was identified by the media as being 'inflated to play on public fears'.[19]

3. Feasibility of Goals and Realities

Once the driving principles are adequately established one needs to be certain that the scheme can in fact be developed within realistic timelines and with reasonable technologies. Can the system in fact be built to match the stated goals and objectives?

If the driving principle is to combat identity theft we must ensure that the scheme will be able to do this without actually making matters worse. This was a well-known critique of the UK scheme that proposed the creation of a single identity register that would contain the biometric information of all residents of the United Kingdom. The new register would involve the creation of a brand new database and the database would be populated by the registration of each citizen. To ensure that fraudulent identities could not be developed, the government argued that all biometrics would be

18 Office of the Auditor General, 2006 Report: Chapter 3, section 3.08 Ontario Health Insurance Plan', p.182.

19 ID fraud figures inflated to play on public fears', Richard Ford and David Charter, The Times, February 3, 2006.

required. Immediately critics began asking whether all these biometrics could actually be enrolled with sufficient accuracy to then prevent the re-enrolment by fraudsters, i.e. upon registration the register would be queried to ensure that the individual had not previously registered those fingerprints and iris scans. Uncertainty grew as to whether this level of computation was actually possible. To this day we are still unsure whether biometric technologies are adequate to this task even though a number of countries are moving to wide-spread deployment. [20]

We need to ensure whether it is realistic to rely on the creation of a new scheme altogether. Recently the UK government announced a shift in its strategy and decided to create the register instead through building on top of existing databases and data sources. While such a scheme is far more feasible from the technological point of view it calls to question the original promises made to Parliament that the identity register would be a fresh database that would not inherit the data integrity problems from earlier databases that are likely to have errant data and multiple registrations. If we do not introduce a significantly new system then we need to question the political risks of bothering at all if the same problems may continue, even if it is likely to be at a reduced scale particularly when the political process relies on promises of radical reductions in social problems.

Generally if a new policy is to build on an existing identity infrastructure and offer innovations such as the inclusion of audit trails for the enrolment process (as is required by the REAL ID Act) or additional biometrics (as is the emerging strategy across Europe) these will encounter similar problems as was identified in the UK. These shifts in existing infrastructures may not result in sufficient reductions in the problems that were originally identified and again will create scepticism as to the purposes of the scheme.

There will also be the legacy problem, which can be seen in the situation of the Ontario health card: those who hold the older health card do not have their photographs on their card, and there is no expiration date on the card so it must exist simultaneously with the new system with the photograph. Eleven years since the introduction of photo-cards, as of January 2006 there were still 5.7 million non-photo based health cards in circulation. The Ontario Auditor General has estimated that it would take until at least 2020 before all Ontarians have a photo-card.[21] This leaves the public to question the purpose of the introduction of additional measures to regulate access to the service if the existing mechanisms are still adequate.

The 'reality-problem' has many dynamics to it. For instance, if a new system is introduced, it won't have any large-scale benefits until a significant portion of the population is enrolled. But the population won't enrol until it has to, which is usually at the point of expiration of an older credential.

---

20 Home Office advisor urges biometrics testing', Tom Espiner, ZDNet UK, October 20, 2006 and 'Untested ID cards tech to go live', Steve Ranger, Silicon.com, October 23, 2006.

21 Office of the Auditor General, 2006 Report: Chapter 3, section 3.08 Ontario Health Insurance Plan', p.183.

This leads to a slow enrolment rate, and this does not provide enough incentives to agencies and other potential 'users' of the system to adapt their own systems to the new identity system. For instance, banks will not start buying new chip-readers until enough individuals hold chip-based cards. But the lack of applications for the credential doesn't create sufficient incentive for people to sign up sooner for the new credentials. If the government were to then compel large populations to sign up, e.g. ordering all teachers to enrol, the enrolment-infrastructure would have to deal with a massive influx of applicants, which will then cause queues and delays, and thus inconveniencing the population.

The alternative is to introduce a mass enrolment into the new scheme though what is called 'the big bang approach', as is being considered in Australia with its new smartcard. They plan to require the entire population to register for a new card within two years of the project going live. The new card would then expire every 7 years. This means that while the entire population would have to attend registration centres to get a new card within years 1 and 2, between years 3 and 7 these registration centres will be relatively empty as staff and buildings await the return of those who registered in year 1 as they return for their new cards in year 8. Such a policy design would be quickly ridiculed as ineffective use of public resources, and again it will introduce political risks.

With deadlines being imposed by foreign bodies (e.g. governments) upon identity systems, the burden becomes even more complex. Shortly after the U.S. Congress passed legislation requiring Canadians to have passports to fly to the U.S., which came into effect in January 2007, there was a massive surge of new passport applications. Passports Canada reported that it was experiencing a delay of 25 business days on top of the standard 20 required to process an application by mail. Some members of Parliament were getting letters from their constituents complaining of 60-day waits.[22] This links back immediately to the political risks that will likely emerge.

4. Effectiveness of the Choices

Even if the system can be built within the existing technological capabilities we still need to ask whether this is the appropriate design specification to meet what is trying to be accomplished, or whether it is merely introducing additional challenges.

In the United Kingdom, industry and government experts stepped forward to criticize the centralized approach to the design for fear that it may introduce additional vulnerabilities. That is, the government's national identity register was criticized for its use of a single register with all this sensitive information as it would provide the ideal opportunity for identity fraud on a grand scale through infiltration of the register.[23] This criticism emerged exactly at the time when the government

22 'It's too late to get a passport for March break', Unnati Gandhi, Globe and Mail, February 9, 2007.

23 'UK ID card a recipe for massive ID fraud, says Microsoft exec', John Lettice, The Register, October 18, 2005.

was changing the purpose of the scheme, and moving it away from combating terrorism towards combating identity theft.

The European Union and the U.S. both encountered this risk after they introduced changes to their passport regimes. The EU member state government decided to push an EU biometric passport through the European Parliament rather than through their own parliaments. They did this to include a fingerprint requirement in EU passports while avoiding national debate on the matter. After getting the policy through the European Parliament, policy-makers noticed that the inclusion of fingerprints in passports would mean that whenever EU citizens travel to other countries outside of the EU then these countries would by default be able to access the fingerprints of EU citizens even though this may not be a requirement. The EU eventually had to introduce a band-aid fix on this through the use of encryption. Similarly the U.S. discovered that contact-less chips would communicate the personal details of U.S. citizens without their consent, identifying U.S. citizens while they travel abroad. This generated significant public concern and the U.S. had to adopt a patch for this problem through introducing elementary access controls. All these patch-solutions decreased public confidence in the policies.

Often information-sharing is seen as a promoter of new identity policy. But this is not easily managed. The UK government decided on a new infrastructure instead of building on an existing one but this would in turn require every single government agency and every private sector partner to redesign their databases and their processes to deal with this new identifier on top of their existing identifiers. This will introduce significant political problems as every other government department would have to find the resources and the willingness to introduce changes. As stated above, this will only happen once there is sufficient take-up of the new policy, but the new policy will only be taken-up once individuals see that there is some purpose to the new system.

There are other approaches to this problem. While the French government considered the creation of a new identification card, another department in France was arguing for a more decentralized option through the creation of a 'card-wallet' that would permit individuals to hold a card that contained multiple identifiers, each one relevant to each government service they used. So the existing health-card identifier would be placed on this new card; but this information would not be relevant to the pension-department as that department has its own unique identifier that is used in its own systems, so that unique identifier would also be placed on the card-wallet. Such a decentralized scheme raises its own feasibility problems as we need to better understand who would govern the system and whether this is consistent with the political goals in introducing changes to the existing practices and schemes. Finally we would need to ask whether such a scheme justifies the creation of a new policy if it is merely a band-aid on top of the existing infrastructure.

5. Costs

Nearly all stakeholders in a debate on identity policy agree that there is probably a need for some form of innovation to meet the noble purposes outlined by proponents of policy change. When the policy is brought forward, however, an often over-riding concern is whether the resulting system is in fact cost-effective.

This is not to mean that we should let costs be the over-arching concern when considering the deployment of a new identity policy. But as with all matters of public policy we must ensure that we are introducing burdens that are commensurate to the gains, and that this is politically palatable to the affected audience. In this case, the 'affected audience' is a combination of government, industry, and the general public.

There are at least four facets of costs-consideration: costs attributed to design decisions, management of costs, opportunity costs, and costs burden.

Immediately costs are incurred due to design considerations. In the United Kingdom a significant component of the costs were due to choices in design. To prevent multiple enrolments, the scheme requires collection and processing of multiple biometrics, each of which incur significant costs (with iris scanning being the most costly at the moment). The centralized register also incurs costs particularly because of the purpose to combat identity fraud - every use of the card would have to be checked against the central register to ensure that the card is valid, and perhaps a biometrics check as well to ensure that the holder is who she says she is. The implementation of untested technologies such as contact-less chips, combined with widespread use, may incur additional costs due to a reduced life-time of the card. That is, currently British passports have a 10 year expiration but this could be reduced due to wear-and-tear on the cards and their contact-less technologies. A National Audit Office report recently found that the new chips contained in the passports had only a two-year warranty.

Similarly, the reduced lifetime of the biometric technologies may also be problematic, as technologies evolve and even as people age. Enrolment centres will have to be geographically dispersed in ways that they are not currently because people are accustomed to sending in passports in the post — which was one driving consideration for the U.S. Department of State in their rejection of fingerprints in the U.S. passport for the time being. Passports Canada only has 33 offices across the country, and relies on people mailing in their applications due to the geographic diversity of the country — so similar problems would arise here unless there is a substantial investment in new offices. Therefore, every design consideration and every additional purpose attributed to the system will have a ramification on the costs of the scheme.

The management of the costs is also significant. That is, which government administrative department will pay for the scheme? In the United Kingdom the interior ministry, the Home Office,

was behind the introduction of the Identity Cards Act. In its regulatory impact assessment the Home Office contended that the scheme would only cost £584m pounds per year to administer, and this was then rounded to £5.8bn over ten years. Contending estimates were in the range of £7 to £19bn over ten years and led to significant public controversy. Eventually it emerged that the Home Office's estimate only catered for the costs to the Home Office to administer the scheme (and even then, only the few departments in the Home Office) rather than the government as a whole. So while the purpose of the card included reducing benefits fraud, the £5.8bn figure did not cater for the costs for the Department of Work and Pensions to integrate the system into its operations and procedures in order to combat fraud. Same for the police, border officials, health departments, and so forth. At that point the government conceded that every department and ministry would have to decide for themselves whether they wished to implement the schemes and if there is a 'business case' to do so. In October 2006 the Home Office announced that the costs over the next ten years would be £5.4bn but still refused to disclose, as does any government department and ministry, the costs of implementing the scheme across the government in line with the stated purposes of the scheme.[24]

Similar dynamics emerged in the United States where the REAL ID Act is now seen as an unfunded mandate. That is, the federal government approved the bill that requires each state to introduce changes to their driving licence issuance process, to the security of the card, and the sharing of data about each card holder. Congress did not fund this initiative and instead left it to each state to implement and fund. This has generated significant concerns across the states with repeated objections from organisations such as the American Association of Motor Vehicles Agencies (AAMVA), the National Governor's Association, and the National Conference of State Legislators to voice opposition to the law. In a report released jointly by the National Governors Association, the National Conference of State Legislatures and the American Association of Motor Vehicle Administrators, state motor vehicle officials estimated it would cost more than $11 billion over five years to implement the technology required by the REAL ID Act, while an earlier Congressional Budget report had originally envisioned costs would be in the range of $20 to $100 million.[25] Now the Department of Homeland Security has estimated costs to be between $17 and $23 billion over the next ten years.[26] We look at REAL ID in greater detail later in this report.

A common political strategy for those who oppose identity policies is to question whether the costs for the scheme would not be better spent elsewhere. Accepting that these policies tend to be quite expensive, critics point to the 'opportunity costs' introduced by the scheme. That is, these funds are better being spent on other government programs. This was one of the leading strategies in the

24 Home Office, Section 37 Report from the Home Office, October 9, 2006.

25 'ID Program Will Cost States $11 Billion, Report Says', Darryl Fears, Washington Post, September 22, 2006.

26 Dep't of Homeland Security, Notice of proposed rulemaking: Minimum Standards for Driver's licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes, March 2007, page 106.

Australian debates in the 1980s where it was argued that the funds should instead be spent on health. In the 1990s in Britain, while leader of the opposition, Tony Blair questioned the Tory's proposed identity card on grounds that the money is better used in policing.

Another related strategy questions whether alternative and existing mechanisms aren't already sufficient and may be improved for a fraction of the cost. For instance, while the UK identity card could help employers enforce legal requirements to verify the immigration status of employees, this is already possible as all foreign employees are required to have visas and passports that are currently being verified and logged by employers. Instead, critics argue, the government is doing an insufficient job of applying existing measures and laws even as they consider new ones. In a sense this was the strategy pursued in the U.S., where instead of implementing a new infrastructure for a national identity card, Congress decided to 'secure' the driving licence, a *de facto* identity card.

Finally, another facet to the costs issue is who will actually have to bear the costs of the scheme. While these schemes may be expensive generally governments are reluctant to bear the full brunt of these costs. There are two predominant strategies used to share the burden, and one emerging strategy. First, as was done in the Netherlands, the government requires that citizens carry around identification papers at all times but do not mandate which form of identification this is. At the same time, they offer a voluntary card that citizens have to purchase. This way the government avoids introducing a perceived tax because it is voluntary. A second strategy is to increase the costs of issuing existing documentation, as is done in the UK, where the price of passports nearly doubled in the period between 1999 to 2009 in order to implement the biometrics required for the identity card. By so doing, citizens do not feel as though the card itself is too costly because they accept that the passport is a document that they have always paid for. Finally, an emerging strategy, again from the UK, is to charge the private sector and other government departments for their use of the card and the associated national register. Every time a bank, telephone company, or even local government agency queries data on the register or reads the card, they will be required to pay a transaction cost (currently estimated between £0.50 and £2.00). If there is sufficient buy-in (possibly enforced through regulation) then these verification-transactions can generate significant funds. The UK government estimates that eventually more than 260 government departments and 44,000 private sector agencies will want access to the register, resulting in an estimated 163m transactions per year.[27]

All these cost dynamics will have significant ramifications on the political risks to the identity policy unless carefully considered. Even the Parliamentary Standing Committee that reviewed the Coderre proposal worried about mounting costs. Costs should not be an over-riding concern for any government policy but it is a predominant concern throughout deliberations over a policy.

27 Home Office presentation to industry, 'Procurement Strategy Market Soundings', Identity Cards Programme, Home Office, October 2005.

6. Who decides the policy and owns the system?

Related to the issue of costs management is the issue of policy-ownership. Whoever has ownership of the policy will likely give rise to specific political, design, and cost risks.

A predominant concern in Canada is whether a new policy would be 'owned' by the federal government or the provinces. If it relied on the federal government to introduce the mandate the provinces could be left to shoulder the burden of the policy, as is the case with the REAL ID Act in the U.S. with the federal mandate but state implementation requirements. As discussed above, this decision will have significant budgetary implications.

Even the choice of ministry can lead to risks. A policy introduced by a ministry responsible for immigration will give rise to concerns that the policy is out to surveil immigrants. There are also design considerations: a policy owned by the policing arm of government tends to be focused on policing; a policy from the Treasury tends to focus on managing employment and taxation. For instance, one of the reasons to include fingerprints in the UK identity card is because the Home Office is hoping to identify the 900,000 fingerprints that have been found at scenes of crimes over the years but not yet resulted in matches on the database of fingerprints of criminals. The scheme is thus seen as being design for policing purposes rather than for administration of government services; and this may reduce confidence in the scheme.

Of course it is dangerous to approach the design of the scheme in such a deterministic way of 'who owns it designs it in his interests'. But an interesting example of this emerges from France: when the ministry for state reform recommended a policy it called for a federated scheme that would serve the interests of the citizen and the existing practices of each government department; but when the ministry of interior called for a new policy it was recommending one similar to the UK Identity Cards Act with a heavy biometrics component, a single identifier and a centralized register.

The prospects in Canada, based on recent developments, are more complex than the situation in the UK. The UK has only one single issuer of driver's licences, health cards, tax numbers, etc. In Canada, as with the U.S., the situation is much more fragmented. Social Insurance Numbers are issued by one body, but driver's licences and health cards are issued and managed by the provinces. Recent policy proposals and changes have focused primarily on the developments in the provinces, particularly in driver's licences, mostly to avoid the reliance upon the more expensive and difficult to administer passport infrastructure. But if licences are to be used more and more as general purpose identification credentials, the issuance agencies will have to begin collecting more and more data (e.g. citizenship status), which carries significant costs. Below we look into the U.S. case as an illustration of what Canada may yet encounter, and how this links up with political risks yet again.

7. How does the system regard privacy and civil liberties?

A predominant concern with the introduction of a national identity policy is the risks it poses to privacy and civil liberties. For instance, to those without identity cards, they conjure images of oppressive and discriminatory governments. Practically every government considers these issues within their policy, but how well they consider it in their design and implementation will influence the level of risk that is likely to arise.

The use of central registries with audit trails, compulsory registration powers, compulsion to identify, extensive use and re-use of personal data and biometrics, and the extent of user-control over the system are key considerations for privacy and civil liberties. Each policy weighs these components differently and this in turn has significant effects on the political risks. For instance, though Germany has a long history of national identity cards and is now implementing biometric passports it has restricted the storage of biometrics in a single register due to fears of abuse. In fact, in their adherence to EU policy on the issue the Germans are insisting that their passports will only contain two fingerprint images and these will only support 1-1 verification, i.e. without a verification against a central register. The French and the British are interpreting the EU requirements differently, by requiring between 8 and ten fingerprint images. Amongst others, Spain and the U.S. have rejected this approach.

The UK did offer an innovation to promote privacy: the creation of an office of the Identity Commissioner who would oversee the privacy implications for the scheme to ensure that there is no abuse of the scheme. It remains to be seen if this will increase public confidence particularly since the design of the scheme is the most invasive seen yet with a central register that logs every verification in such a way that the audit logs will show every single transaction done by the individual with that card (e.g. every time it was verified at a border, at a hospital, at a benefits agency, by a bank, etc.) and essentially mapping out many of the actions that constitute the daily life of an individual. The UK government contends that this will empower the citizen because the citizen will be able to verify this audit trail to see whether a bank, benefits agency, or hospital has access his personal details to ensure that there is no abuse. The result of this debate remains to be seen but the UK government policy does run a significant risk of being seen as privacy-invasive in ways that other countries' governments have managed to avoid.

Canadians are said to value their privacy, and this has been validated through numerous polls and surveys. They are also quite concerned about the processing of their personal data. Identity policies are amongst the greatest recent challenges to promoting, enhancing, and safeguarding privacy. Identity policies can enable or prevent the collection, processing and sharing of personal information across government departments, and even with the private sector. Considering all the other challenges and risks of identity policies, it is likely that privacy may yet produce the largest political risk in the Canadian context.

Case: REAL ID [28]

Americans are generally opposed to ID cards and have rejected all prior proposals to implement such a system, but in February 2005 the U.S. House of Representatives approved H.R. 418, the REAL ID Act. It became law in May 2005 following unanimous approval in the Senate after it had been attached to a funding bill for the military operations in Iraq, and Tsunami relief. Until this point, the legislation had encountered significant opposition from politicians and groups from across the political spectrum.

A relevant aim of the law is to establish and rapidly implement regulations both for State drivers' licenses and for identification document security standards. The law requires States to deny drivers' licenses to undocumented immigrants: this requirement is seen as moving the license into the realm of a national ID card.

According to the American Immigration Lawyers Association:

> "Preventing immigrants from obtaining driver's licenses undermines national security by pushing people into the shadows and fueling the black market for fraudulent identification documents. Moreover, it undermines the law enforcement utility of Department of Motor Vehicle databases by limiting rather than expanding the data on individuals residing in a particular state. Perhaps more to the point, it is clear from the 9/11 and Terrorist Travel staff report that the proposed restrictions would not have prevented a single hijacker from obtaining a driver's license or boarding a plane. (...) The terrorists did not need US-issued driver's licenses to board the planes on September 11; they had foreign passports that allowed them to board airplanes. Use of foreign passports to board airplanes would still be permitted under this provision."[29]

The Act also requires that States sign up to the interstate compact for sharing licensing information. The database that is generated under this regime will also be shared with Mexico and Canada. The card data elements include: Full legal name, Date of birth, Gender, License or ID card number, Digital photograph, Principal residence address, and Signature, all of which are required by legislation to be held in the database.

REAL ID requires that federal agencies refuse any drivers' license that does not meet minimum document requirements and issuance standards, including verification of immigration status. As a result, temporary residents in the U.S. will only get a driver's license that is valid until their authorized

28 This section was aided by the participation of the ACLU in the Vancouver workshop.

29 American Immigration Lawyers Association, The REAL ID Act of 2005: Summary and Selected Analysis of Provisions, January 27, 2005, http://www.aila.org/contentViewer.aspx?bc=10,911,5516,8191.

period of stay expires. For all other non-citizens, licenses will be valid for only one year. This introduces significant burdens upon driver's and vehicle licencing authorities (DVLAs).

Though it is presented as a 'voluntary' scheme, in that states can refuse to take part, if a state does refuse, that state driver's licenses and state ID cards will not be accepted for "federal purposes" – including boarding an aircraft or entering a federal facility – unless they meet all of the law's numerous conditions, which include: card data elements and security features, a machine readable zone, a 50-state inter-linked database, 'breeder document' (aka foundation document) standards, verification of these documents, and other administrative requirements.

There are fears voiced by civil liberties groups in the U.S. that REAL ID would violate privacy by helping to consolidate data, facilitate tracking and could lead to discrimination.

CONSOLIDATE: National IDs would violate privacy by helping to consolidate data. There is an enormous and ever-increasing amount of data being collected about Americans today by everyone from grocery stores to online retailers. This can be an invasion of privacy, but privacy has actually been protected by the fact that all this information still remains scattered across many different databases. But once the government, landlords, employers, or other powerful forces gain the ability to draw together all this information, privacy could be compromised, and it was argued that that this is exactly what a national identity system would facilitate.

TRACKING: A national ID like REAL ID would also facilitate tracking. When a police officer or security guard scans an individual's ID card with his pocket bar-code reader, for example, it will likely create a permanent record of that check, including the time and your location. The end result could be a situation where citizens' movements inside their own country are monitored and recorded through what is now tantamount to "internal passports."

DISCRIMINATION: The emergence of a National ID will foster new forms of discrimination and harassment of anyone perceived as looking or sounding "foreign." Latinos, Asians, Caribbeans and other minorities will became subject to ceaseless status and identity checks from police, banks, merchants and others. Failure to carry a national ID card would likely come to be viewed as a reason for search, detention or arrest of minorities. The stigma and humiliation of constantly having to prove that they are Americans or legal immigrants would weigh heavily on such groups.

According to a `National Impact Analysis' from the National Governors Association, the National Conference of State Legislatures, and the American Association of Motor Vehicle Administrators,

noted above, the costs could reach in excess of $11 billion USD over a five year period. According to other reports, the costs could mushroom to $23.1 billion over a ten-year period.[30]

The political opposition to REAL ID is growing, on both the costs and privacy implications of the system. There are also concerns that it would actually increase identity theft, and could cause the increased collection of personal data by private sector organisations. There are even legislative proposals to repeal the act. State legislators in Maine and Idaho have rejected participation in REAL ID. Prior deadlines have had to be extended and there are concerns that the full fledged system will never get implemented. This is remarkable for a piece of legislation that was once unanimously approved by the U.S. Senate.

30 'Senators skeptical of REAL ID Act rules', Anne Broache, News.com, March 27, 2007.

3. Benefits of a National Identity Policy Framework

Canada is in the midst, as one observer described it, of a 'perfect storm' of activity that is leading to an increased focus on identity within information management activities. Though this is an emergent area of interest, there have been a number of earlier activities that now act as the building blocks for current thinking about how to approach identity.

Countless generations of credentials have been issued by governments, companies and groups, usually in the form of identity cards, security passes, memberships cards and passports, often reliant upon some form of identity verification and vetting processes that use biographical, biometric and/or personal information. The growth of computing gave rise to renewed concerns regarding authorization rights and profiles, linking roles with privileges. Combined with the spread of computer networking issues, renewed interest in authentication emerged as more people focused on how individuals could assert their rights within these privileges.

With concerns about financial, national and commercial security, all stakeholders needed to find a solution to the problem of confidence. How can confidence in our transactions be ensured in the age of global communications, travel and trade? Since the 1990s there has been a flurry of activity at the consumer, business and government levels to deal with the issue of identity assurance to ascertain the level of confidence one needs in a claimed identity for a specific context and transaction. In a number of countries this led to coalitions of government departments, business and consumer groups working together to look into how credentialing, identification, authorization and authentication could work across multiple systems and business contexts. Working together towards a national identity infrastructure could prove beneficial to all these parties, and has led to confidence-enabling policy regimes and standards abroad.

Why identity assurance is important

The establishment of a national identity assurance infrastructure for Canada may, even at this late stage, prove highly beneficial to the needs of business. For example U.S. studies have shown that as many as 30% of U.S. adults have changed their online behaviour due to fears of identity fraud, while some have even stopped shopping on-line, resulting in billions of dollars in lost business. Similar data from Europe has shown that data protection, privacy and security concerns are among the top barriers to shopping online. Solutions are required to increase consumer confidence, and global co-operation is required in the search for technology and regulatory aids. These findings also show that consumers need support to repair their identity after a crime or other identity breach. If the necessary support and protections arise then increased confidence may yet emerge.

Business generally has a pragmatic approach to identity. Seeking absolute knowledge in the identity proofing and vetting in all these domains is beyond the realm of reality for many organisations. More pragmatic approaches generally involve the balancing of trust, convenience and risk, accepting that there is a threshold of tolerance for error, while there is also a threshold for the tolerance of inconvenience. Companies generally have to balance the efficiencies gained from sophisticated identity schemes against the level of fraud that is being prevented. Thus a sophisticated approach to understanding organizational needs is often required before the introduction of advanced policies and technologies. As one commentator put to us, "identity assurance needs to be 'good enough' to solve today's problems without getting caught gazing at 'blue sky' solutions." Often the example of credit cards emerges, where credit card companies understand that consumers and merchants are not interested in sophisticated forms of identity assurance if they are inconvenient. As a result, credit card companies have incorporated the risk of fraud into their business models. It is no surprise, therefore, that credit card companies have never proposed a comprehensive identity scheme with onerous registration processes.

The growth in concern and interest in the identity space highlights an increasingly complex field for policy, regulation and technology. The growth of legal compliance for employment management (e.g. immigration verification, criminal records verification) has driven a significant level of activity by employers, likely also due to concerns regarding the mobility of labour. As employees work across boundaries, whether geographic or organizational, solutions are being sought to maintain efficiency gains from working in an 'e-trust' environment that must comply with numerous policies. Meanwhile, many companies, particularly in the finance sector, have encountered more extensive regulations on customer authentication through 'Know Your Customer' requirements imposed to deter fraudulence and such illegal activities as money laundering.

This environment introduces a delicate balancing act for companies. Apart from the efficiencies vs. fraud balance, companies must also consider compliance risks through the pursuit of due diligence. They must take on additional verification procedures and processes that may go well beyond their original organizational risk assessments.

The increased attention to identity management introduced by regulatory activity should not be interpreted solely as an economic loss. Public trust and confidence may be raised through the deployment of effective identity assurance mechanisms, and this activity may actually lead to more advanced business models. If again we look at the example of the credit card industry, new techniques of authentication have been introduced around the world (e.g. chip and pin payment mechanisms), and new business models have also emerged (e.g. identity theft insurance and credit checking services) even within this highly regulated environment.

Competitive advantage may yet emerge through the advanced deployment of identity assurance policies and management practices. As businesses learn to find new ways to manage risk and make

use of information they hold on consumers, and as businesses find new ways to interoperate with other organisations, the balancing act of efficiency vs. risk becomes even more sophisticated. New models of doing business may evolve from this.

Policy leadership is required from which regulation can steer activities through consultation and the creation of compelling argument for change, in turn guiding behaviour. Following on from examples we have seen in other countries where identity cards are nurtured not only for use in the private sector, but also where consultative processes are established to develop and promote authentication principles and assurance best practices.

A national infrastructure is much more than mere technology, and is instead also a forum where decisions and policy may be made regarding security, liability, shared experiences, practices and lessons; but must also nurture a myriad of other emerging techniques, practices and technologies. It has, for example, been argued that the spectrum for mobile communications, along with utilization of handset technology, would provide an ideal and convenient platform within an identity architecture. More such opportunities may emerge that will shape both government and business practices and institutions. A truly effective national identity infrastructure will shy away from monopolies that focus only on governments' needs and will instead look to how a policy regime can be established to cultivate and nurture identity assurance across the Canadian economy.

Uses for Identity Assurance in Various Sectors

Business sectors are increasingly aware of the need for identity assurance. Companies are collecting increased amounts of personal information relating to their employees, their clients and collaborating organisations. As businesses become more aware of the need to manage their information assets in light of new business practices and new regulatory requirements, they are likely to seek new solutions for identity assurance.

Although there is increasing awareness of the role of identity within the business community, some of the recent attention on identity has focused on legal compliance. While this approach has been helpful at raising the issue of identity management, it has not taken the dialogue as far as it should--to the extent of including identity into business practices as an opportunity.

Compliance

In the area of identity assurance, pressing compliance issues surround the area of fraudulent activity, problematic accounts and hiring practices.

Fraud and fraudulent activity has emerged as one of the urgent challenges for legal compliance. With increased public concerns about identity fraud, businesses and policy-makers are calling on increased support for compliance with the law. Identity assurance has a key role to play in this respect.

Some of the attention regarding identity fraud has focused on the banking and payments sector. In this sector there are a number of forms of identity fraud, including card fraud, check fraud and online fraud.

The larger scale crime occurring in this sector is identity fraud, where a person applies for an account in someone else's name, or conducts a take-over of an account through stealing and redirecting post and conducting transactions in someone else's name.

Regarding regulatory compliance and identity assurance in the financial sector, it is important to note that identity assurance is merely one part of the solution. As the Chairman of the UK Financial Services Authority announced in 2005:

> "We have given – repeatedly and I hope clearly – the message that we expect firms to manage their money laundering risks effectively by placing less emphasis on ID and using the full range of [Anti-Money Laundering] tools."

This statement follows a criticism made by the UK's Better Regulation Task Force, referring to the increased identification requirements as 'creeping regulation'.

> "Last year many of us found our banks writing to us to ask for proof of our identity, even when we had held accounts with them for many years. It's unclear where this requirement came from, and this is one of the examples that we will be investigating in our study on regulatory creep."

In fact the Better Regulation Task Force has repeatedly drawn attention to the poorly formed presentation of the case for identity checks that would introduce an additional layer of red tape.

Alternative solutions have emerged to solve some of the problems, including:

- behavioural profiling on accounts to reduce fraudulent activity, particularly in card transactions.
- chip and pin to ensure that there is some 'secret data' involved in transactions that are not necessarily visible on the card (replacing the previous signature-based transaction)
- additional credential verification for credit card purchases online including (1) Address Verification System/Card Security Code (AVS/CSC) that allows for verification of credit cards for the accurate billing address, and (2) SecureCode from Mastercard and Verified by Visa are more global schemes that require additional authorization
- increased online verifications where a card is verified in real-time to be active, with the additional safeguard of the Industry Hot Card File (IHCF).

In the UK there have also been calls for the release of a list of 'deceased' records to prevent accounts being opened fraudulently. This appears similar to the National Routing Service that is being discussed within Statistics Canada.

Opportunity

The incentives for a truly national identity assurance infrastructure requires more than mere compliance with laws that mandate assurance. Users need to be convinced that there are many benefits to paying attention to identity assurance. In the case of the private sector, legal compliance alone is often an inadequate reason to change processes, procedures and technologies.

We often forget that legislation is just one response to a condition within an environment. For instance, concern is expressed about fraud, and so legislation is set in place. But the concern about fraud is also symptomatic of a larger problem with the need to manage information within organisations.

Identity assurance can very well improve the state of the Canadian economy, and in some cases there can be substantial improvements achieved.

Areas for improvement in identity management include:

- The introduction of risk management and liability management regimes within the private sector. We have already seen a number of solutions emerge from the private sector to reduce identity fraud, such as through online verifications, the use of chip and pin, and well-circulated lists of stolen cards. In our consultation we were repeatedly reminded how credit card companies have long managed the problems of fraud and criminality in the use of credit cards by including the risk of loss and abuse within their business models. We have also noted the entry into the marketplace by information aggregators who promise to deliver information to consumers so that they can themselves monitor fraudulent activity perpetrated in their names.

- In a world with global movement of the workforce and an increasing use of contractors who are self-employed and who work outside of the office environment (e.g. at home) more sophisticated regimes for identity assurance may be required. An entire industry could emerge from the vetting of job applicants' qualifications to ensure that the applicant indeed has the requisite skills. Companies will also need to develop more sophisticated identity assurance techniques for mobile employees who may work from many places around the globe, and may never actually enter the formal office environment. This must occur even as enterprises learn to find ways to join up their databases and manage their employees' authorizations more effectively.

- More sophisticated customer management regimes will continue to emerge. With the advent of on-line marketplaces such as eBay we have seen how individuals may create multiple pseudonymous credentials but have verifiable chains of authorizations to conduct business without having to divulge too much personal information. Meanwhile, more sophisticated use of identity assurance may permit businesses to personalize product and service delivery while enhancing the autonomy and flexibility of their customers. Pay-as-you-go regimes have proven that this flexibility is required, and identity assurance mechanisms should proceed in step, e.g. to permit 24/7 or on-line upgrades and account top-ups.

Economic Benefits of Leading a National Discussion

To date much of the discussion of identity assurance has resided only within the Federal government, and within some provincial governments. Meanwhile, Industry Canada has been leading discussions about authentication principles, bringing together government and the private sector, along with non-governmental organisations and academia. This could be a model approach to starting a discussion within Canada on the issues and potential benefits of identity assurance particularly in organizational settings.

Through our consultations with key UK and Canadian experts and organisations in this domain we were able to gain access to some of their findings and estimates.

The enhanced ability for employers to discern appropriate applicants and authorize their employees for the appropriate tasks could provide substantial benefits to the Canadian economy.

Previously identities were created by many departments (Human Resources, Finance, IT support, etc.), and sometimes in many regional locations and for different purposes. In fact these identities were often stored physically in a number of different places on different platforms. As users moved from place to place and job to job during their careers, and as processes affecting them (the facts linked to them) grow in volume and importance so too does the cost of maintaining them. This cost has been hidden somewhat thanks to being distributed across an organisation.

If organisations were able to improve the effectiveness of identity management, through a single enterprise directory, this could lead to substantial cost savings and efficiency gains. Critical transactions tied to a simplified and streamlined process will occur faster, generating additional market opportunities and therefore additional revenue and taxes. There exists a by-product that arises from bringing more structural emphasis on having one user across functions and boundaries, whether organizational or geographical, which is that businesses are forced to better understand the way in which users cross service silos and therefore eliminate redundancies in process. Processes that were previously impossible, or had latency built-in as they crossed business domain boundaries, are rendered faster and more convenient for users. As well as the direct administration advantage this represents an indirect (but directly associated) cost and service (or revenue) gain.

In turn, businesses would no longer have to build authentication processes into every application because the identity issuer will do that for them. Furthermore, as long as end-point security and access control is properly managed the possibility is opened up for transacting across public networks and in open communities because greater certainty as to the exact parties in a given transaction, and the encryption of data between them allows for the use of non-proprietary systems.

This also opens the possibility of sharing services between organisations whose primary emphasis becomes one of knowing the user and the context in their specific transaction relationship, rather than "defending the boundary" and tightly containing transactions within an application or domain. By introducing descriptive facts such as a change in status or social condition (such as the loss of a job) into business decisions may reduce risk and loss. The scale of web-enabled business and the volume of information transactions across networks is now allowing us to develop a more statistically relevant view of on average how many incidents are likely to occur as a result of failure to apply responsible approaches to identity assurance, and what the impact of an average "event" will be.

Likewise, pattern matching through combining statistically relevant data points together to draw conclusions at the network layer, which allows organisations to generalise intelligence around user-centric transactions, can calculate the risk that any given user is not who they say they are. For low risk and or low value information exchanges this can even avoid the intrusive and expensive need for active authentication.

If identity and authentication processes were universal, corporations would not have to invest in a suite of products in a layered environment to protect against fraud. Annual spending in this domain is already in the billions.

As a result of these changes in organizational practices, tens, even hundreds, of dollars per user per annum of direct cost can be saved, depending on the degree of improvement towards complete identity assurance compared with existing structures and approaches. According to studies undertaken by British Telecom, one of the largest firms in the UK, the implementation of such a scheme within their own organisation saved the firm £88m per year. The firm identified a variety of benefits including:

- Administration: Labour expenses to provide electronic access (identity, credential, privilege, and account configuration), supply resources and manage passwords.
- Lost Productivity: Paid for but not effective end-user hours waiting for access and resources, or waiting for password reactivation.
- Assets: Capital write-off and cash exposure (such as monthly cell phone or pager accounts not closed) assigned to terminating users.

The firm concluded that:

- Looking at 'hard benefits', through Improved IT efficiency, reduced help desk cost, and quicker access, the firm calculated savings of over £300 per user.
- If 'soft benefits' including IT Cost Reduction, User Admin Cost Reduction, Increased User Productivity, and Asset Management benefits were included, the annual benefit per employee can reach as high as £1900.

It is important to note that there are necessary costs in implementing these types of solutions that may erode some of the benefits. A number of oversight and support organisations will be required, including a Security Office, Regulatory Audit and Compliance Office, Privacy Office and help/support desk.

Separate from satisfying the current legal requirements upon organisations, there are other benefits to implementing identity assurance schemes. Sufficient thought about identity management and how it can be integrated into business and commercial transactions could lead to even larger gains by reducing fraud and increasing both consumer convenience and confidence. If properly implemented, this could result in reduced threats of impersonation and identity fraud, which has substantial financial impact if processes are integrated to leverage maintained descriptive facts.

Depending on circumstances, if applications are tiered for their sensitivity, many of the things a user does frequently may not require any real time access control whatsoever avoiding associated administrative processes, and making the navigation of the session very easy even as the user engages multiple businesses. On top of this, the business process between companies that do not even have a relationship could be integrated. For instance, the user could order a retail vendor to debit a checking account at the bank named as a descriptive fact tied to the identity to trigger funds transfer before the session terminates, or the vendor could confirm payment prior to launching a shipment process. Avoiding redo and process confusion would reduce some internal costs. According to our discussions with experts, citizens and consumers already have on average around 1,000 different identity registrations each stored in a wide variety of places for a wide variety of purposes.

This is not to say that a centralised solution is necessarily the ideal solution. The marketplace is littered with the remnants of fallen companies and failed ideas that promoted highly centralised identity management solutions. As is the international landscape.

Lessons from Abroad

Other countries and environments have long been conducting the necessary dialogue and research into identity assurance practices, procedures and techniques. We can learn from their experiences.

Sweden

The Swedish approach shows how much of the technological and development risk can be carried by the private sector through negotiated solutions with the public sector.[31] Swedish citizens are active on-line users. For instance, in 2005 the number of income tax declarations performed electronically doubled to a third of all declarations.

Instead of issuing a unique identifier for all e-government services, Sweden opted for a market driven approach integrating standards from the private sector. With this model, private vendors rather than government agencies have carried the heavy investments. The market-led electronic identification procurement policy has no upper limit for suppliers thus, in principle, forcing government agencies to accept multiple software clients and electronic identification certificates. In practice however, the multitude of standards has not materialized as most suppliers use the same formats. When designing the software, particular attention has been paid to compatibility and hence the electronic identification solutions used in private banking services are accepted for government services and vice versa. As a result, more than 5 million Swedish electronic banking customers can now use their electronic identification to access the various services offered by both central and local government agencies as well as private businesses.

The electronic identification solution is based on a certificate that is stored on the citizen's computer or a smart-card solution where the information is stored on a credit card sized piece of hardware. The Swedish Agency for Public Management (Statskontoret) has signed an agreement for implementing a standard electronic signature with the six largest banks. Citizens who have online access to their bank account can freely download the software. The hardware solution is offered by the telecom operator Telia Sonera and the largest Nordic retail bank Nordea Bank. Nordea bank also offers their credit card account-holders a chip-based credit card that can also carry the electronic identity used for government services. The suppliers of the certificate are paid every time an identity assurance service is used.

Challenges remain in this market-led solution. As government agencies pay vendors per transaction, the cost of new services is difficult to discern, and thus agencies lose the incentive to introduce new services because of the higher financial risk involved. To mitigate this, the Swedish Agency for Public Management has struck an arrangement with a number of private vendors to supply verification services at a fixed cost. The deal only covers the largest agencies and regions, and hundreds of agencies and municipalities still have to pay per transaction, but it is not however expected to create major disruption in the innovation of new electronic services.

31 Status Report from the 24/7 Agency Delegation, 'E-identification for secure –services, February 2005.

Hong Kong

The Hong Kong case shows how a limited-purpose strategy for identity assurance can be expanded into a national infrastructure. The Hong Kong ID card was initially introduced as a measure to deal with immigration and border control, in particular to manage the large temporary population and mass tourist flow from Taiwan. Policy-makers envisioned an expansive scheme, however, and as a result they implemented an advanced smartcard-based scheme as it cost only 10% more than the less flexible model and could be used eventually across multiple government services. The card itself only holds minimal data while the remaining data is held in a number of government databases.

This ability to include additional services on the card has enabled a number of other programs to make use of the identity infrastructure. The Hong Kong Post is now using the card, as it added an "e-Cert" option by which the card could be used to create digital signatures. Card-holders can visit kiosks located around the city to update the extra e-Cert information accessed by the card. In turn, online banking, stock trading, and on-line payments are thus enabled and made more secure and convenient.

Malaysia

Malaysia has an advanced identity card that has branched out in an attempt to become the core component of a national identity assurance infrastructure, but there were some obstacles on that path. Malaysia has long had a national ID card, but in 2001 moved towards a smartcard scheme to replace both the older ID card and the driving licence. The card is called ‘MyKad’, or Malaysian Card, and is also referred to as the Government Multi-Purpose Card.

The chip on the card originally had a 32k memory storage, but the next generation card consists of a 64k chip. The card is voluntary, and as a result the government has found it difficult to convince citizens to upgrade to the new chip-card, and went so far as to introduce a lottery-prize system for those who applied for the new cards (though this was recently abandoned). The new card's capacity would permit the storage of multiple certificates, issued for specific government services. The chip contains a thumbprint and other personal information, including basic health information. The plans were that the card would be used to pay road tolls, to access automated teller machines and also act as an electronic-purse. As a result, the card would be more of a 'wallet', acting as a national ID, passport, driving licence, health card, an e-Purse and ATM card, to enable contactless road tolling by placing the card into a transponder in the vehicle, and finally to enable remote authentication using a digital certificate. It also has the option for a payments scheme called 'Touch n' Go' where money can be loaded onto the card at a bank and then used for small payments.

The private sector has been reluctant to integrate their cards into the 'wallet' because of security concerns. Banks have dissuaded customers from using the card for banking purposes due to the same issue. Card-holders were also concerned that if they lost their identity card they would also

lose access to their bank accounts. Instead, banks have added functionality to banking cards to make them more appealing. Similarly, according to reports, Malaysian police have insisted on asking for driving licences instead of the identity card because they lack the readers necessary to scan the driving licence credential off the smartcard. Less than 15% of the population have added the licencing functionality to their card. Also, reports indicate that few hospitals have the capacity to read the data.

Despite this, however, there are plans to implement digital signature technologies on the card to enable on-line transactions. There are also plans to introduce loyalty schemes for retailers to link to the card.

Other cases

In our discussions with experts from across Canada and around the world, we were informed of other world-leading processes that we were unable to properly research and report here and we recommend further research on these: Norway, New Zealand, Asian APEC countries and the U.S. and its work through the Federal Trade Commission.

Conclusions

There are many benefits to beginning a national discussion on the need for effective identity policies across Canada. We are not proposing the creation of a national system, but rather we need to look at how various public and private sector initiatives can thrive in a multi-purpose, multi-identity landscape. That is, just because we are able to identify advantages and benefits to establishing a national identity policy framework does not mean that a centralised solution through a national policy decided by government will actually lead immediately to these benefits. More work at the ground-level is required, within organizational, commercial, and consumer- and citizen-facing environments.

The main problem with government efforts to create centralized identity architectures is they are based on enterprise architectures for identity and access management. Enterprise architectures centrally house the capability to electronically trace and profile all participants. This gives the enterprise the power to provide and monitor access by employees (and possibly “extended” user groups who access corporate resources, such as suppliers) to their corporate resources from a central location, and to centrally shut down all their access rights in case they leave the company.

Applying such a model to the government-citizen relationship would be problematic. Instead we can start coming up with solutions that are compatible with citizen-government, consumer-business, and intra- and inter-business relationships. The core questions that remain include: can this be done in Canada? Is there a sense of need and momentum behind this, or are we only going down the path of reconsidering the 2003 proposal for an ID card?

4. Research Workshops and Consultations

As part of our research process we conducted outreach and consultation to a number of experts across Canada. This report builds on workshops held in Vancouver and Ottawa, as well as indirectly on one held in Toronto June 2006, before the project formally began.

Within this project we ran two workshops to reach out to various government departments, industry sectors, stakeholders, and experts in order to bring their experiences in to frame discussion on the issue of identity policy. A discussion paper was circulated at each workshop with our initial findings and statements of challenges and opportunities, and following short presentations from the project team members we heard from participants in formal and informal presentations throughout the 5-hour sessions. Breakout groups were organized for specific tasks and the groups then reported back to the full group, followed by some discussion. The workshops concluded by establishing a number of points that the researchers could take away with them to future workshops and to the final report.

The Vancouver workshop was organized in association with the British Columbia Civil Liberties Association and the American Civil Liberties Union. The event was held at Simon Fraser University's Harbour Centre campus, on December 8, 2006. The goals of this workshop were to:

- Understand the plans for new border controls and the practical implications.
- Grasp the challenges introduced by REAL ID and other new identity standards.
- Assess the economic and cultural repercussions of changing legal conditions.
- Explore the privacy, security, and technological challenges to these new developments.

There were over twenty participants in this workshop, ranging from academia, civil liberties organisations, offices of provincial privacy commissioners, and provincial ministries from Alberta and British Columbia.

The Ottawa workshop was organized in association with the Canadian Internet Policy and Public Interest Clinic at the University of Ottawa, held on January 12, 2006. This workshop focused more on the activities of the Canadian Federal Government, and the goals of this workshop were to:

- Analyse the drivers for a national identity policy.
- Understand the changes to the Canadian Passport and explore changes to other travel and immigration documents.
- Build on the work of Industry Canada on authentication principles.

- Explore the challenges and risks in increased data-sharing.

Discuss the privacy, security, and technological challenges to these new developments.

There were nearly thirty participants in this workshop, ranging from academia, civil liberties organisations, provincial privacy commission representatives, and federal ministry officials.

These workshops played integral roles in informing our research and shaping the outcome of this report, but we do not claim to represent the ideas and opinions of those who participated in our events.

These results presented below were accumulated through a round-table discussion as well as through breakout discussions. They do not intend to present a consensus of the group or any of the individuals involved.

One useful analytical point that was raised from the earlier Vancouver workshop was that we needed to separate the practical and the strategic challenges. As a result our presentation of the findings of the workshops breaks these results into these two categories, though the sub-categories were identified by the researchers in the analysis stage of this research.

Strategic Issues

The discussions around 'strategic issues' looked primarily at the more abstract concepts of what are the identity policy dynamics, the variety of drivers for identity policies, the political issues surrounding policy making, the processes through which policies could be devised, and the implications for data-sharing and privacy.

Conceptual

Early on in the workshops there was some discussion about the nature of a policy on identity. There were a wide variety of ideas circulated on the constitution of an identity policy. For instance, it was argued that this process should not be about a single identity policy or identity system. Similarly, it was argued that the term 'National ID card' was also too deterministic and complex, and instead we should focus on the 'national identity system' or a 'national identity policy'. The conclusion of this strand of thought is that we need to consider the possibility of multiple identity policies and devise strategies for managing multiple systems. After all, there are a variety of levels of risk depending on the specific application of identity (e.g. medical vs. financial transactions). There is no one-size-fits all solution, and therefore a set of policies and systems will be required.

On a more specific level, it was argued that we need to distinguish whether we are talking about identity-verification or uniqueness assurance. That is, uniqueness is concerned with discerning whether a customer is a unique individual, and is not necessarily reliant on verifying the identity of this particular individual. Identity verification is more concerned with proving that individuals are who

they say they are. Indeed there are more variations on the degree of identity specificity, such as anonymity and pseudonymity, both of which in turn have varying degrees.

One theme that continually resurfaced was that perhaps there shouldn't be a national identity policy at all. Instead, it was argued that what Canada needs to do is understand that identity is an issue that is context-based — and that a national policy may be oxymoronic. In fact, it was argued that perhaps a piecemeal approach to identity policy is not necessarily problematic and may in fact be ideal. This piecemeal approach through multiple policies of multiple schemes, both small and large, could mitigate the risks that are often associated with large-scale national schemes because of the incremental steps taken to establish these smaller and multiple schemes that are designed to deal with specific problems and situations.

One particularly interesting theme that emerged was that in fact the entire discipline of identity management is overly abstract and does not reflect the way identity functions in the 'real world'. That is, we lack a good intellectual grasp of how people enact their identities in everyday circumstances. Without this understanding we will never be able to build functioning grand architectures of identity.

There was unease regarding the growing sense of inevitability around a national identity system. Historically, large-scale identity management was for management of large populations of criminals, soldiers, or colonists. The purpose of these systems was to identify undesirable and inadmissible elements within the population, and usually erupted into political troubles. Now we are considering policy imagining similar benefits, e.g. managing immigration, welfare, and fraud. Therefore we must be prepared for the potential ramifications of these systems.

The need for an identity policy

Many participants in our workshops identified concerns over the need for a scheme. Even in organizing the workshops a number of potential participants voiced their concerns in joining in such discussions because they feared that we would come out in favour of a national policy while the participants remained concerned that there was no clear grounds for a policy other than the deterministic 'inevitability' argument that has so frequently emerged in other countries, and even more recently in the Canadian initiative.

With particular references to the Coderre proposal in 2002-2003, a number of participants argued that there may be an ambition for a solution but this is far too often coupled with a poor understanding of the problems that will be dealt with by this 'solution'. As with any policy, we need to identify the risks and fears that we're trying to address, and possibly even desensitize them before they get built up too much, particularly within the post-9/11 pressurized environment. Many therefore called for the establishment of a solid business case as a pre-condition to any discussion and deliberation of a national policy. The purpose of this 'business case' is to verify that there is a 'real need' to introduce a national policy.

This is not to say that there was wholesale opposition to discussion of identity policy. Many argued that there are indeed a lot of problems that may be resolved through some kind of policy. But even these 'proponents' were concerned that some of the 'problems' were in fact are manufactured, some are merely perceived, and other problems get defined in confusing ways used ill-defined terms. For instance, 'identity management policy' as a term embodies a number of assumptions:

- Assumption 1. Canada needs a single policy. In fact it was argued that we need many, depending on the problem being identified.
- Assumption 2. 'Identity' as a term is well understood. In fact it is an ambiguous term because there are many functions that government performs that does not require the disclosure of identity e.g. establishing that an individual who wishes to purchase alcohol is over-19 years of age.

Finally, some participants voiced their worries that through the establishment of a policy what Canada would in fact end up doing is adopting a technologically driven approach for a socially engineered demand.

Many participants voiced concerns about the focus on 'fixes' rather than focusing on identifying the problem. For instance, identity theft, although often a rationale for mandatory identity documents and biometrics, is not as simple as it is painted out to be. Inadequate authentication is only one part of the problem, and in fact there are so many leak points and sources of the problem, including inadequate security safeguards. Rather we should be searching for data-breach law, as Ontario has already established for health information, but across all sectors. This will create incentives for organisations to improve security, and they will stop appearing as gold-mines for identity thieves. Meanwhile the criminal law regime and the lack of resources for law enforcement are only contributing to the problem.

While the drivers are commonly misunderstood, at the same time the lack of adequate tools for proper identity management are becoming a problem. The electronic provision of health information and services was given as an example: e-health involves coalescing electronic health information across a province. For this to work there is a need to identify citizens, doctors, health care providers, etc. There isn't an identity management tool available in the provinces that we can trust to provide these identity services to citizens. But this is not to say that a compulsory scheme, nor a monolithic database-driven scheme, is ideal. In fact, it could be more dangerous and could introduce greater risks. Rather an opt-in approach was promoted. But this approach is to be taken with great care, however, because there were a number of concerns over any system being sold as 'voluntary'. In fact, it was argued repeatedly, voluntary policies are rarely really voluntary, but is instead mandatory through stealth.

Some participants argued that both the need and the purposes for the resulting solution should not be driven by government departments and agencies making their case for a new policy, but by the development of evidence by others. For instance, some participants believed that the 'case' for identity policy could be established through a process of collaboration among academics and other experts, who together could devise a path forward for Canada through establishing a set of reasons articulating why it is necessary to start a national discussion on identity policy. Otherwise the traditional statements from government departments could lead to a highly complex and dangerous system.

Politics and Jurisdiction

Canada, with its federal structure and with its orientation to 'Canadian values', is a challenging political and legal environment for identity policy. The essential question here, that although wasn't always a high priority in the discussions, but rather lurked in the background of many of the statements is: Who is going to assume the responsibility and the leadership roles, and are these going to overlap and be redundant? There are a number of political discussions that need to be conducted before any progress is made. According to some participants who had experienced the debates around the last policy initiative on a national ID for Canada, the 'Coderre proposal', the primary result of that process was that we must reduce the 'fuzziness' around the political debate. That is, it was argued, before you go out calling for a national ID card, you need to tell people what it is going to do and what it is not going to do. A number of participants argued that until we can articulate that, we shouldn't be doing it.

Following from the issue of political leadership is the nebulous issue of jurisdiction. Participants pointed to the problem on how to get a single national policy or scheme to work across provinces, territories, and even abroad. For instance, interoperability with the U.S. would be ideal particularly with the need for moving goods and people across boundaries. But co-ordinating the provincial and the federal agendas alone would be difficult. We already have difficulties in identifying the differences in the existing regime of identity schemes across Canada, who are the responsible departments, and how the provincial measures mesh with the federal agenda. A mandatory multi-purpose identity system would involve a level of consultation at both the federal and provincial levels that would make it almost impossible to get off the ground, unless it was at such a high level that the emerging policy would be virtually meaningless.

Engagement and Deliberation

Following immediately from the political and jurisdictional issues comes the challenge of the policy process: if we decide to move forward on identity policies, how do we proceed? Some participants even noted that it is already difficult to establish transparency over the identity processes that are already being implemented. For instances, a number of participants (and researchers) voiced

concern that it was particularly difficult to gain access to information about how the Canadian Passport is going to change in the coming months and years.

A large amount of concern was raised about the need for consistency in communications about when new schemes will be introduced and what they will look like. There was a concern that there wouldn't be sufficient political and public debate. Worse yet, the slow emergence of de facto policies and credentials could result in the emergence of a national identity system without any debate and consultation at all. Many argued that there was a need for sustained public debate with 'real information', which relies on the transparency of government — and some argued that this had not previously occurred on a number of other policies (the 'no fly list' was mentioned repeatedly).

Identity systems are large complex computer systems, and highly ambitious; so we need to involve those who are implicated by the systems into the design process. This would ensure that the final policy fits people's needs and enables trust, rather than just meeting the interests and needs of a specific government department. It was felt that consultation would lead to transparency into the design decisions, ranging from how a card or a database is designed and how the interactions are managed. Without this, and without the necessary protections for privacy, there could be significant protests against any policy or system.

To promote protections it was recommended that the provincial and federal privacy commissioners be actively involved in the policy deliberation process. A public consultation would be difficult, however, considering the make-up and demographics of Canada. Participants also reminded us that we must be conscious that there is more than one 'public' in Canada. It was essential that all the different groups were consulted, e.g. aboriginal groups, language groups, ethnic groups, etc. Reaching out to the public for engagement is not simple. Some participants asked how we could reach out to the public on such a complex issue. One suggestion was to run an education project to create awareness of the key issues.

Informing the various publics must be done with great care, though there are some promising examples previously, e.g. flu shots, West Nile virus, recycling; but these are non-controversial issues and the dilemma is more difficult in a polarized debate.

The essential question of technology policy emerged in the workshops: do people really need to understand the details of the technology in order to make a decision about it? You need some understanding, but not necessarily a comprehensive education on the matter, many concluded.

There was great concern about power dynamics as well. The imbalances between NGO, industry, and political forces, and enormous money to be made in endorsing some schemes could lead to politically charged debates that are fuelled by simple-minded approaches to the problem. There was also concern that Canada does not have an active civil society acting as a safeguard, as other countries do, e.g. the U.S. There was a feeling amongst some participants that this would result in a

situation where the institution that 'owns' the policy will shape it in their own image, and debate would be minimized as government and industry forces would come to a solution at the expense of other stakeholders.

Repeatedly it was noted that the debate must occur in Parliament at the very least. A number of participants pointed to the lack of consideration of the no-fly list, which was never discussed in Parliament. Parliamentary debates help inform the public, some argued. Participants also raised the categories of debate about identification, and identified that we need a debate on 'Canadian Values' and 'Political questions and comments that arise'.

- Under 'Canadian values' the purpose of the 'debate' would be to see how the rule of law, tradition of law, charter of rights, plurality, and the fundamental trust in Government can be mixed together to result in a policy.
- The political question needs to look at the continuum of views people hold on questions related to identity is different from the political continuum, e.g. the left and right spectrum does not work particularly well in this domain.

Based on these values and political dynamics, participants concluded that only through a transparent policy process, including deliberation in Parliament, could a binding policy emerge. More importantly, a 'Made in Canada' type solution could emerge, which was considered essential to the success of the policy.

Therefore any approach taken must deal with the concern over the democratic deficit that is sensed in this domain. The lack of discussion about the existing policies only fuels these fears even more so. For instance, it was argued, the Smartborder agreement was implemented without any legislation, resulting in integrated systems that lack a government structure to provide accountability and transparency.

Yet some commentators noted that there are so many false dichotomies within the usual debates, where we compare 'demands from the state' and 'warning of privacy advocates', and in so doing we over-simplify the true nature of the policy domain. We need to be more reflexive about roles and responsibilities within the policy process and possibly ask how these traditional roles can be transcended for the best possible policy outcome.

One idea that emerged was to adopt the U.S. model of 'negotiated rule-making', where representatives of all the stakeholders meet repeatedly to establish the specifications for creating the relevant system. According to one participant, this was highly successful in the U.S. on the harmonization of drivers' licence standards, until the REAL ID Act did away with this process in favour of a government-sponsored solution.

Information Sharing

As identity policies grow in size, they tend to be seen as both an enabler of and enabled-by information sharing. The eventual systems take on a new momentum as government departments, in theory at least, start sharing more and more personal information.

Information sharing is considered one of the key obstacles and opportunities for identity policy. The technical capabilities are now available and ready to be implemented so as to enable information sharing. Previously the barriers were provided by functional separation. Functional separation came about naturally and provided a protection to abuse, but some participants pointed out that it is wrong to rely upon ineptitude as a guarantor of rights. Identity is one of the first policies forcing issues of a larger issue of connectivity increase, followed by porous borders, networked states, and networked individuals. This leaves governments in a situation that they need to reorganize in this new context, but we need to find ways to ensure against misuse.

Participants noted that Federal Government has become aware of information-sharing barriers, and are calling for mechanisms to reduce these barriers because they are seen to prevent the creation of efficient business practice and are obstacles to ensuring good services. A secure identity-aware network will allow government organisations to exchange information to enhance access to government services.

In many ways, however, this is unlikely to arise easily. Building from the jurisdiction issue above, there is little, if any, synchronization of data across government. For instance, different organisations and databases have different definitions and these can not be easily joined together. One recommendation for fixing this problem was to require organisations to conduct Privacy Impact Assessments (PIA). The PIAs would help by ensuring that public bodies have the proper authority for every specific piece of information they are collecting. The legal and administrative challenges of sharing would be much better identified, as well as some of the necessary barriers more properly understood.

Information sharing with the private sector was also raised as a concern (see below for privacy). On the other hand, this data-sharing may be an integral part of the identity issuance process. For instance, private registry agents are involved in Alberta's driver's licence issuance process. Another concern that emerged from this was not only the Government collection of information held by the private sector, but the possible use of identity data by the private sector emerging from the creation and use of an identity system.

Information sharing and its nexus with identity also raised a number of points around the implementation of biometrics. One useful and classic example was offered on 'biometrics done badly'. The use of biometrics in welfare programs has led to a reduction in the number of applications for welfare. This could be perceived as a drop in fraudulent access to welfare, but in fact

led to situations where people were taken off welfare when they should legitimately be on the program. In other cases individuals were afraid to give biometrics (e.g. fingerprints) for fear that the data would be used against them, whether re-purposed or shared with other government departments (e.g. police). The lack of clarity regarding linkages and data-sharing, and unclear prohibitions on cross-verifications led to a fall in participation in these programs.

While there is some support for the idea of 'breaking down the silos' that separate government departments' information and create inefficiencies, there was little support within the workshops for a multi-purpose scheme that would institutionalize this approach. Some participants called for a different approach, to replace the 'breaking the silo' vision. Rather, it was argued that we should permit 'linkages if need be', where the linkages would be vetted against some set of principles, to minimize them but while also ensuring the system isn't entirely in a vacuum. That is, individuals could choose to link up their driver's licence credential with their health access card credentials. Though they could use one identity document to gain access to multiple services, this would be done on an opt-in basis and strictly controlled.

Privacy

To our surprise, and with little intervention of our own (except with our statement that the Office of the Privacy Commissioner of Canada was funding our research through a contributions grant, that we announced on the day of the workshops), privacy was mentioned by almost every participant, if not all. The pro-privacy sentiment was strong and it was felt that this was a reflection of Canadians' attitudes and values.

Many felt that there was a lack of detail on the table regarding existing and proposed identity systems. With regards to these schemes, it was felt that too little was known about which identity information would be collected, how it would be used, what controls existed, etc. Particular attention was geared towards the emerging 'border card' policies, such as the pilot 'BC/Washington State' card.

There was also a concern about the perceived need to abolish anonymity when in fact in some, if not many, situations people may wish to gain access to government services anonymously. There was a concern that within the public debate and within the language surrounding identity solutions we were forgetting that ubiquitous identity was not an inevitability, nor even a necessity.

Another concern emerged regarding the use of additional identity information for a transaction when minimal data was actually required. One repeated example was geared towards the private sector, particularly bars and restaurants, who would scan and copy drivers' licences in order to create profiles of individuals (and one participant highlighted that this would happen more to women).

Many of the concerns that emerged to the 2003 proposed identity card still applied, according to some, including the concern that ever increasingly linked databases increases the potential for

surveillance, data mining, hacking and criminal access. Concerns were heightened with the idea of including biometric data. One interesting point is that there is hardly an opportunity to protect the proportionality principle if there is a single card-system-policy for a myriad of problems and situations.

At a very minimum, participants argued, there should be parliamentary debate, oversight and a commissioner established as a safeguard. Some believed that this could be an opportunity for a national discussion on Canadians' sentiments regarding privacy.

A strong set of arguments was offered to call for privacy to be built into systems at the design stage. There was a worry that projects are being developed where biometrics were be chosen solely on how 'neat' the technology is, without adequate consideration of the ethical and privacy implications.

There was a large amount of criticism towards using Privacy Impact Assessments as a safeguard. Many argued that far too often PIAs are only being considered as an 'end of process' issue, where boxes are ticked to post-rationalize the privacy components of a project. Rather we need to look towards the right to privacy, as established repeatedly in law, resulting in a set of principles that have stood the test of time: the requirement for a justification for the limits on freedom in a free and democratic society must deal with three aspects:

1. Rational connection between the legitimate goals
2. Minimal impairment of rights and freedoms
3. Proportionality between the ends and the means

In the context of authentication, it was argued that we should require the minimization of the collection of personal information.

On Data Protection, there is a sense that there is an enormous and growing trade in personal information, and we can not just sit back and accept this because the more that it is stored and traded, the more vulnerable the data is to unauthorized access. The fact that we assume consent to data collection through application of the opt-out consent rule, this has led to the creation of a 'monster network of digital dossiers'. Unless we have a strong foundation to protecting privacy within identity systems, any national policy will likely make matters worse. A paradoxical example was offered: audit trails that come to the aid of privacy. For instance, the BC Ministry of Health permits individuals to gain on-line access to their medical records and to look at the audit trail of the usage of their records, so that citizens can know who accesses their records. This centralization both enables access to the medical record to other users and institutions but also may enable the citizens to better ascertain who is accessing their sensitive personal information.

Need for Principles

There was much discussion around the idea of coming up with a strong statement of guidelines or principles that would guide (and possibly place strong conditions upon) the deliberation, decision, implementation and management of an identity policy and resulting identity systems. This was felt necessary in particular to ensure that Canadian values and privacy were promoted and protected, if not enhanced.

Repeatedly in the discussions participants mentioned the existing principles from the private sector and public sector work around the world, e.g. Treasury Board Secretariat principles, Kim Cameron's Laws of Identity, etc. There was some discussion of whether principles actually have value. Some saw principles as non-binding and non-restricting statements that would fall victim to 'exemption creep', where principles are set up through measures in law, and then regulatory changes would exempt large portions of personal information from protection. The result, some participants argued, was that the more principles you have the more likely you can keep on shifting information around.

There was a strong level of support for principles, nonetheless, provided that they could be made binding and relevant to the context at hand. Paradoxically, a number of participants called for the verifiability and testability of the principles — this seems to move beyond principles as a guide into principles as a specification. The midpoint, as some argued, was that principles should have a level of specificity as we have with the Data Protection Principles, or Fair Information Practices, where there are 'must haves', e.g. data subject access, which in turn act more like tests.

Although it is still considered 'early days' for identity policy, some participants argued that principles should be subject to tests themselves, but they in turn can become tests for the practices that are done out in the real world. The 'measurables' around the principles could model the CSA code on privacy that asks questions such as 'what does it mean to be 'accountable'?' But not all principles are considered equal, as some are procedural and some are substantive. For instance, U.S. Fair Information Practices are more like checklists, while the CSA code makes specific demands, e.g. to limit purposes for data processing to what is necessary, with built-in tests to verify this. Therefore some principles are more test-worthy than others. Finally a number of participants argued that the principles should be derived from a rights-based approach, because otherwise principles would be bypassed entirely.

Practical Issues

The discussions around 'practical issues' looked primarily at the more detailed aspects to identity policies and identity systems. Some of these discussions start of conceptually, but quickly begin looking at the detailed ramifications. Technological choices end up in discussions of implementations. Similarly, the strategy to build a new identity system or to build on top of existing systems ends in detailed discussions of the merits and challenges of each. Similarly, above we

discussed the virtues of a 'voluntary' system but the details are interesting as well. Other practical issues discussed below include concerns regarding costs and complexities of specific system designs, and problems with adjudication and enrolment.

The technology

There is nothing simple nor linear about the selection and implementation of technologies for identity systems. Concerns varied widely, including concerns regarding the life-cycle for the cards, the implementations of contactless technologies, and the creation of national monolithic databases.

Some workshop participants called for an assessment of the effects of technological choices on privacy. Meanwhile it was argued that the protection of privacy through technology was not only about minimizing collection based on existing technologies, i.e. 'good implementation of bad techniques', but it is also about designing technologies in such a way that they don't collect information, and thus creating a marketplace for privacy-enhancing technologies, i.e. 'creating good techniques'.

There is some positive work towards creating better understandings of how technology works, and what are the best practices for their implementation. We were informed regarding the Federal government's 'Biometric working group', involving 22 agencies that discuss issues, standards, testing and are working on best practices. The driving purpose of the working group was to establish some understanding of the application of technology. That is, it is only too easy for each government department to work within its own project/working team to come up with biometric solutions to problems, but sharing this knowledge and the experiences across departments will enhance the understanding of how and when biometrics are best applied, e.g. asking whether the project actually requires biometrics, what types, etc., to avoid vendor-driven decisions. There is also a Canadian Biometrics Centre of Excellence proposal being considered. Others were concerned that biometrics were being oversold.

Build on top or build anew?

While there are many strategic aspects to this choice, the decision to build a new identity system or to enhance existing identity systems for new purposes comes with many practical challenges. Many participants noted that the existing identity systems may be sufficient. The Social Insurance Number is already a de facto identifier that crosses boundaries. This was also used as a justification for a new separate scheme, stating that a national system was not prohibitively complex or challenging because we already successfully implemented national systems such as the SIN.

On the other hand we can build on top of existing identity systems, following examples from elsewhere in the world. The BC and the U.S. governments have met to discuss a joint pilot project to build a new identity standard on top of the drivers' licences to deal with increased demands under U.S. border policy. The primary purpose of building upon the licence infrastructure is to avoid the

need for passports at the border due to economic and tourism concerns. In particular, more than 18,000 businesses are associated with the tourism industry, and every change in documentation standards has implications on the tourism industry. In fact some asserted that the drivers' licence can be improved to such an extent that it could be made more reliable than a passport. This view was enhanced by a discussion of the developments in the Albertan driver's licence through the use of biometrics.

A number of participants and one presentation in particular discussed the disadvantages of building on top of an existing identity system. The case of the REAL ID Act from the U.S. shows that there are a number of practical problems in establishing standards that will apply across jurisdictions. The privacy concerns also arose here, where participants were concerned that 'scope creep' will emerge as identity credentials developed for one purpose being used for another. For instance, the swiping of drivers' licences to verify whether the holder is legally permitted to purchase alcohol actually discloses far too much information (the information on the driver's licence) instead of restricting the disclosure to what is strictly necessary (the status of whether the holder is over the drinking age). As a result, too much identity information was being disclosed.

Another method of dealing with this issue would involve strengthening foundation or 'root' documents. For instance, birth certifications could be electronically protected and verifiable. This strengthening of existing identity documents could be done without expanding their uses, but could enhance verifiability and assurance against fraud.

Root documents, adjudication, and enrollment

A large amount of discussion focused on root documents and the 'inherent' problems herein. For example, birth certificates are not strong documents but are relied upon too much. There are also problems of consistency on how different organisations are dealing with different documents, reference points, etc. and as a result we have overlapping programs and more information being held than is strictly necessary. It is possible, therefore, that an identity policy could reduce these burdens and in turn reduce the amount of information held by third parties.

The enrolment process was also identified as key component of any identity policy. If individuals are compelled to come into an enrolment centre, for example a driver's licence authority, these authorities will need to be able to verify the root documents and to understand the standards for these documents from across the country, or even around the world. If adjudication also involves some form of interview or referee process, these take time and involve additional expenses. The inconvenience of actually having to show up at an office rather than process your identity documents through the post (particularly for renewal purposes) is significant, not only in introducing greater costs but will likely increase the political risks.

Costs and complexity

A lot of this discussion focused on the complexity of the schemes being devised. In the experience of some in the room, what start off looking like simple solutions turn into complicated ones involving great costs, amongst other problems.

Even the policy process alone would be expensive, according to some participants. If a policy initiative begins, a lot of policy discussion will emerge, risk assessments will be conducted, and consultations will be done across the country. We'll likely see failed attempts at co-ordination between Federal and Provincial governments, significant survey research, a lot of funds for consultants, and a lot of academic analysis that may be out of date by the time it is useful.

Others were worried that based on previous high profile system failures (e.g. the gun registry) there is already a lack of trust and confidence in government's ability to avoid future failures.

Mandatory vs. Voluntary

Repeatedly the question of a mandatory v. voluntary policy came up. As mentioned above, this was often a strategic issue, but also as a serious practical matter. Voluntary schemes are likely to come near to being mandatory, such as through the driver's licence example where it is a de facto identity card provincially at least. But the primary purpose of the licence is to manage who may drive and to keep track of infractions. If it truly becomes the de facto identity scheme, this may impose a number of duties on driver's licence authorities and other record keepers, taking away from their core business, and introducing new risks and costs.

Others asked how the voluntary regime could be sustained against policy developments. That is, could limitations be set on how a card could be used, preventing it, for instance, from becoming mandatory for certain purposes? This was then linked to the notion of credibility: if a scheme that is introduced as being voluntary then becomes mandatory, there was a concern that these vacant or false promises would further reduce the credibility of government in light of recent scandals.

At the same time, a convincing argument was presented stating that concerns over privacy shouldn't prevent some people from using an identity system if they so choose to. An opt-in basis must be permitted so people can act as informed consumers to choose to use identity services, as we wouldn't want to restrict people from being enabled to use these services and credentials in a safe and controlled environment.

Summary

Each workshop that the research team participated in, and previous to this research project and subsequent to it, had a number of similar results. The key points emerging from the workshops that should be taken forward are as follows:

- As a precondition for starting a national debate on identity policies, we must establish the objectives and specific purposes of whatever regime is proposed.
- Transparency of process was considered essential. This presumably means striking an honesty with the population that the process will be open, and thorough. Draft legislation was offered as a possibility, or you can start from scratch and get the public to contribute to initial discussion and inform design.
- As a guiding policy principle, participants recommended a 'pull' rather than 'push' approach. That is, we must enable citizens rather than create a punitive identity system across their lives. This could serve to establish the distinction between a policy and system that enable service delivery rather than law enforcement. Though it was noted that a law enforcement centred model could still involve convincing people that you have something to sell.
- If you create the technological enablement for data-sharing, how do we draw the line for how it is used?
- There were serious concerns about the adequacy of existing privacy protections. Some argued that before there are any discussions about a national policy, there must be a strengthening of regulators' powers. Others argued that this would probably not happen. One conclusion was that one of the only regulators with adequate trust and powers is the auditor general.

A resounding conclusion from many of the participants was that Canada is not ready for a big bang policy or another national ID card initiative. Despite this sentiment, however, the participants believed that Canada was not doing a good job on the levels of identity documents. There was optimism in the workshops that we can start making steps on improving how they're used today and there was hope that we can also establish the necessary limits, whatever they may be.

5. What's Happening in Canada

We need a better understanding of the changes currently occurring in Canada, while also learning from some of the recent experiences in identity policy. Below we cover some of the initiatives of recent years.

Ontario Smart Card Project

The Government of Ontario officially announced its intention to introduce a smart identity and entitlement card in the Speech from the Throne October 21, 1999. The card was to be central component of the Ontario government's broader e-government strategy. At the time of its announcement, the Ontario Smart Card Project (OSCP) was one of the largest and most ambitious initiatives of its kind in the world in scope and in scale, granting access to a wide range of government programs and services for all residents of Ontario, more than 12 million people. Despite a substantial investment (approximately $12.5 million over the course of the project), the project was quietly cancelled in late December 2001.[32]

There are several probably reasons for the OSCP's failure. It was an extremely ambitious and complex initiative. There were organizational challenges that were not insignificant. The OSCP was lead by the Management Board Secretariat. However, the wide range of programs and services the OSCP wanted to included required a high level of co-operation between multiple Ministries and agreement on the vision of the card. Furthermore, the needs of all the different programs, which previously operated with a greater level of autonomy, would also need to be considered and somehow built into the system.

There were also logistical challenges, such as registering all Ontarians some of whom live in very remote locations. Furthermore, since the project was strongly considering the use of biometrics this would likely require in person registration, again a particular challenge for those living in remote locations. This would also increase the cost of the program.

Another major hurdle was the lack of public support for the OSCP. There were concerns about privacy, particularly with respect to the use of biometrics. These concerns were exacerbated by the lack of information about the project in the public domain. While government websites at the time indicated that the main goals of the project was to increase efficiency, reduce fraud, while increasing privacy and security, little other information was available. It was not clear how privacy would be maintained while allowing for this increased efficiency and the data matching involved in reducing

32 For a detailed description of the Ontario Smart Card Project, see K. Boa, Smart Card, Weak Effort? Public Consultation in the Ontario Smart Card Project, Master of Information Studies Thesis, University of Toronto, 2003, p. 72-82.

fraud. Internal documents reveal that building privacy into the design of this system was somewhat peripheral to the main work of the project. Although mandated by government policy to conduct a privacy impact assessment (PIA), the PIA never moved beyond the initial stages over the two years of the project.

Finally, the OSCP was not only an extremely ambitious project to design and implement a multi-application smart card, but also Ontario wanted to do this on an aggressive timetable. Internal documents show that initially, the project planned to have everything designed and rolled out by summer/fall 2002 – a mere 2 years from its inception. The project rapidly fell behind schedule. By Summer 2001, they had moved the launch date forward by one year.

Together the complexity of this project and the desire to design and implement it on such an aggressive timetable in the absence of public support and with little to no public consultation likely lead to its failure. It seems that the challenges of such a complex and ambitious project were not fully considered before the project was announced.

Identity documents in Quebec

In this section we look briefly at Quebec's initiatives to update and change its Health Cards and Birth Certificates.

Quebec's Smart Health Cards

From the early 1990s until 2002, it appeared that Quebec was going to implement a smart health card for the province. This did not happen and it is not clear from available information what happened.

During 1993-1995, Quebec conducted a pilot project using smart cards for health in the Rimouski area, which included 7250 patients and 300 health professionals.[33]

> "The card carried personal and health data, secured by a PIN, in five categories– identification, emergency, vaccinations, medications, and ongoing care (history, consultations, follow ups, etc). It was designed to enable patients to provide more complete information to their care provider to reduce redundancy of tests; to reduce the risk of drug interactions; and to improve the quality, continuity, and integrity of care. The evaluation judged the project a success in improving availability of clinical information while protect-

33 Roderick Neame, "Smart Cards: The key to trustworthy health information systems" BMJ, 1997, 314:573 (22 February). Online at http://www.bmj.com/cgi/content/full/314/7080/573

ing personal privacy and encouraging better follow up, and it was especially useful in emergencies."[34]

In 2001, some press articles indicated that Quebec was moving ahead with a smart card system for healthcare. However, in 2002 it became clear that they moved away from this plan.[35]

The Current Quebec Health Card

The current health card in Quebec is valid for 27-75 months, contains a digitized photo and signature, along with other personal information, including organ donation information on the back of the card.

The following information appears on the face of the card:

1. A Health Insurance Number, unique to each person, consisting of:
    - the first three letters of the last name;
    - the first letter of the first name;
    - the last two digits of the year of birth;
    - the month of birth (to which 50 is added to indicate female);
    - the day of birth;
    - an administrative code used by the Régie [de l'assurance maladie].[36]
2. The person's name(s) and card history:
    - first name (if the number of characters in the first name exceeds the space available, only the initial will appear on the card);
    - last name at birth;
    - husband's last name, if requested by a woman married before April 2, 1981 or by a woman married outside Québec who exercises her civil rights under that name;
    - the number of cards issued to the person since 1984.
3. The person's birth-date and sex.

---

34 Ibid. I located the citation to an evaluation that seems likely to be the one referred to in this quote but cannot find of the document itself. The citation is: Fortin, J.-P., et al., Évaluation du projet québécois d'expérimentation de la carte santé à microprocesseur. 1996, Régie de l'assurance maladie du Québec: Quebec.

35 http://www.cmaj.ca/cgi/content/full/166/5/640-a

36 The transparency of whence derives each element of this identifier is interesting. I don't recall this information being made so clear in other jurisdictions or with respect to other identifiers.

4. The year and month of expiration.

5. The person's photograph and signature, both of which are digitized and incorporated into the card. Cards issued to persons not required to provide a photo and a signature, such as children under age 14, have no photo or signature spaces, while cards issued to persons exempt from providing their photo, their signature or both, are marked "exempté" in the appropriate space(s).[37]

The exemptions for photos and signatures are most interesting. Children under the age of 14 and persons over the age of 75 are exempt from the photo and signature requirements, although those over 75 can include them if they prefer. Also exempted from photos are persons too ill to submit to the procedure and persons temporarily outside the province and are renewing (or applying) by mail.[38] There is no mention, however, of exemptions on religious or cultural reasons.

Registration can be done online (for those who are coming to Quebec for the first time or returning after an absence) or in person, but the authentication is meant to happen in-person, unless other circumstances exist. To follow the authentication process, the individual presents the form, two identity documents, and a photo at an Régie de l'assurance maladie office. The acceptable identity documents are: Health Insurance Card, Driver's Licence, Birth Certificate or Copy of an Act of Birth, Passport, Certificate of Canadian Citizenship, certificate of change of name, certificate of change of designation of sex, a Canadian or Québec immigration document, Social Insurance Card.39 The authentication document is then signed in the presence of an official and the whole package is sent to the Régie de l'assurance maladie.

Quebec Birth Certificate and Baptismal Certificates

Until recently, Quebec baptismal certificates were equivalent to birth certificates to prove Canadian citizenship. However, there has long been concern about forgery with the Quebec baptismal certificates. While the fraud rates are not publicly disclosed, the most widely known case was that of Ahmed Ressam, the millennium bomber.[40] Ressam attempted to enter the U.S. using a false identity, with authentic identity documents, including a Canadian passport, for that false identity. He was found to have obtained these identity documents using forged foundation documents, one of which was a forged Quebec baptismal certificate. In response to this case and general concerns about fraud as of October 25, 2001, Quebec birth certificates, baptismal certifications, and marriage certifications issued before January 1, 1994 are no longer acceptable as proof Canadian citizenship.

37 C.f. This list of 5 elements is taken directly from the Government of Quebec website: http://www.ramq.gouv.qc.ca/en/citoyens/assurancemaladie/carte/carte.shtml

38 http://www.ramq.gouv.qc.ca/en/citoyens/assurancemaladie/carte/except_exempt.shtml

39 http://www.ramq.gouv.qc.ca/en/citoyens/assurancemaladie/carte/photo_pieces_identite.shtml

40 See Bijon Roy (2005), “A case against biometric national identification systems (NIDS): ‘Trading-off” privacy without getting security,” Windsor Review of Legal and Social Issues, 19).

Specifically the CIC website declares:

> "Baptismal certificates, birth certificates and marriage certificates issued by the government of Quebec before January 1, 1994 are no longer accepted for issuing a proof of Canadian citizenship. This applies to applications for replacement of your certificate as well as first time applications for certificates. New documents will be required from the government of Quebec for yourself, your child, your parent or your husband to establish proof of citizenship."[41]

Birth certificates are now requested through the Directeur de l'état civil Quebec. First, a birth is declared and entered in the register of civil status. This must be done within 30 days of the birth. The birth is attested to by the accoucheur (the person who assisted in delivering the birth), and the attestation accompanies the registration from. It contains some interesting stipulations around names:[42]

- Surname
  - Must come from either of the parents surnames or both using a hyphen
  - It may not include more than two parts, even if both parents have hyphenated surnames.
  - May not contain numbers or an initial
- First name
  - No more than 4 names are recommend and hyphenated names are acceptable
  - The registered spelling of the name will match that which appears on the declaration.

Registering the birth of the child is necessary to obtain a health card.

This situation is most interesting because it seems that it requires the re-registration of an entire population (for those born before 1994 at least). In our research this was a relatively unique situation. This is a form of re-enrolment that is logistically challenging but is one way of avoiding the creation of a complex central register of biometrics, using alternative forms of establishing some form of uniqueness, i.e. the structure of the proper name.

41 http://www.cic.gc.ca/english/applications/guides/CIT0001E3.html

42 c.f. http://www.etatcivil.gouv.qc.ca/English/birth.htm

Alberta's Drivers Licence

The old drivers licence was on paper containing the name and address and other similar personal information. This was upgraded to a plastic card with photo and signature because paper documents were easy to tamper with, particularly after criminals broke into the registry office. The new card is a laser engraved card, and uses other technologies that are not available on the open market. The card is manufactured and personalized in the same location to increase security. The card also contains a unique audit control number to track the card in the process of manufacturing and distribution.

Enrolment takes place through the presentation of supporting documents. The eligible documents were changed recently. The facial biometric and the written signature are collected and stored in a database. Residential status is verified to get a card.

If the card is lost you can use the picture on file as a credential to get a new one. Registry agents have to verify that client's existing image is compatible with new image. The system verifies photograph against database of photographs to ensure against multiple enrolments. This verification is done in the back office because of the processing power that is required. Applicants are issued with a temporary card at and then verification takes place. Once approved the new card is then created.

The card does allow for background checks due to the greater certainty the scheme allows regarding personal information (such as address information). The motor vehicle registry and driving licence database is not subject to the provincial FOI and Privacy Act. Regulations do control the release of information in the database. For instance, while some agencies are granted access to the registry, on-line access to the registry is audited to ensure it is purpose-based. The audit trail is not accessible by citizens. If police in Alberta stops a citizen, the police can call in for verification with the name, number, or address. A Privacy Impact Assessment was conducted and submitted to the Albertan privacy commissioner. In fact, Alberta designed a new PIA tool to enhance the process.

There has been a challenge in the courts over the use of the photograph and at the time of the workshop this had gone to the appeals process.

BC Ministry of Health

British Columbia is currently trying to envision alternative mechanisms for managing identity. Though their plans are not yet settled, some of their ideas are worth noting here.

A key driver for new identity services is the need to enable access to electronic health information and services. The requirement is to issue digital identities to users of health services, such that individuals can view and directly control disclosure of their electronic health information. Given that

personal health information is involved, the need for strong assurance of identity is paramount. The key question is this: How can the government obtain strong assurance that someone presenting themselves online is indeed the same person that is the subject of a set of electronic health records?

Currently there is no central citizen identity registry in BC. Health service users are identified through two types of identifiers: Personal Health Numbers (PHNs) are used to identify people who receive health services in BC, and Medical Record Numbers (MRNs) are used to correlate medical records within a facility. While these identifiers are generally based upon verified identities, there are a variety of circumstances that allow the creation of identifiers without verification of an individual's identity. As a result, knowledge of a PHN, MRN or other related identifiers, is insufficient to provide strong assurance of identity, or even uniqueness, and particularly in an online context.

At the moment the health ministry is focusing its attention on BC residents who are also Canadian citizens (and thus not considering, for the time being at least, BC residents without Canadian citizenship and non-residents with or without Canadian citizenship). These are the clients that are the primary focus of eHealth efforts, and as such are being treated as a priority.

The guiding principle for identity within one of the ideas being considered is that participation must be optional and self-directed (i.e., 'opt-in'). That is, individuals may choose to participate, and according to one statement (provided during one of our workshops), "any incident involving identity records must be with the full knowledge, consent and action of the individual." The essential point to this approach is that health services requiring online authentication must be strictly 'value-added'. That is, core health services will not and cannot be made available exclusively over authenticated electronic channels. Other delivery channels must also be available for access to core services.

Identities could be uniquely distributed through an online registration process. 'Over the counter' processes would be kept to an absolute minimum in order to reduce administrative burdens. The enrolment process would involve citizens going online and presenting a foundation identity document number. For instance this could involve entering one's birth certificate registration number. There would then be a check against background databases for the validity of the birth certificate and to ensure against double enrolments. A digital identity would then be set up with a rudimentary level of assurance, sufficient for access to some services. Additional adjudication through substantiation of further information would also be possible — for example the individual may be asked to state the result of line 150 of his or her tax return. The service would thus support varying levels of identity assurance, from unverified to 'strongly identified', as needed to support varying levels of authentication across different online services. There will be no card involved; in fact the proposed model could be characterized as a 'digital identity card' system.

The identity established within this system could also be extended across other government services. Again this process would be optional, where individuals can establish 'linkages' to other identity services and service providers.

Smart Borders

There are three main policy drivers that relate to developing a “smart border” between Canada and the United States:

- the Canada-U.S. Smart Borders Declaration and 32-point Action Plan;
- the Security and Prosperity Partnership of North America (SPP);
- and the Western Hemisphere Travel Initiative (WHTI).

All three have direct implications for Canadian identity policy, particularly with respect to what is accepted and/or acceptable at the U.S. border.

The relationship between the SPP and the Smart Borders Declaration is not entirely clear. The SPP seems to be an updated and expanded version of the latter. It is also unclear whether or to what degree the Smart Borders Declaration is still active; however, it is listed in on the Canadian Border Services Agency’s website as one of the ways in which Canada is working in partnership with the U.S. In addition, the Smart Borders Declaration and the SPP are much more comprehensive and far reaching in subject than simply identity documents, however border security and identity documents do form a significant part of their mandate. The WHTI is the most focused on identity documents of the three and dictates changes to what is acceptable documentation to enter the U.S.

The Canada-US Smart Borders Agreement and 32-point Action Plan

The Smart Borders Declaration and its associated 32-point Action Plan[43] is a formal agreement between Canada and the U.S. signed in December 2001 to ensure “the secure flow of people, the secure flow of goods, a secure infrastructure, and the co-ordination and sharing of information in the enforcement of these objectives”.[44] Regular status reports and updates were issued by the Canadian and U.S. governments until December 2004. It seems that the SPP supercedes the Smart Borders Declaration since the most recent Status Report was released in December 2004 and the SPP was initiated in March 2005.

43 The Action Plan initially consisted of 30-points in 2001/02 but had expanded by 2003 to include 32 points. See Appendix A for a copy of the Action Plan, with asterisks’ indicating the two points added later.

44 http://www.dfait-maeci.gc.ca/anti-terrorism/declaration-en.asp

The “secure flow of people” element, comprising 13 points, focuses most directly on identity issues. Identity, identification, and information sharing, including personal information, form a significant part of the agreement.

With respect to biometric identifiers, the first point listed in the action plan, the December 2004 Status Report indicates:

- Agreement to develop common standards for biometrics
- Agreement to adopt interoperable, compatible technologies to read these biometrics
- Mutual desire for cards that can be used across modes of travel (e.g., marine, air, road)
- Work with the International Civil Aviation Organization to determine and develop international standards for biometrics for travel documents
- NEXUS Air program using iris recognition and the NEXUS Highway program fingerprints
- Canada will be issuing facial biometrics in passports on a smart chip by mid-2005
- US will start piloting passports that include biometrics by the end of 2005
- Development and expansion of US-VISIT, which collects index fingerprints and facial biometrics from all foreign nationals entering the United States, except Canadians and Mexicans at this time.[45]

With respect to permanent resident cards, the second listed point, the Action Plan stipulates the need to “develop and deploy a secure card for permanent residents that includes a biometric identifier”.[46] While a secure permanent resident card was issued in 2002 and required for re-entry to Canada by 2004, this card does not include a biometric, although it does have the capacity to hold one.[47]

The NEXUS program comes up in two points of the Action Plan – biometric identifiers and the Single Alternative Inspection System. NEXUS is a joint program between Canadian Border Services Agency, Canada Customs, Citizenship and Immigration Canada, and U.S. Customs and Border Protection. The NEXUS programs, originally divided into Air, Highway, and Marine, have now been rolled into a single program, called NEXUS.[48] NEXUS is in place at 11 land border crossings and according to the December 2004 Action Plan Status Report, as of October 21, 2004, the program had enrolled approximately 71,000 participants (for NEXUS Highway). NEXUS has been operational

45 http://geo.international.gc.ca/can-am/main/border/status-en.asp

46 http://www.dfait-maeci.gc.ca/anti-terrorism/actionplan-en.asp

47 It would be interesting to know more about why biometrics were not included.

48 It is not clear exactly when this happened, but it was in the last 6 to 8 months.

at the Vancouver International Airport since late 2004 and was recently launched by Canadian Border Services Agency at Toronto's Pearson International Airport (February 2007) and will shortly be expanded to the following international airports: Edmonton, Calgary, Winnipeg, Ottawa, Montreal and Halifax.[49]

Security and Prosperity Partnership of North America

The Security and Prosperity Partnership (SPP) was initiated in March 2005 between the U.S., Canada, and Mexico. The SPP

> "provides a framework to advance collaboration with Canada's neighbours in areas as diverse as security, trade facilitation, transportation, the environment and public health. This partnership has increased institutional contacts between the three governments to respond to a shared vision of a stronger, more secure and more prosperous region.".[50]

This is not a formal written agreement, but is described as a "framework" or "a dialogue" between the three countries. The U.S. leadership in the SPP is much clearer (more directly articulated) than it was the Smart Borders Declaration, although there too there was concern that it was a U.S.-led initiative. The U.S. SPP website explains that this

> "is a White House-led initiative among the United States and the two nations it borders – Canada and Mexico – to increase security and to enhance prosperity among the three countries through greater cooperation."[51]

The SPP describes even more extensive collaboration than Smart Borders Agreement. Broadly it is divided into a security agenda and a prosperity agenda. The main areas covered by the SPP included: Strengthening Competitiveness in North America; North American Emergency Management; Avian and Human Pandemic Influenza; North American Energy Security; and North American Smart, Secure Border.[52] The final element, most relevant to issues of identity, calls for "a border strategy to build smart and secure borders that rely on technology, information sharing and biometrics".[53]

Canada allocated funds specifically to meet SPP goals in the 2006 Federal Government Budget.

> "[The] budget will invest $303 million over two years on a range of initiatives. Key among these is the border strategy aimed at efficient and secure movement of low-risk trade and

49 http://www.cbsa-asfc.gc.ca/newsroom/release-communique/2007/0212toronto-eng.html

50 Canadian Budget 2006, available at http://www.fin.gc.ca/budget06/bp/bpc3de.htm

51 http://www.spp.gov/myths_vs_facts.asp

52 http://www.pm.gc.ca/eng/media.asp?category=1&id=1085

53 Budget 2006, http://www.fin.gc.ca/budget06/bp/bpc3de.htm

travelers to and within North America, while protecting Canadians from threats, including terrorism. This strategy includes the following key activities, as well as other efforts related to emerging SPP priorities."[54]

These areas are:

- Air-passenger data transfers. Originally implemented in 2002 to 'identity and intercept high-risk individuals'. Budget 2006 provides $25 million over two years to expand this program to allow more effective information gathering from European airlines.[55]
- The NEXUS Air pilot project 'to speed passage of low-risk travellers between Canada and the United States' will be expanded to seven other major Canadian airports. Budget 2006 provides $25 million over two years to extend this system.

The most recent progress report, the 2006 Report to Leaders[56] covering the period March 2006 to August 2006, does not explicitly address identity issues. However, some of the accompanying Security Annex, indicates that a border issues are ongoing.

1. The goal to "develop and implement equivalent biometric standards and systems to enhance security for passports, visas, permanent resident cards, transportation credentials and other border documents"
2. The goal to "develop and implement compatible immigration security measure to enhance North American security, including requirements for admission and length of stay; visa decision-making standards; lookout systems; and examining the feasibility of entry and exit procedures and systems"
3. The goal to "work to ensure compatibility of systems to share data on high-risk travellers and examine the feasibility of a real-time information-sharing program on high-risk travellers to provide for risk management decisions on travellers destined to or on transiting North America."[57]

The foreign ministers of Canada, Mexico and the U.S. met again in Ottawa February 23, 2007. Much of the press coverage so far claims that border issues were a top priority, but there are few specific details available. Any subsequent comments on the border pertain to the avoidance of hampering trade (and tourism).

54 Budget 2006, http://www.fin.gc.ca/budget06/bp/bpc3de.htm

55 Budget 2006, http://www.fin.gc.ca/budget06/bp/bpc3de.htm

56 http://www.spp.gov/2006_report_to_leaders

57 p. 49-50 of 2006 Report to Leaders.

There are concerns in both Canada, Mexico, and the U.S. that the SPP is too secretive, too focused on big business needs, and will have ramifications for sovereignty. Interestingly the question of the SPP's implications for sovereignty is dealt with in the U.S.'s Myths and Facts webpage;[58] however, the Canadian government's information does not address this issue explicitly.

Western Hemisphere Travel Initiative

The Western Hemisphere Travel Initiative (WHTI) is part of the US Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004. The WHTI puts forward new requirements for all individuals entering the United States (including U.S. citizens). Everyone must now present a passport or other some other secure identity and citizenship document. These new requirements come into effect for different ports of entry (air, land, and sea) at different times. The essential question is what documents other than the passport, if any, will be accepted by the U.S. government.

The WHTI requirements for arrival in the U.S. by air began in January 2007. Canadians must now carry a passport or a NEXUS card "when used at a NEXUS kiosk at designated airports".[59] The deadline for WHTI compliance at land and sea ports of entry has been extended from January 1, 2008 to June 1, 2009, in the fiscal year 2007 Homeland Security Appropriations Act.[60]

Given that alternative documents are being accepted at airports, it seems likely that alternative documents will also be accepted at sea and land ports of entry, particularly given the extension of the deadline for compliance. One option, in addition to the NEXUS program, is some form of an upgraded drivers' licence that contains citizenship information. Also, Ontario and British Columbia are looking at options for implementing new "secure" licences, which could be deemed acceptable travel documents for crossing the U.S. border. British Columbia is working with Washington State to look at acceptable options. The Premier of Ontario, Dalton McGuinty, announced in February 2007 that he was speaking with U.S. officials, in order to ascertain whether the drivers' licence would be considered, as Ontario begins to plan its new drivers' licence system. In a press conference he indicated that the only additional information needed for the drivers' licence to be used as a travel document is "encrypted citizenship information".[61] McGuinty is drawing on the idea that it is better to upgrade something we already have than to develop yet another identity document.[62]

Details of what will be acceptable for land and sea border crossing are still in flux. In addition to discussion focusing on the acceptability of the drivers' licenses, Secretary of Homeland Security,

58 http://www.spp.gov/myths_vs_facts.asp

59 http://www.cbsa-asfc.gc.ca/agency/whti-ivho/what-quoi-e.html

60 Signed in to law October 4, 2006.

61 CBC radio hourly news, Feb 26, 2007.

62 For more information on these stories see http://ca.news.yahoo.com/s/capress/070222/national/us_border_passports and http://www.thestar.com/News/article/184971

Michael Chertoff announced in February 2007 that children (under 15) would not be required to carry a passport to enter the U.S. by land or sea.[63]

Key points:

- The United States seems to be driving changes to identity documents, not only within their own country but also in Canada.
- The idea that 'secure borders' are deeply tied to technology, information sharing, and biometrics is deeply embedded in all three programs.
- There is a growing momentum behind the harmonization of technologies, practices, and policies, particularly in the area of risk assessment. This harmonization process is not only between Canada and the U.S., but within the SPP this expands to Canada, the U.S., and Mexico. This degree of harmonization raises significant concerns about issues of sovereignty and adequate policy transparency and deliberation.
- Which documents will be acceptable for crossing the United States' border have not been firmly established, but what the United States decide will have direct implications for Canadian identity and travel documents.

We expect to see even more flux and uncertainty in this domain before final results emerge.

Biometric Passport

The first formal announcement of a pending Canadian biometric passport came with the Smart Border Declaration in 2001. Since then it has been mentioned in each of the subsequent policy statements discussed above, but beyond this there is remarkably, and disturbingly, very little public information available. In 2002 the Passport Office began issuing passports with a new, more tamper-resistant design, but without biometric encoding. It required digitally produced photos, and famously, prohibited applicants from smiling in these photos, presumably to ease automated facial recognition. These images are scanned and used in printing the passport, but there is no machine-readable digital storage of the image on the passport itself.

In 2004 the Passport Office sought approval from the federal Office of the Privacy Commissioner (OPC) to use its recently tested facial-recognition technology in processing passport applications.[64] A summary of the resulting Privacy Impact Assessment (PIA) identifies 10 areas of concern/risk[65] and

63 http://www.theglobeandmail.com/servlet/story/RTGAM.20070221.wpports0221/BNStory/National/

64 Jim Bronskil, Plan to match Canadian passport photos with terrorist watch lists in works, Canadian Press, August 29, 2004 <http://cnews.canoe.ca/CNEWS/World/WarOnTerrorism/2004/08/29/pf-608375.html>

65 The six areas of 'concern' draw from EPIC's privacy analysis of facial recognition technology: Storage, Vulnerability, Confidence, Authenticity, Linking and Ubiquity, The four other areas of 'risk' mentioned are: Function creep, Third party access, Centralized retention and Individuals' loss of control.

lists 18 recommendations by the OPC for bringing the use of facial recognition into compliance with privacy standards. The Passport Office agreed in principle with most of the recommendations, but on the first two, concerning establishing a legislative/regulatory framework and lawful authority, it dissented. [66]Nor so far is there any substantive public information about how it will meet the recommendations agreed to in principle.

On September 1, 2004 and again June 15, 2006, the federal Parliament amended Section 8 of the Passport Order (the Act that governs the passport in Canada) to read:

> 8.1 (1) The Passport Office may convert any information submitted by an applicant into a digital biometric format for the purpose of inserting that information into a passport or for other uses that fall within the mandate of the Passport Office.
>
> (2) The Passport Office may convert an applicant's photograph into a biometric template for the purpose of verifying the applicant's identity, including nationality, and entitlement to obtain or remain in possession of a passport.[67]

In July 2006 the Passport Office issued a public Notice of Proposed Procurement inviting vendors to submit bids for a "a high volume Facial Recognition Solution (FRS) that will verify and process digital images of passport applicant's picture as part of the passport application process"[68]. The bidding period closed September 28, 2006, but so far there has been no public announcement of the contract.

Although the biometric passport is far behind its original schedule, there is clearly work underway on it. However, the federal government has chosen neither to inform nor consult the public about what is planned. The serious issues concerning rationales, privacy, security, function creep, costs, oversight, governance, information sharing (e.g. with the U.S.) and national sovereignty have not been addressed openly. This raises questions about what exactly is being planned and strongly suggests that the Government of Canada does not trust Canadians. Not only does this call into question the legitimacy of the exercise, it undermines the public support that will be needed to make the deployment successful.

In all these federal policy and identity system initiatives discussed above, we see a remarkable lack of transparency. Far from heeding the Parliamentary Committee's advice about addressing key questions and involving the public in a deliberative process, the federal government has been proceeding with national identity initiatives without clearly specifying the purposes for them, the necessity for new systems rather than improving existing means, the financial costs (for start up and on-

---

66 A summary of the Facial Recognition Project PIA is available on the Passport Canada website http://www.ppt.gc.ca/publications/facial_recognition.aspx?lang=e Access to Information (ATI) requests to obtain the full PIA and that for the biometric passport itself are pending.

67 Canada Gazette, September 23, 2004. http://canadagazette.gc.ca/partII/2004/20040922/html/si113-e.html,

68 http://www.merx.com/English/SUPPLIER_Menu.Asp?WCE=Show&TAB=1&State=7&id=PW-%24EEM-006-14751&hcode=shsxpr2tIBMeERly4npDoQ%3D%3D

going administration, liability and cost sharing arrangements), the handling of personal information, the security of documents, devices, and databases, among other matters of public concern.

Treasury Board Secretariat Identity Management Initiatives

Identity Management is often confused with ID cards, access controls, privilege management, and datasharing. To help resolve this problem, the Treasury Board Secretariat established an inter-departmental subcommittee working group to open up work in this area. TBS hopes for an eventual policy for cross-government identity management, in the expectation that a common understanding of identity could provide gains in economic, social, and international arenas. Towards this end they have proposed the following eleven principles, which will be revisited in a later section on Identity Principles:

> Principle 1. Justify the Use of Identity: The Government of Canada will identify individuals and businesses only when it is authorized by legislation, policy or program mandates.
>
> Principle 2. Identify with Specific Reason: The Government of Canada will identify individuals and businesses only when there is a specific reason to do so.
>
> Principle 3. Use Appropriate Methods: The Government of Canada will use acceptable and appropriate means to identify individuals and businesses.
>
> Principle 4. Use a Risk-Based Approach: The Government of Canada will use a comprehensive, risk-based approach to identity management that balances all relevant considerations, including privacy and security.
>
> Principle 5. Enhance Public Trust: The Government of Canada will use transparent identity management processes to enhance public trust in government.
>
> Principle 6. Uphold the Rights and Values of Canadians: The Government of Canada will use identity to uphold the rights and values of Canadians.
>
> Principle 7. Ensure Equity: The Government of Canada, in identifying individuals and businesses, will ensure equity.
>
> Principle 8. Enable Consistency, Availability, and Interoperability: Through a government-wide approach to identity, the Government of Canada will enable consistency, availability and interoperability of government programs and services.
>
> Principle 9. Maintain Accuracy and Integrity: The Government of Canada will maintain the accuracy and integrity of identity information.

Principle 10. Be Collectively Responsible: The Government of Canada recognizes that identity is the collective responsibility of all governments and the individuals they serve.

Principle 11. Preserve Proportionality: The Government of Canada will ensure that identity management activities remain within their intended scope and jurisdiction and are proportional to the stated goals.

Because the final report from the interdepartmental working group is still in draft mode, we were unable to review it in detail for the purpose of our study. Here we will cover some of the other work that TBS has done previously to get an idea of its project plans and purposes. Earlier, in 2005, the Treasury Board Secretariat completed their project to map identity management across the federal government. This report, Identity Management: Mapping the Continuum: Phase 1, was obtained through an Access to Information (ATI) request to Treasury Board Secretariat.

The following highlights the main points of interest in this document, followed by a more detailed summary.

- The report reveals the main problems of identity management for the Government of Canada (GoC). Essentially the GoC administers a great number of programs and services that require that the identity and/or entitlement of individuals be determined before granting access to these programs and services. These determination processes rely on a wide range of identifiers and documents (11 identifiers and 55 documents for the 29 programs and 71 services covered in this report), which have different degrees of reliability, different issuing processes and are from different jurisdictions (federal, provincial/territorial).[69] It shows that identity management is currently far from systematic, and raises some concerns regarding the potential for fraud, etc.

- According to one of the authors of the TBS report who now works on identity management policy at TBS, the goal of identity management in the GoC is "making sure you are dealing with the right person."[70]

- The project finds that currently identity management at the GoC contains "no clear line between proving identity and establishing eligibility. In fact, each identifier/document may

69 The inter-relationships between programs and documents are presented in a matrix in the accompanying document, file name: IDM ID-DOC Interrelationships, which is an appendix to the report.

70 Tim Bouma, "Identity: Setting the larger context and achieve the right outcomes," presentation at CACR 2006 (November 3, 2006), slide 14. Slides and a video of the presentation are available online at http://www.cacr.math.uwaterloo.ca/conferences/2006/psw/agenda.html

serve any combination of 1) proving identity (both as a primary and/or secondary proof of identity) and, 2) establishing eligibility (primary and/or secondary proof of eligibility)".[71]

- Identity management at the GoC relies heavily on identity documents from other jurisdictions, to the extent that 29 of the 55 identity documents are from elsewhere. This is particularly the case in the area of foundation documents, such as birth certificates. TBS concludes that as a result, "identity management is an inter-jurisdictional concern".[72]
- The mapping itself describes the practices and procedures of the GoC. Several models are presented throughout the document and appendices that depict these processes and the ways in which the GoC understand identity, identity management, and identity and entitlement authentication.[73]

Details

The 'mapping report' is the culmination of a mapping project conducted by Treasury Board Secretariat, in conjunction with Public Works and Government Services Canada, Foreign Affairs, and Passport Canada.[74] The report states the project's objectives as two-fold:

> "To map the current state of identity management of individuals requesting programs and services from the Government of Canada", and
>
> "To identify opportunities that will enable the transformation of identity management in Canada with service improvement and greater trust".[75]

To meet these objectives the project conducted a series of workshops (the total number is unknown and they are not described in the report). The federal jurisdictions organizations that participated included: Citizenship and Immigration, Canada Revenue Service, Elections Canada, Indian and Northern Affairs, Passport Canada, Social Development Canada, Veterans Affairs Canada, Canadian

71 Page 40 of the mapping report.

72 Ibid.

73 For the benefit of the avid reader, the most useful/revealing models are: a. States and transitions model, figure 1, p. 14 of the main report; b. Information model, figure 2, p. 16 of the main report; c. Current state of Programs and Services relevant to Identity Management; c. Identity Management Program and Services Alignment Model.

74 The final report and appendices have been provided to the rest of the project team. This report appears to have been intended to be the first in a multi-phase project. It is not clear that any further phases have been initiated or will be initiated.

75 Page 8 of the report.

Border Services Agency, Public Safety and Emergency Preparedness Canada, Public Works, Government Services Canada, and Treasury Board Secretariat.[76]

The project approached the issue of identity management from two perspectives – that of individuals (the users or programs and services) and 'program owners' (those who deliver the programs and services). Although both are represented in the report, this work is definitely from the perspective of government – what government needs in terms of identity verification in order to deliver programs and services only to those who qualify.

The TBS report pays a great deal of attention to defining and delineating a variety of concepts in identity management for the Canadian environment. The report breaks down the category of individuals into Individual Canadians, Individual Non-Canadians, and Undocumented Individuals. Each group is then further broken down into line of business roles (types of individuals who will be clients of particular programs or services). For example, Individual Canadians are delineated as being: students, Canadian forces, veterans, dependants, youth, abroad, naturalized, homeless, inland, by-birth, low income, etc.[77]

The same degree of attention is paid to delineating the needs of individuals and of program owners, and the problem with the current identity management approach and their root causes.[78] The main problems of identity management are divided into two groups according to perspective – the 'program owners' perspective', on one hand, and a 'common perspective,' on the other. The 'common perspective' lumps together both program owners and individuals. There is no individual-specific perspective.[79]

The common approaches to identity management in the GoC are identified as:

- Establishing a unique identity
- Proving individual identity claims
- Eligibility assessment

One of the primary results of this work is a matrix of service interrelationships focusing on types of services and the required documents to obtain that service. The project identified 24 programs, 71 services, 11 identifiers and 55 types of documents in use that are issued either by the federal

76 The final four listed here are identified as being observers in this process. This role, however, is not defined or distinguished from the work of the other participating organizations.

77 For a full list of these delineations, see p. 12-13 of the TBS report.

78 p. 23 of the TBS report.

79 Of course, as 'individuals' were not part of this process (the workshops), it might be too much to ask that the perspective of individuals (essentially those who must prove their identity in some way to obtain government services) were not given the same degree of attention.

government or the provincial and territorial governments. This mapping exercise is by no means exhaustive. However, even with this restricted scope, the range and type of documents in use is noteworthy. The identifiers or documents relevant to a given service are categorized as one of three things:

1. Primary identifier or document (P), which must be provided to obtain the service or participate in a program. It is the essential document.
2. Supporting identifier or document (S), which may be required to corroborate the individual's identity claim
3. Additional identifiers or documents (X), which may be required upon request.

Finally, a number of 'innovations' were identified and rated in order of priority by workshop participants (high, medium, and low). Those identified as 'high'[80] are:

- Identity token accepted by all – fields and data are protected/controlled at source
- Single database of biometric identifiers
- Identity Agency – with a commissioner for oversight among other things
- Finding a way to upgrade other countries to international standards
- On-line enrolment for all services
- Cross-referencing numbers – linking identity (identifiers) across systems
- DNA & fingerprinting (during a single enrolment process) and consent to transfer information
- Foundation document standard
- Vital events – death notification across all programs
- Evolution of Privacy Act in relation to Authentication of Individuals
- Education and communication strategy for Identity Management, particularly as the public needs to be informed of what's kept on individuals, communicate value, raise awareness of risks, identity/theft/fraud
- Tracking of emigrants, border exit controls, etc.

80 It is not clear on what basis these ratings were determined. In addition, there are some numbers in the table presenting the results which are not explained in the report. They could indicate the number of participants who gave each level of rating.

It is interesting to see the severity of some of the measures proposed, e.g., DNA and fingerprinting. This list appears to be simply a display of workshop participants' opinions and certainly emphasizes the bias of increased efficiency in service provision and fraud reduction. Given who participated in these workshops, the support for a large comprehensive system to support the GoC's interests and needs is not surprising, but it certainly reduces the power of these results.

Ultimately, this is a rather thorough mapping in that it delineates a wide range of individuals (including program owners), theirs needs, the problems currently being encountered and their root causes. The research for this report culminates in a tentative vision statement regarding identity management:

> "The Government of Canada aims at promoting and protecting public interest by ensuring efficient and effective identity management and service eligibility assessment through state-of-the-art, integrated and interoperable means and processes resulting greater trust."[81]

Considering the expansive and complex mechanisms under consideration, such a simple statement carries little weight until we get firm statements as to the intentions of the GoC. More attention to individual needs and for the protection of privacy would alleviate more concerns but considering the willingness to consider large-scale systems, and the lack of openness in the workshops to date, leaves us concerned that the idea of centralized identity management has already taken root.

Industry Canada

Industry Canada's Electronic Commerce Branch is playing a global leadership role in addressing what they call the 'trust and confidence agenda'. The driving concerns are the need to protect privacy, in accordance with PIPEDA, the need to protect the Internet and online markets from threats, and to protect and secure transactions and identities on-line. The work on authentication principles builds on other work on cryptography policy, consumer protection, privacy, e-signatures, spam, and Government Online policy framework and regulations.

Extensive consultations have taken place over the past six years, through discussions with industry, academia and civil society both in Canada and abroad regarding identity assurance, leading to its consensus-based 'authentication principles' that will guide future action by government and industry. The principles were devised through a number of meetings held around the country since 2000, and were also informed through Canada's leadership at the Organisation for Economic Co-operation and Development (OECD).

81 p. 39 of the TBS report.

The goal of the work was to devise a set of principles at the 'broad, technology-neutral policy level' to foster competition and ensure a well-functioning market place. The vision was to lay the groundwork for an industry-led approach to authentication, and develop a set of principles to guide development and use of authentication services in Canada. Yet the guiding principle for digital identities is firmly founded in end-user control over identity information. This work resulted in six principles that outline the responsibilities of participants in the authentication process, consideration of risk management, security, privacy, disclosure requirements and complaints handling.

The technology-neutral approach permits the re-assessment of the principles in light of new technological developments, where the participants in the working group discussions can consider the need for additional policy instruments as the need arises. The primary purpose of this approach was a sense amongst the Canadian officials that technology independent policies are needed for establishing assurances for identities in a 'fit for purpose' way.

Statistics Canada's National Routing System

Statistics Canada is responsible for managing information from a variety of sources across Canada. Part of its work entails dealing with the 'registration of vital events', i.e. the recording of births and deaths. SC is proposing a National Routing System:

> "The National Routing System (NRS) is a secure electronic communications environment permitting provinces, territories and federal departments to exchange vital event information. It allows provincial and territorial vital event registrars to validate birth information that is essential to authenticate identity and to notify federal departments of deaths in order to manage changes to program entitlements in a timely manner."[82]

To date it has conducted a pilot where they linked information from data-producing organisations with data-subscribing organisations. That is, the information sharing occurred between the Vital Statistics Offices in British Columbia and Alberta, with Statistics Canada, Passport Office, and Canada Revenue Agency. Of the many benefits mentioned, the list includes 'reduction of fraud' in the case of authenticating identity, and in turn will enhance document integrity and reduce entitlement fraud. It was reported that through the use of the NRS by the Passport office, officials were able to uncover quickly keying errors.

82 John Menic and Mel Turner, "National Routing System for Vital Events," (June 2006), Available at http://www.unece.org/stats/documents/ece/ces/sem.54/3.e.pdf.

Statistics Canada promises that privacy will be protected by ensuring that "data is transferred following established rules and security protocols",[83] but this only covers a smaller component of the data privacy concerns.

Other government departments are looking upon this project favourably. For instance, in response to criticisms by a Senate committee regarding the slow progress on tracking and verifying people's identities, Public Safety Canada responded:

> "The issue of reliable documentation is partially addressed through the National Routing System (NRS), a joint federal-provincial project that provides electronic verification of vital event data. This initiative needs to be funded to achieve full implementation. It should also be noted that amendments to existing Canadian document programs to make them more secure for cross border travel will also have funding implications."[84]

Each province funds its own vital statistics organization, however, and integration of these systems will not be easily managed. The pilot alone cost $4.3m to implement over a two-year time-frame, and ended in March 2006. It was declared "an unqualified success", particularly as technical, legal and policy barriers were overcome to deliver a solution within budget.

Synthesis

There is a great deal of activity taking place in Canada with regards to identity policy. We have only covered a small proportion of these activities, and even then only briefly covered some of these dynamics.

Generally we can see that the main drivers here are more efficient access to government services, immigration and border management, and credential management. Some schemes are even looking to increase user autonomy and control. Interestingly, terrorism prevention does not seem to be a driving concern any longer, at least explicitly. Similarly, law enforcement's goals seem to only be playing a driving factor within the work at TBS and some of the work at the border.

A number of the policy initiatives consider privacy as an over-riding concern, yet we have received reports that this is not always the case and the drive to efficiency and effective identity management plays the greater role. In the appendix to this report we include some analysis of the privacy provisions and jurisprudence under the Canadian Charter of Rights and Freedoms, and how identity issues may be considered.

---

83 Ibid, p.6.

84 Public Safety and Emergency Preparedness Canada, "Response from PSEPC/Portfolio on Reports from SCONSAD," (August 30, 2006), p.8 [from Senate Border Crossing Report]

6. Analysis of Drivers: Key Challenges for Canada

Canada is already embarking on large-scale transformations of existing identity policies and practices. Yet Canada is also making many of the same policy mistakes made elsewhere. This is a nearly inevitable outcome of a set of policy processes that lack open research and deliberation. The lack of information on border and travel documentation is alarming even as we are facing strict deadlines. Alterations to traditional documentation such as birth certificates and driver's licences are being made without consideration of the practical challenges. The purposes behind these changes are constantly mentioned but rarely questioned. Below we discuss some of the hazards of the current Canadian approaches to identity policy, and possible alternatives and ways forward.

Technological Optimism

Far too often biometrics are seen as an immediate and simple solution. For instance, in a report from the Canadian Senate's Committee on National Security and Defence,[85] the Senate Committee posed the following question as though it was trivial:

> "Using biometrics is no longer a particularly expensive, complicated or revolutionary process. Many new computers now accept a simple application of an approved user's thumb to the correct spot on the computer as a password. As for introducing identity cards that swipe, there are very few credit cards and other types of formal identification that do not swipe anymore. So why not come up with a standard set of modern identification that is reliable and easy to use?"[86]

The Committee went on to recommend that by 2007 all people entering Canada (including Canadians) must have a tamper-proof, machine-readable, biometrics-enhanced identity documents that must be "known to have been issued on the basis of reliable documentation."

In a later set of reports, the view was further developed. First, the Senate Committee separated their concerns about borders into three: sea borders, airport,[87] and land crossings.[88] The reports included responses from government departments to their earlier reports. The Senate Committee responds to the government with great impatience, however.

---

85 Canadian Senate's Committee on National Security and Defence, 'Borderline Insecurity', An interim report, June 2005.

86 page 44

87 Standing Senate Committee on National Security and Defence, 'Canadian Security Guide Book 2007 Edition: An Update of security Problems in search of Solutions — Airport', March 2007. Hereafter the 'Senate Airport Report'

88 Standing Senate Committee on National Security and Defence, 'Canadian Security Guide Book 2007 Edition: An Update of security Problems in search of Solutions — Border Crossings', March 2007. Hereafter the 'Senate Border Crossing Report'.

In the Border Crossing Report, the Committee repeats many of the concerns articulated by the U.S. Congress in their appeal for standardized documentation.

For instance:

> "There have been all kinds of Canadian resistance to the United States stiffening its requirements for security identity documentation for people entering its borders, but the Americans are going ahead. So should Canada. (…) There is no reason that they cannot coordinate their efforts in developing sophisticated identity cards that will work for both countries."[89]

The Senate Committee states that developing secure and efficient identity cards is 'critical' and 'should not be beyond the technological capabilities of either of these two very advanced countries.'

Similarly, in the Airport report, the committee supports biometric technology by stating 'the word biometrics instills such confidence'.[90]

The mistake to be so optimistic about technology is perpetrated across political and party lines.

For instance, the Minister for Public Safety stated in 2006 that the drive of technology is essential:

> "I don't know if we'll call it that, but we want good, law-abiding people to have smooth and quick access at all border points — not just North American, but international. We also want to be able to stop people who are a menace or a threat from getting in or getting out, so that's the overall goal. I think it's fair to say that in both Canada and the U.S. we do want some kind of enhanced security provision. Whether that's some kind of a biometric approach, an enhancement on a driver's licence — all of that needs to be explored, so we do want to see enhanced technological capacity in that area."[91]

Michael Ignatieff, deputy leader of the Opposition Party, made an even stronger statement in principle in 2004.

> "Consider the question of a national ID system. Instead of crying "1984," the civil liberties lobby should be taking an honest look at the leaky sieve of the existing driving license ID system and admit how easy it was for the hijackers to talk their way into the ID's that got them onto the planes. Instead of defending a failed ID system, civil libertarians should be trying to think of a better one. One possibility is for Congress to establish minimum national standards for identification, using the latest biometric identifiers. Any legislation

89 (page 17-18 of Senate Border Crossing Report.

90 Senate Airport Report, page 18.

91 'Day Proposes National ID Card', Canadian Press, February 17, 2006.

should build in a Freedom of Information requirement demanding that the government divulge the data it holds on citizens and purge data that is unsound."[92]

The drive to consider applying technology has appeared in almost every country around the world, particularly with the focus on biometrics.

Interestingly, however, there are few assessments of biometric technology in the setting of a national verification scheme. Research labs around the world have conducted studies and assessments of biometric technologies, but the field tests have been insufficient to prove that a biometric scheme can be used against an entire population for general identity management purposes. As such, we are shocked to hear of biometric systems being implemented, such as for biometric driver's licences, without adequate research and assessments of the technologies' capacities and capabilities. This is bad public policy.

The Federal Government, through leadership from Public Safety Canada, is conducting research and consultation on identity technologies. PSC is developing critical insights on reflexivity on roles and responsibilities for implementation of technologies such as biometrics. It has established a cross-government working group on biometrics in order to share ideas and experiences. It researches and assesses biometric implementations to discover whether biometrics are appropriate and effective solutions. According to PSC, they are reaching out to the academic sector, private sectors, non-governmental organisations and other governments to open up the discussion of biometric techniques and implementations. In these discussions they raise issues for the programs including asking questions about the very need for biometric technologies. Such an approach goes some way in avoiding vendor-driven choices. It is their belief that better choices will be made if government departments have a better understanding of biometric technologies and how they can be used, while understanding their limitations, as well as alternative choices and implementation of existing technologies.

It is our hope that PSC and the government working group pays attention to how biometrics can be implemented in dangerous ways. There are a number of experiences around the world about biometrics implemented poorly, which in turn have limited access to government programs and decreased public confidence. It is possible to pick appropriate technologies that deal with ethical and privacy concerns, and even to design the technologies for privacy-enhancing purposes. The greatest worry is that organisations will choose to implement 'neat' technologies rather than proportionate and necessary technologies. We need an open and careful dialogue about the use of biometrics. This needs to be informed by an understanding of their actual performance characteristics, such as their error rates within wide-scale and complex implementations that apply across entire populations, so that we do not unintentionally exclude citizens from gaining access to services. An open and honest

92 Michael Ignatieff, 'Lesser Evils', The New York Times, May 2, 2004.

dialogue is required, not one based mainly on technologically deterministic attitudes and impatience, nor pre-conceived notions of efficiency and privacy-invasion. We remain optimistic that this may take place under the rubric of PSC's outreach work.

International Obligations

It is no surprise that much of the momentum behind many of the current identity programs actually emerge from foreign policies. The U.S. is the leading source of the 'international obligations' upon Canada to enhance our identity policies.

The U.S. is not alone, however, as international organisations have also been involved in leading calls for new policies to ensure the free flow of people across borders. The International Civil Aviation Organisation has created new standards for 'e-passports', under leadership from Canadian officials. The Asia-Pacific Economic Co-operation forum has long been calling for biometric travel documents, through its 'Secure Trade in the APEC Region'[93] and the information experts group on 'Business Mobility'.[94] Again, Canada plays a leadership role here, and reports to APEC on its developments. For instance, in 2006 Canada informed APEC that it was intending to trial facial-recognition and fingerprinting at the border over the next 12 months. We have not seen any open indication of these trials reported to Canada.

In fact we are alarmed by the lack of clarity on plans for changing Canadian identity policies. We are aware of changes being planned, if only because of what we hear from international organisations and from foreign governments, but we remain in the dark as to how Canadian agencies are proceeding. For instance, repeated attempts by this research team to reach out to Passports Canada were ignored and rejected, even as we have established positive working relationships with passport officials in the U.S. and in the United Kingdom, and have positive relationships with other Federal ministries and agencies.

This lack of transparency is an inappropriate method of deciding upon and implementing policy. In other countries where this lack of transparency was resolved through more open consultations and discussions, a number of favourable results emerged. For instance, the U.S. Department of State reversed its opinion on what it considered an adequate level of security in its implementation of contact-less technology in U.S. passports based on project members' outreach and discussions. The U.S. is now going through additional means of securing the identity information on U.S. passports as

93 'The White House, Fact Sheet: Secure Trade in the APEC Region ("STAR"), October 26, 2002.

94 Information Experts' Group on Business Mobility, 'Biometrics Capacity Building Initiative 2006, 22-23 May, 2006.

a result, leading the U.S. to advise other countries that in their programs to implement biometric passports, "you can not underestimate privacy concerns."[95]

The lack of transparency and open deliberation on identity policy transformation can not be attributed to the need for quick implementation of international standards and requirements. Other countries have already started issuing new identity documents to comply with international requirements. This was also a source of frustration for the Canadian Senate committee on national defence and security, in its March 2007 report:

> "The Committee is concerned that the government is dragging its feet and a lack of funding would hinder the government's ability to match deadlines set by the WHTI. If the government continues to move on this I.D. card at the same pace as it is currently issuing passports, then it will be years until the new I.D. card is designed and implemented. Let's move."[96]

Again, we caution against such haste. The committee went so far as to call for politicians to be activated to speed up the process through a public campaign. It went on to reiterate its recommendation in June 2005 regarding the marketing of the idea of secure borders. The Committee then stated that "politicians don't listen to rational arguments – they listen to constituents who will be annoyed with them if something doesn't get done."[97] They then conclude:

> "People in striped pants talking to people in striped pants isn't good enough. Radio ads? TV ads? Comic books? Blogs? How about a Superbowl ad? We don't care. Just do what needs to be done. This relationship is crucial to the economic well-being of every Canadian. Spend some money promoting it – to the right people."[98]

We're not calling for a speedy approach to implementing new identity systems, however, nor an ID card. Apart from the lack of clarity in the decision making processes surrounding the adaptation of international obligations into Canadian identity systems, our greater concern is that these international influences prevent Canada from developing a 'made-in-Canada' policy. That is, Canada should not be considering only how to implement international obligations for specific forms of biometric identity documents, the Canadian government should be looking into the exact type of questions that the PSC working group is recommending: are biometrics appropriate, how well do they work, and what are their limitations?

---

95 APEC, Case Study on U.S. Passport submitted by U.S. Department of State, 2006/SOM2/IEGBM/SEM/005, May 22-23, 2006.

96 Ibid.

97 (Ibid, page 67.)

98 (Ibid.)

For a 'made-in-Canada' policy to emerge, we would expect a national discussion with experts within government, industry, and civil society to discuss how identity policy needs to be reconsidered in light of all developments, not simply because of international obligations and momentum towards biometrics. The 'international obligations' argument may well successfully get a policy through Parliament, or avoid Parliament as we have been told repeatedly was the case with the no-fly list, but it is not a means for managing political concerns with the general population.

Innovative Thinking

When the United Kingdom embarked on an identity policy, the government decided early on that it wanted a large-scale system that was reliant upon advanced technologies, a centralised register with multiple biometrics with real-time on-line access and verification. Having successfully gained Parliament's approval for policy, it now is stuck having to implement the system on time, on cost, and in the real world. The government is encountering numerous challenges along the way.

The one benefit of that UK's exercise, however, was that it raised the level of discussion regarding identity policy. Not to its credit, however, it raised the level to an untenable pitch. Although nearly the entire country was considering identity policy, they were focused overly on the government choice of system rather than looking at the purposes of the policy and some other systems that could be devised to meet those needs.

Identity policy does seek to resolve large and complex problems. But that does not mean that large-scale solutions are absolutely necessary. Smaller and more piecemeal approaches to resolving identity problems can and must be sought. The guiding principle is that these alternative approaches can be proportionate and simple, but must increase public confidence in the processing of personal information.

These smaller solutions are much more specific to the data processing application at hand, while a national identity card solution is inherently the opposite. That is, a national identity card and numbering system usually forces the replacement of existing ministry and agency records-systems, supplanting existing identity policies in favour of the new system, usually offered by other agency or ministry. Rather a culture of identity policy transformation could be raised in each and every government ministry and department, across Canada, to raise the profile of identity policy and to call for the emergence of better identity management practices.

We have already seen innovative solutions emerge, such as the ideas being considered in the British Columbia ministry of health's opt-in identity solution. This solution would also enable other forms of identity management across the public sector, while still permitting the individual to maintain some control over which identities are linked together.

Other solutions are as simple as verifying that the identity credential being issued, e.g. a passport, is not being issued in the name of a dead person. While this form of identity fraud has long been known, passport agencies around the world have only recently moved to implement adequate measures. Similarly, it was recently discovered in the UK that the Passport Service had given 9 passports to the same individual, a suspected terrorist: apart from his real name, he had two passports in other names. More worrying, however, was that he had seven UK passports in his name. How was it possible for him to get 7 valid passports issued by the same Passport Service? Even if he had reported his passport lost or stolen, this data would not be recorded even by UK border officials, and until very recently, the data was not been shared with other governments.

Simpler solutions could lead to reduced costs, less information sharing, and reduced complexities. But we should warn the reader that this is not always the case, and what seems simple and uncontroversial at first can turn around quite quickly.

The National Routing Service sounds promising as a potential micro-solution to the problem of verifying identity details. This project, run by Statistics Canada, would enable information sharing regarding key life events such as birth, marriage, and death, which would permit driver's licencing and passport officials to verify personal identity information. While the prospects are promising, serious questions need to be asked regarding this project. For instance, when news of a similar project plan emerged in Britain the resistance was fierce. The plans for the Citizen Information Project, run by the Office for National Statistics (ONS), was due to cost £400 million to establish, until it was shelved and later subsumed by the National Identity Register. The CIP would create a register of births, marriages, and deaths that could be verified online, through the creation of a "through life record" for everyone in Britain. That is, according to the original consultation document:

> "It is envisaged that an up-to-date 'living record' will be valuable to both individuals and Government for providing identity and for verification purposes... Computerising the records of births, deaths and marriages will make it easier for this information to be used by others. In future, instead of producing a paper certificate when applying for a passport, driving licence or other Government service, the individual will agree to his or her birth registration information being checked and the service provider will do so electronically as part of processing the application. Similarly, the next of kin could agree to an insurance company or bank viewing the death information electronically, thus removing the need to provide a paper death certificate."[99]

Controversy arose over the creation of the database that would act as a central focal point for access to personal information, and could allow access for inappropriate uses. The ONS even ran a risk review process where it identified key areas for improvement and 57 risks, after the UK Treasury

99 c.f. 'UK birth certificates to morph into your life story, and more?', John Lettice, The Register, August 5, 2003.

labelled the project a 'High Risk Mission Critical Project'. Amongst the key 'high risks' were 'Political legislative risks' and 'financial risks'.[100] The Information Commissioner referred to the CIP and its sister schemes as a sign that the UK was heading towards a 'surveillance society' and when the scheme was shut down (or subsumed), the media responded with headlines like 'Big Brother scheme axed'.[101] Political challenges almost always arise.

Statistics Canada does not appear ready to consider any of these dynamics and speaks of 'resounding successes' instead of risks. Yet the NRS is already encountering funding problems, again because of the Federalist structure, where provinces provide much of the information that will be collected. Greater protections and reviews by the Privacy Commissioners must be implemented immediately to raise the confidence levels of Canadians, or at least once they hear of this project. A better public education job must be done in the future to notify citizens regarding such plans, regardless of whether they are pilots or not.

Consent and Consultation

Identity policy has the potential of transforming the relationship between the citizen and the state. Such transformations have been noted previously around the world once new identity policies have been introduced. The mere accumulation of information by government entities introduces new relationships with the data subjects, and new potentials for how that information may be used, and by whom. As we have already seen, Canadians are not confident of how their information is being used, and something must be done about this. The Canadian population must be able to give its consent to enabling these transformations.

Identity policy is also a complex policy arena with multiple interests and actors, some with extensive expertise. These institutions and actors must be actively consulted. 'Neat technology' is too easily offered as solutions to poorly understood problems. We need better consultation processes to bring in all the experience and knowledge that exists across Canada, and around the world, to better understand the risks and challenges of the changes that are taking place.

We are shocked and alarmed how little consultation has taken place to date, considering the broad and significant changes that have already been introduced. This situation was must corrected.

Public consultation and participating in policy making with respect to identity systems is essential, not only because it allows the public to express their positions in these important debates, but it also improves the quality of decision-making. Of course, this improvement is only possible if the motivation for consulting is genuine (those consulting truly want public input), the methods used are

100 Office for National Statistics, 'Risk Status Paper for the Citizen Information Project, September 19, 2005.

101 The Guardian, April 19, 2006

sound, and members of the public have access to appropriate and relevant information on the issues and systems at hand.

While the criteria for strong public consultation practices discussed here are important in public consultations generally, identity policy and systems are particularly challenging because of the complexity of the issues and technologies involved. As a result, providing high quality and accessible information to the public is paramount if people are to be able to understand the implications of the system and develop informed positions and opinions. Furthermore, the issues that arise in these consultations, such as privacy and surveillance concerns, can be quite contentious. Therefore, sufficient time should be allotted for consultation early enough in the policy and decision-making process to allow serious public debate and to allow the outcomes of this debate to inform the development of the systems.

The following describes three categories of criteria[102] necessary to conduct a strong public consultation:

1 Information provision

- Access to information (easy to find and understand)
- Quality of information (complete, objective, relevant)

2 Methodological Soundness

- Representativeness of those consulted
- Duration of consultation activity
- Methods/questions used to gather feedback

3 Genuine consultation

- Timing within planning process
- Use of consultation feedback

Canada has a mixed history with respect to public consultation on identity policy and programs. The following describes two proposed identity and entitlement cards systems in Canada and examines them through this criteria: the Ontario Smart Card Project (OSCP) in 1999-2001, and national ID card proposed under the federal Liberal government and Minister Dennis Coderre (then Minister of Citizenship and Immigration Canada) in 2002-2003. While neither project reached the development

102 K. Boa, Smart Card, Weak Effort? Public Consultation in the Ontario Smart Card Project, Master of Information Studies Thesis, University of Toronto, 2003.

or implementation phases, they are our best examples of public consultation in identity card initiatives in Canada. Since this time, there has been no public consultation on identity policy, neither for broad jurisdictional ID programs, nor for the numerous changes to extant ID programs or new identity documents and systems.

As mentioned above, the Ontario government announced the Ontario Smart Card Project in October 1999. This smart card was intended to serve as both an identity card and an entitlement card for all residents of Ontario (over 12 million people at the time). While it was never entirely clear how many programs and services would become connected to the card, it appears that most of the major programs would be, including drivers' licences, health services, social services, education, as well as a range of hunting and angling licences. This was an extremely ambitious project that in some ways never really got off the ground, partly due to its scope and scale. It was quietly cancelled in December 2001.

The criteria discussed above were developed to evaluate the Ontario Smart Card Project (OSCP).[103] In so doing, it became clear that the OSCP had a weak consultation strategy. Little to no information was available in the public domain about the project. Therefore the information was neither accessible nor of high quality. Furthermore, internal documents obtained through freedom of information requests revealed a Cabinet Directive to "maintain [a] reactive approach and low media profile." This is certainly not an attitude that fosters the provision of information, or strong consultation.

Furthermore, those with whom the OSCP chose to consult were not representative of the large Ontario population. The OSCP advisory council was heavily weighted in favour of banks and card technology companies, although there were a few members representing other interests, including Ontario's Information and Privacy Commissioner. Project staff also consulted widely with representatives of the technology, banking, and credit industry. While they did conduct several interest group consultations, these focused on selected marginalized populations, such as the homeless population.

Finally, no broad-based public consultation was conducted in this project, outside a small amount of opinion polling (based on very few, and often leading questions). Internal documents show that some kind of public consultation was planned. Although no decisions were made about what methods they would use, there was some indications that the public consultation would use the discussion paper and written comments approach. It was clear, however, that there was a strong desire for a short consultation period with minimal opportunity for public discussion, which effectively would prevent a large number of people from participating.

103 K. Boa, Smart Card, Weak Effort? Public Consultation in the Ontario Smart Card Project, Master of Information Studies Thesis, University of Toronto, 2003.

On almost every point, the OSCP consultation strategy was weak with many indications that there was not truly an interest in public participation in this initiative.

The second identity initiative was the proposed national ID card in 2002. When this was first announced, the decision was made to have the Standing Committee on Citizenship and Immigration study whether this was a good idea for Canada. The Standing Committee chose to conduct a public consultation as part of their research into this issue.

Consultation and public debate on this proposal started at a much earlier point than in the OSPC, before any particular initiative was put forward. The question was whether a national ID card should be considered in Canada.

The Standing Committee's consultation process was generally quite thorough. They released a discussion paper (no longer publicly available) and invited written submissions from the public at large. The discussion paper was informative and written in such away as to be accessible. It concluded with a series of questions to which individuals might address their comments. The committee also held public hearings across the country and surveyed international perspectives. The committee produced an interim report[104] released in October 2003, which found that a national ID card was a challenging policy issue with the potential of serious ramifications. They called for a broad public review and debate before going further in this direction. Overall, the interim report was understood to be unfavourable to implementing a national ID card and the idea of a national ID card for Canada was dropped.

The information provision in this consultation was quite strong. The methods were also generally strong, although the period for written submission was a little short (about 1 month). This consultation was significantly more representative in terms of who could participate than anything conducted by the OSCP. Finally, what was most impressive, is that this seemed to be a genuine consultation – it was conducted early enough to influence the decision-making process and it appears that the Standing Committee's findings were influenced by the written submissions received and the presentations at the public hearings.

The model used by the Standing Committee is worthy of emulation in future consultations. As is the approach taken by Industry Canada in its work towards the Authentication Principles, through broad consultations and workshops with experts, industry, and academia. However, given the importance of identity policy and the fact that Canada currently does not have a systematic approach to identity management and documents, it would be useful to consider developing an even broader public debate on what residents of Canada want and feel they need in terms of identity documents.

104 Standing Committee on Citizenship and Immigration, 'A national identity card for Canada?' October 2003, available at http://www.oipcbc.org/pdfs/public/cimmrp06-e.pdf.

Conclusions

In reality most countries with identity cards have relatively simple systems and these have passed the scrutiny and held up to the test of the relationship between the citizen and the state (though they probably went some way in defining that relationship). Changes to those policies are likely to have similar effects as the introduction of a policy where there wasn't one previously. The relationship between the citizen and the state is an odd one: nearly impossible to define, steeped in tradition, history, and myth and worthy of greater consideration, though elsewhere. But the introduction of policy changes or even a new policy will go some way in changing how people regard their governments.

A clear and open consultation, with appropriate consideration of technological opportunities and weaknesses is required. The changes currently being introduced across Canada, mostly behind closed doors, run the risk of generating political friction. The change can be as simple as increased annoyance about yet another administrative step within an already busy life; or one that is a positive feeling of enfranchisement through a sense of recognition of status by the state to the individual. The change can be as sophisticated as enabling the effective and efficient administration of government services while securing society; but as troublesome as being seen as a costly and burdensome intrusion into the lives of the individual only to the benefit of the state. In our research and experiences, everywhere around the world where the introduction of new identity policies was at first considered trivial, it was soon discovered to be amongst the greatest challenges for government.

7. Identity System Strategies

As Canada is already embarking on devising identity policies and designing systems, we believe that we can, from international experience and discussion with key experts, draw out elements of best practice that will assist the evolution of a Canadian approach. Building from the points raised in the previous sections, particularly on 'innovative thinking', 'technological optimism' and 'consultation' we present the technological case for advanced identity systems with realistic goals that implement best practices.

Hazards of a National ID Card System

First and foremost we must address whether a single national identity card system can resolve many of the problems being faced in Canada. With apparently mounting fraud problems, and momentum behind biometric solutions due to border management issues, unless Canada is careful it will set down a hazardous path.

One of the key problems with implementing a national ID card where there is currently no such infrastructure is the 'expectation' issue. That is, government policy-makers begin imagining what their country would look like with a new and expansive identity card system. The excitement leads to the fundamental redrawing of the relationship between the citizen and the state as applications and services are seen everywhere.

It is important to remember that individuals can currently gain access to government and private-sector services without disclosing a universal identifier. In a number of countries with identity cards, this practice is constitutionally essential. Citizens either present entitlements that are not inescapably linked to identifiers or they provide service providers with local identifiers that cannot readily be linked to other identifiers used by the same individuals in other activity domains.

It is also good security to have multiple identities and identifiers. Individuals today are represented by an abundance of local identifiers that are each relied on by only one or a few service providers. Local identifiers enable service providers to identify individuals within their own domains, to create accounts on them, and to effectively deal with fraudsters. At the same time, the segmentation of activity domains ensures that identity thieves (whether outsiders or insiders) cannot cause cross-domain damage, and that service providers and other parties have limited profiling and surveillance powers over individuals.

As an example of bad practice, the UK's proposed national ID card would replace today's local non-electronic identifiers by universal identifiers that are processed fully electronically. This migration would remove the natural segmentation of traditional activity domains. As a consequence, the

damage that identity thieves can cause would no longer be confined to narrow domains, nor would identity thieves be impaired any longer by the inherent slowdowns of today's non-electronic identification infrastructure. Furthermore, service providers and other parties would be able to electronically profile individuals across all activity domains on the basis of the universal electronic identifiers that would inescapably be disclosed whenever individuals interact with service providers.

A variation of the envisioned UK ID card architecture where service providers would delegate the authentication of individuals to central authorities would serve to worsen these problems. These central authorities would become all-powerful in that they would house the power to track and trace all actions of individuals across all service providers in real time. In addition, these authorities would have the power to selectively impersonate individuals wherever they go and to deny them access to services across all activity domains – all at a single press of a central button.

The currently envisioned ID card architecture for the UK also has severe implications for the autonomy and security of service providers. When the same universal electronic identifiers are relied on by a plurality of autonomous service providers in different domains, the security and privacy threats for the service providers no longer come only from eavesdroppers and other traditional outsiders. A rogue system administrator, a hacker, a virus, or an identity thief with insider status could cause significant damage to service providers, could electronically monitor the identities and visiting times of all clients of service providers, and could impersonate and falsely deny access to the clients of service providers.

Components of Effective Identity Systems

Based on our research, we believe that effective identity systems can be designed. But first, we have adopted the following assumptions:

- No national identification system is totally secure, nor can any system ever be immune to the risk of accepting false or multiple identities. Any such claim would not only be demonstrably false, but it would lead to substantial and sustained attacks. Biometrics can be spoofed, registration data falsified, corruption exploited and social networks manipulated. At both a human and a technological level, a fixation on achieving perfect identification across the entire population is misguided and counter-productive. Such emphasis is disproportionate and will lead to substantial problems relating to cost, security and trust.
- The choice of any national identification system should involve careful and sensitive consideration of key aspects of cost, security, dependability and functionality. This exercise is not necessarily a Zero Sum equation where the value of one element is traded off against the value of other elements. The aim of a genuine evolution of thinking is to achieve high scores

on all key elements of the scheme. Only a spirit of openness makes it possible for this outcome to be achieved.

- Public trust is the key to a successful national identification system. Public trust can only be secured if issues of cost effectiveness, dependability, security, legal rights and utility are addressed, and are seen to be addressed. We believe it is possible to achieve these goals while also ensuring a system that offers reliable means of achieving the government's stated objectives.
- A genuinely co-operative approach to finding a national identity solution must involve consultation based on principles as well as objectives.

We have identified a set of components that should guide the design and execution of a national identity system:

- An identity system must be proportionate. Aspects such as complexity, cost, legal compulsion, functionality, information storage and access to personal data must be genuinely proportionate to the stated goals of the identification system.
- An identity system should be inspired by clear and specific goals. Successful identity systems embrace clear objectives that facilitate responsive, relevant and reliable development of the technology, and which limit the risk of exclusion and abuse.
- Identification systems must be transparent. Public trust is maximized when details of the development and operation of an identification system are available to the users. Other than the identifier and card number, no information should be hidden.
- Identity disclosure should be required only when necessary. An obligation to disclose identity should not be imposed unless the disclosure is essential to a particular transaction, duty or relationship. Over-use of an ID system will lead to the increased threat of misuse and will erode public trust.
- An identity system should serve the individual. Public trust will not be achieved if an identity system is seen as a tool exclusively for the benefit of authority. A system should be designed to create substantial economic, lifestyle and security benefits for all individuals in their day-to-day life.
- A national identity system should be more than just a card. Identity systems must exploit secure and private methods of taking advantage of electronic delivery of benefits and services.
- Personal information should be controlled by the individual. Any biometrics and personal data associated with an identification system should remain to the greatest possible extent under

the control of the individual to whom it relates. This principle establishes trust, maximizes the integrity and accuracy of data and improves personal security.

- Empathetic and responsive registration is essential for trust. Where government is required to assess and decide eligibility for an ID credential, the registration process should, to the greatest possible extent, be localized and co-operative.
- Revocation is crucial to the control of identity theft and to the personal security of individuals. Technology should be employed to ensure that a biometric or an identity credential that has been stolen or compromised can be revoked.
- Identity numbers should be invisible and restricted. Any unique code or number assigned to an individual must be cryptographically protected and invisibly embedded within the identity system. This feature will protect against the risk of identity theft and will limit “function creep” through extended use of the number.
- Capability for multiple authenticated electronic identities. An identity system should allow individuals to create secure electronic identity credentials that do not disclose personally identifiable information for use within particular social or economic domains. The use of these different credentials ensures that a “master” identifier does not become universally employed. The master identifier assigned to each individual authenticates sectoral credentials. The use of these identifiers and their control by individuals is the basis for safe and secure use of federated identity systems.
- Minimal reliance on a central registry of associated data. Wherever possible, in the interests of security and trust, large centralized registries of personal data should be avoided.
- Permit secure and private backup of associated data. An identity system should incorporate a means of allowing individuals to securely and routinely back up data stored on their card. This facility will maximize use of the identity credentials.

The design phase for a national identity management system is crucial to its success.

There exist effective, trust-based and non-intrusive methods of establishing the architecture for a national identity system. Over the course of the past two decades, the cryptographic research community has developed an array of entirely practical privacy-preserving technologies that can readily be used to design a better national identity system, if we wish to do so. The system would not need to be centralized and could build on existing societal relationships, to better ensure security and privacy.

Technologies such as digital credentials, privacy-friendly blacklist screening, minimal disclosure proofs, zero-knowledge proofs, secret sharing, and private information retrieval can be used as

building blocks to design a national ID card that would simultaneously address the security needs of government and the legitimate privacy and security needs of individuals and service providers. The resulting solution would minimize the scope for identity theft and insider attacks. A federated solution would also better model and suit existing relationships, whilst ensuring proportionate data practices.

These solutions are well known to the private sector, but are rarely sought out when governments endeavour to develop national identification systems. The reasons for government reluctance to consider these technologies are many. One is the poor design principles behind national ID cards, always perceived as large projects that enable only the full flow of information, rather than the proportionate flow of information. Another significant reason may be because these alternative authentication systems empower individuals to control the amount of information that is disclosed.

If the Government wishes to improve identification in general throughout Canadian society, it needs to consider all the relationships involving the citizen. A national identity system could be designed to allow proportionality and adaptability to local conditions.

Proper use of privacy-preserving techniques would allow individuals to be represented in their interactions with service providers by local electronic identifiers that service providers can electronically link up to any legacy identity-related information they hold on individuals. These local electronic identifiers by themselves are untraceable and un-linkable, and so today's segmentation of activity domains would be fully preserved. At the same time, certification authorities could securely embed into all of an individual's local identifiers a unique "master identifier." This embedded master identifier would remain unconditionally hidden when individuals authenticate themselves in different activity domains, but its presence can be leveraged by service providers for security and data sharing purposes – without causing any privacy problems.

In Federated Identity systems, there is a plurality of Credential Providers (public and private sector) who issue cryptographic security tokens for representing identity in some limited domain, or linked set of domains. The credentials can be designed to be permit records of transactions to be either linkable or unlinkable, or on some spectrum of properties between the two. For example, it is possible for identifiers to:

- be bi-directional or unidirectional, so that multiple identities can be traced from one domain to another, but not in the reverse direction;
- for facts ("attribute values") to be asserted and trusted without disclosing a specific identity;
- for separate identities to be selectively united, either under the control of the individual or another party;
- for infringement of rules to be penalized by disclosure of identity if and only if infringement occurs.

Embedded master identifiers can also be blacklisted across multiple segmented activity domains to ensure that fraudsters in one domain can be denied access to services in other domains, while preserving the privacy of honest individuals. Similarly, service providers would be able to securely share identity assertions across unlinkable activity domains by directing these assertions in digitally protected form through the ID cards of their data subjects in a privacy-friendly manner.

There is thus ample scope for designing identity systems for e-government with rules that can be specifically tailored to intentionally isolated domains of health entitlement and patient records, taxation and benefit claims, border-control and travel, and inter-operation with private sector systems. The rules of each system would constitute the procedure for Data Protection compliance, and could allow good governance of data-sharing for legitimate public policy reasons, whilst limiting infringements of privacy to the minimum necessary.

Such flexibility does not of itself answer difficult questions about how much data-sharing and non-consented identification is justifiable in a democratic society conformant with human rights. However adopting such a fine-grained system allows the processes of democratic legislation and oversight many more options than a monolithic identity system predicated on a unique and ubiquitously traceable identity for each individual. Monolithic systems have much poorer resilience and scaling, and offer nugatory privacy, security, and reliability protection in comparison to Federated ID.

The practice of illicitly loaning Federated ID credentials to other people is discouraged by the fact that those to whom a credential is loaned can damage the owner's reputation, incur liabilities in that domain and learn personal information.

Nevertheless, biometrics may be necessary for applications requiring a high degree of identification (such as travel and border-control). A local-biometric card scheme could be devised which checked for duplicate IDs in a compartmentalized way.

Simplifying the cryptographic details, the card could present a biometric template encrypted with a different key specific to the health system, Asylum/Immigration etc., in such a way that duplicate (encrypted) biometric identities could be detected and traced within a limited domain (e.g. an international border-control system), but ad-hoc data-matching across domains could not occur unless designed and authorized.

Is there a "pressing social need" for a general purpose central biometric database if the interests of national security, the prevention or detection of crime, the enforcement of immigration controls, prohibitions on unauthorized working or employment and efficient and effective provision of public services can all be accomplished with Federated Identity systems and biometrics compartmentalized to specific domains, physically stored only in tamper-resistant devices, and matched by off-line biometric readers?

It is illegitimate, not "sensible", to create a single electronic internal passport just because there is an international imperative to introduce biometrics into border-control systems. It is technologically unremarkable to design an international travel and immigration biometric system, which links to other sector-specific identity systems only to an extent that is foreseeable, explicitly legislated, enforceable, and compliant with data protection rights.

8. Identity Policy Principles

It is common for government agencies when developing identity policy, as with other complex policy areas, to formulate concise sets of overarching principles. These are intended to focus discussion on the central issues and guide subsequent action. In this regard the Government of Canada is no exception. As we have seen, an interdepartmental working group lead by TBS, through consultation with various identity handling departments and drawing on prior collections of identity principles[105], is developing the foundations for a common, government-wide approach to identity management. So far it has articulated the set of eleven Identity Principles enumerated above in section on What's Happening in Canada?

These provide a useful basis for developing identity management policies and practices. They address some of the central concerns, such as the need for lawfulness, transparency, and public trust. Each principle is distinctively valuable[106] and all are necessary. However this list, as well as the conceptual framework and the assumptions that underlie them, are limited in several important respects and so are not a sufficient foundation for a government-wide approach to identity management. This calls for re-conceptualization of basic identity definitions and additional principles derived more broadly. Reflecting a drafting process conducted exclusively within the Government of Canada, this formulation understandably adopts a government-centred view of identity issues. Appropriately, the various principles repeatedly begin with the phrase, "The Government of Canada will …" However, several important dimensions of identity policy are missing – most notably a client-centred focus incorporating the perspectives of individual 'identity subjects' as well as a grounding in constitutional human/civil rights rather than organizational/bureaucratic mandates.

To overcome the limitations with the current Government of Canada approach as discussed above, we turn to outlining an alternative, multi-perspectival framework. It draws on the earlier analysis and critiques, mainly by turning them into positive statements of what would be desirable in developing a 'made-in-Canada' identity policy framework. This section proceeds by first broadening the basic definition identity, then outlining additional identity precepts, rights and principles intended to reinforce and supplement the current framework. It closes with reflections on the challenges facing a principle-based approach to policy development.

105 Mainly these earlier sets of principles were from Canadian and other English speaking jurisdictions. For the list of sets of principles, see Appendix B.

106 However, Principle 10 - Be Collectively Responsible, while recognizing appropriately that maintaining the integrity of a client's identity involves collaborative effort by various parties, should not make it harder to locate individual responsibilities in cases of breakdown or failure.

A Citizen-Centred Definition of Identity

Drawing on the interdepartmental working group definition, we expand the definition of a person's 'identity' to:

> Identity: a reference or designation associated with an individual, consisting of information collected about that person enduringly linked with categorical judgments assigned by the organization used to confirm a status or conduct a transaction.

There are two key points to note here. First, that the essence of identity for citizens is not just their personal information (e.g. name, date of birth, etc.) but also their standing vis-a-vis the organization with which they are dealing. In short, it is mainly about the person's 'reputation' vis-à-vis the organization in question. Secondly, and flowing from this, is that identity records are more than the 'personal information' normally considered in privacy discourse, and specifically includes the categorical assignments made by (identity assigning and data holding) organizations. This broadens attention from the data collection, storage and handling practices that are central to privacy protection measures, and helps focus on the key judgments organizations make about individuals based on the information so collected. Arguably, from the point of view of the individual 'identity-subject', it is this aspect that is the more consequential – i.e. the organizational actions taken upon an individual that affect the outcome of everyday transactions as well as cumulatively a person's life chances.

This enlarged definition of identity also helps show better how much is at stake for individuals as well as governments, and hence why it is a sensitive issue for many people and so often politically charged.

Guiding precept

Based on our prior international review of identity schemes, we found that the greatest risk run by a government in establishing an identity policy is likely political.[107] That is, any policy involving personal data collection and processing, and especially ones that decisively define status in society as identity schemes of national scope do, an identity policy hinges on public trust. If the government doesn't earn public trust in its identity scheme, it risks rejection of the scheme and even its own public mandate. Posed positively, this suggests the following broad precept for guiding identity policy development:

For any jurisdictional identity system to be legitimate and effective in achieving its intended purposes, it must earn very wide acceptance and trust among the relevant public based on transparency and accountability.

107 See Boa, et al 2006, CAN-ID: Visions for Canada's Identity Policy: Understanding Identity Policy and Policy Alternatives.

To give this precept practical substance, more specific principles are needed. There are various ways for developing such principles, depending on the perspective one adopts. Rather than combining these principles into a single integrated list from the start, we will here explore several approaches to identity, each from a different perspective bringing along their associated conceptual presumptions and interests. At this point we are aiming for a relatively comprehensive treatment, which will mean some overlap and duplication, which provides the basis for a subsequent consolidation into a tighter framework with less redundancy.

Some fundamental rights in relation to Identity

Identity documentation in national jurisdictional contexts is the sine qua non of citizenship, and hence needs to rest on, as well as reinforce, the fundamental rights of citizenship. In Canada, these citizenship rights are most definitively spelled out in the Canadian Charter of Rights and Freedoms. Here are some proposed rights pertaining to identity derived directly from the Charter[108].

Integrity of (personal) Identity

> Everyone has the right to the integrity of their personal identity.

This is the most fundamental of the distinctively identity rights, but is currently not (yet) recognized as a right per se. Like the closely related right to privacy, it can be based directly on the constitutional right of "security of the person" (sec. 7) and "to be secure against unreasonable search and seizure" (sec. 8)[109]. In keeping with the definition of identity mentioned above, this includes the right to reliable identity documentation and goes beyond personal information protection to include the judgments

---

108 Note: These are based on a lay reading of the Charter, and not on an expert legal analysis. The Charter can be found at http://laws.justice.gc.ca/en/Charter/index.html. The sections of the Charter used here include 7, 8, 9,10, 11, 15 and 27::

7. Everyone has the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice.

8. Everyone has the right to be secure against unreasonable search or seizure.

9. Everyone has the right not to be arbitrarily detained or imprisoned.

10. Everyone has the right on arrest or detention

a) to be informed promptly of the reasons therefor;

b) to retain and instruct counsel without delay and to be informed of that right; and

c) to have the validity of the detention determined by way of habeas corpus and to be released if the detention is not lawful.

11. Any person charged with an offence has the right…

d) to be presumed innocent until proven guilty according to law in a fair and public hearing by an independent and impartial tribunal;

15. (1) Every individual is equal before and under the law and has the right to the equal protection and equal benefit of the law without discrimination and, in particular, without discrimination based on race, national or ethnic origin, colour, religion, sex, age or mental or physical disability.

(2) Subsection (1) does not preclude any law, program or activity that has as its object the amelioration of conditions of disadvantaged individuals or groups including those that are disadvantaged because of race, national or ethnic origin, colour, religion, sex, age or mental or physical disability.

27. This Charter shall be interpreted in a manner consistent with the preservation and enhancement of the multicultural heritage of Canadians.

109 It should be noted, however, that the Charter jurisprudence so far is very limited in its applicability to establishing a right to personal identity integrity.

about the person made by an authority based on this data, such as profiling, categorical treatment, etc.

Presumption of Anonymous Entitlement

When an individual asserts a claim for entitlement or to conduct a transaction, the initial presumption is that they are so entitled by virtue of their existence. Where there is a requirement to deviate from this, the onus is on the authority to justify the need to go beyond anonymity and establish some form of pseudonymity or collective or individual identity.

This right is founded on Sec. 11d - presumption of innocence.

Judgmental transparency and accountability

Where an agency has made an (enduring categorical) adverse judgment about an individual, this shall not be done arbitrarily. That person has the right a) to be informed promptly of the reasons therefor; b) to retain and instruct expert advice without delay and to be informed of that right; and c) to have the validity of the judgment determined by way of habeas corpus and to be reversed if the judgment is not justifiable.

This is based in Sec 9 and 10. – Arrest or detention.

Equality, diversity and cultural inclusion

Every individual will be treated equally in terms of identity documentation and practices, recognizing our multicultural heritage.

This is based in Sec. 15 – Equality and Sec. 27 – Multicultural heritage.

Fair Identity Practice principles?

It is evident that the policy issues around identity management are closely related to those around privacy protection. Indeed, in some cases they are indistinguishable. However, with the making of enduring categorical judgments about individuals by organizations recorded as part of the person's 'identity package', there are some important distinctive and novel elements about identity that warrant reformulating the familiar privacy principles of fair information practice to take account of these organizational judgments about individuals. Here we re-consider the principal Canadian version of fair information practices, as articulated in the CSA Model Code[110] and consequently PIPEDA, in light of this identity concern, modifying each principle to highlight the corresponding identity issue. This code and the principles it enumerate reflect the perspective and responsibilities of an organization that is a custodian of personal information and that makes and records judgments about individuals on the basis of this information. In what follows, 'identity judgments' refers to the categorical

[110] Derived from CSA Privacy Principles in Summary http://www.csa.ca/standards/privacy/code/Default.asp?articleID=5286&language=english

assignments made by the organization about the individual that become part of the stored records about that individual. Changes to the original privacy/data protection text are shown underscored.

1. Accountability

An organization is responsible for personal information and identity judgments under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

2. Identifying Purposes

The purposes for which personal information is collected and identity judgments made shall be identified by the organization at or before the time the information is collected.

3. Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, as well as in making identity judgments, except where inappropriate.

4. Limiting Collection

The collection of personal information and making of identity judgments shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected and identity judgments made by fair and lawful means.

5. Limiting Use, Disclosure, and Retention

Personal information, including identity judgments, shall not be used or disclosed for purposes other than those for which it was collected or made, except with the consent of the individual or as required by law. Personal information, including identity judgments, shall be retained only as long as necessary for the fulfillment of those purposes.

6. Accuracy

Personal information, including identity judgments, shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

7. Safeguards

Personal information, including identity judgments, shall be protected by security safeguards appropriate to the sensitivity of the information.

8. Openness

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information and the making of identity judgments.

9. Individual Access

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information, as well as the making of identity judgments, and shall be given access to that information and identity judgment making process. An individual shall be able to challenge the accuracy and completeness of the information as well as the identity judgment making process and have them amended as appropriate.

10. Challenging Compliance

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

These ten principles can be supplemented by eight more which can also serve usefully to regulate organizational practices around identity.[111]

11. Identity minimization:

An organization shall minimize the degree of identification required of an individual, preferably conducting transactions anonymously or pseudonymously.

12. Identity Repair and Mitigation

Where a person's identity has been impaired unjustifiably, the organization shall repair and mitigate the harm done, compensate the individual appropriately and take reasonable steps to avoid recurrence.

13. Identity Breach Publicity

When an organization breaches its identity management responsibilities, it shall publicize appropriately any such breach, proportionate to its severity and taking due account of the privacy rights of any individuals affected.

14. Universal Accessibility

111 The last two principles are inspired by Microsoft's '7 Laws of Identity', notably 'laws' 5 and 7 (Pluralism of Operators and Technologies and Consistent Experience Across Contexts) which go beyond single organizations and require at least government-wide coordination. The wording here is drawn directly from the Ontario's Information and Privacy Commissioner (2006) re-interpretation of these laws. As the OPC notes, all seven laws are highly consistent with well-established privacy principles. The other 'laws' that are oriented to individual identity handling organizations, notably 1-4 and 6, can be found in the first 15 principles listed here.

An organization shall ensure that its identity documentation and practices are accessible for all, regardless of age, disability, language preference, education and income. In particular, communications must be clear and understandable via interfaces that are human comprehensible and controllable.

15. Proportionality

An organization shall ensure that the means, criteria and costs of assuring identity are proportionate to the intended purposes, benefits expected, risks incurred and control that can be exercised by each party.

16. Reciprocity

An organization shall ensure that to the greatest extent feasible, identity transactions will be based on reciprocal rights and responsibilities by minimizing the effect of power differentials between it and its clients.

17. Pluralism of Operators and Technologies

The interoperability of different identity technologies and their providers must be enabled by the identity scheme ('universal identity metasystem'). Both the interoperability *and* segregations of identity technologies may offer users more choices and control over the means of identification across different contexts.

18. Consistent Experience Across Contexts: Enhanced User Empowerment and Control

The identity scheme ('unifying identity metasystem') must guarantee its users a simple consistent experience while enabling the separation of contexts through multiple operators and technologies.

Identity system desiderata

Flowing from and assuming compliance with these foundational identity rights and fair practice principles, the following are intended to serve as criteria for assessing jurisdictional identity systems from the perspective of various outsiders (e.g. identity subjects, citizens, civil society organizations, legislators, technical experts). In some cases these repeat themes mentioned above as part of the Fair Identity Practice principles, but here the emphasis shifts from individual usage to the scheme as a whole identity package (of organization, technical system, practices, regulation and governance).

These desiderata range from those deemed important in any large-scale, government-wide infrastructure to those that are specifically relevant to identity systems.

Transparency of objectives, standards, processes, redress mechanisms, … to facilitate individual empowerment and collective accountability

Accountability of the ID agency and its identity activities to democratic norms and institutions, achieved through independent oversight by competent technical, legal and political authorities

Necessity – the need for the identity system is clearly demonstrated

Clear purpose specification – the identity system has a clear, publicly stated and broadly accepted purpose

Effectiveness – the identity system demonstrably achieves the stated purpose

Cost effectiveness – the identity system demonstrably achieves the stated purpose in an efficient manner

Client-Centred – the identity system is organized around the needs and rights of individuals rather than predominantly administrative priorities

Proportionality of means to justifiable risks and desired ends

Minimization of civil liberty risks and effective mitigation of risks where unavoidable

Multiple, purpose specific ID token/systems, rather than a single all purpose ID token/system

Open technical standards to avoid reliance on 'security though obscurity' and facilitate testing by independent experts

Technical neutrality, to avoid vendor dependence

Eligibility authentication rather than identity authentication where feasible (e.g. by using 'electronic signature cards' rather than 'ID cards')

Two-way device and authority authentication so that individuals conducting identity transactions can as quickly and easily check the authority for the collection of personal information and subsequent judgments as the agency checks the individual for identity assurance.

Back-up ID documents readily available in case of loss or theft

No central storage of biometrics, as this presents unacceptable risks of being compromised

Identity system development desiderata

The principles or desiderata sketched so far pertain to properties of an identity management regime once established. The processes for developing the regime in the first place and keeping it 'on track'

need to be consistent with the desired outcome. There are many well-recognized principles for developing and maintaining complex informational/institutional systems. Here we list a few that are especially relevant given the particular challenges that developing a jurisdictional identity system face:

Participatory Design approach

Since a jurisdictional identity system so vitally affects individual clients as well as society more broadly, it is vital that all the stakeholders have an effective influence over its development. This requires the active, facilitated, informed, effective, and resourced civil society participation throughout the development process.

Social Impact Assessment driven

The development should involve from the beginning social impact assessment and design approaches facilitated by competent experts and publicly accountable bodies that take appropriate account of the privacy, civil liberties, equity and other relevant social/cultural issues. Such SIA's should play a formative role in the early stages where they can help avoid problems before they emerge and become difficult to remedy.

Identity practice foundations

The design process needs to be grounded in a clear appreciation of the identity practices of individuals in everyday lived situations. It is conventional in the design of complex informational/institutional systems to take a top-down, deductive approach. But to achieve the good operational fit on which effective performance and public trust rely, the design of identity tokens, systems, rules … need also to be grounded in the particular ways people acquire and handle their identity documents and engage with relevant organizations.

Privacy enhancing/preserving techniques

The full range of up-to-date privacy enhancing (and preserving) technologies (PETs) and methods (e.g. encryption, digital credentials, and others mentioned earlier) should be considered for appropriate incorporation into the identity system.

Ongoing assessment and re-design

To ensure that an identity system continues to meet its objectives even as these may shift, there needs to be on-going mechanisms for feedback about scheme strengths and weaknesses as well as regular systematic assessments of performance, both of which are linked to revising the scheme in light of emerging difficulties, needs, and opportunities.

Reflections on Identity Principles

The sets of principles presented above build on and contribute new ingredients to the prior work that has been done in this area. However, we are still at an early stage in formulating workable guidelines. Their very number and diversity so far illustrate the complexity of the issues involved, but at the same time point to significant limitations in the usefulness of these principles and the need for further refinement.

First, these principles should be subject to tests of necessity, completeness, clarity, parsimony and relevance. It is this last that is probably the biggest challenge since so little is known about the ways that people actually identification in their daily lives. This calls for significant on-the-ground research to elicit the understandings people have about identity as well as what their needs and desires are around this. In the absence of such grounded research, any formulation of general principles is suspect.

A further step is to turn each of these principles into clear tests that can be applied in practice to identity systems, both proposed and in operation. Strong tests, such as those outlined in the next section, will be valuable in assessing clearly whether the corresponding principles have been observed properly or not. Without such operationalization, even the most refined set of principles will be useless, or even dangerous, if they are used to promote identity systems which then cannot be held to account.

9. Conclusions

Based on international evidence, it is clear that the establishment of a secure national identity system has the potential to create significant benefits for society. Secure identity, if implemented in the right way, can enhance security, reduce identity fraud and promote the development of the e-commerce environment. However, an appropriate identity system for Canada should be one based on a foundation of public trust and user demand rather than one based on enforcement through criminal and civil penalties. The goal of public trust would be made possible, in part, through the use of reliable and secure technologies and the creation of a flexible "citizen-centred" model.

More importantly, a national initiative to promote identity policy, through the possible creation of an identity policy framework, would place Canada in a position to create an infrastructure that permits a wide range of practical applications for day-to-day dealings with businesses. This scenario would make use of purpose-specific identity technologies that would give consumers a more secure and simple means of accessing commercial organizations in an electronic environment.

An effective identity infrastructure at a national scale will be a crucial component of the future Canadian economy. This infrastructure will include identity systems and identity policies that are specific to their environment, relevant to the users, and proportionate to their goals. Failure to achieve this level of co-ordination will result in escalating direct cost to government and industry, loss of competitive advantage at an international level, substantially increased opportunity costs, and will hamper future development of markets and services. Seizing global leadership in the field however will enhance Canada's future international competitiveness and permit a more integrated global engagement for industry and government.

To support and enhance a dynamic economy government policy relating to identity management must be seen as a promoter of identity assurance, rather than establishing a monopoly over identity. Previous policy emphases on law enforcement and legal compliance should be refocused on creating new opportunities. An appropriate and economically valuable identity infrastructure needs to support the development of solutions that are based on "buy-in" by citizens, consumers and business. These solutions must be cost effective, flexible, secure, trusted and convenient to use, while being appropriate to their many operating environments.

It is inappropriate for government to model the design of a national identity card infrastructure for citizens after architectures for enterprise identity management that centrally house the capability to electronically trace and profile all participants. The privacy implications for citizens of such panoptical identity architectures would be unprecedented.

Using modern authentication technologies that have been designed to preserve privacy, it is entirely feasible to build a national identity infrastructure that simultaneously addresses the legitimate security and data sharing interests of government and the legitimate privacy needs and autonomy interests of citizens. This approach is not only much better for the citizen, but also for government itself.

Security and privacy are not opposites but mutually reinforcing, assuming proper privacy-preserving technologies are deployed. In order to move forward constructively with its own identity policies and systems, it is important for government to adopt approaches and technologies that provide multi-party security while preserving privacy and the integrity of personal identity.

The provincial and federal governments should move forward in a spirit of co-operation and partnership to achieve these goals. If action is taken concertedly and sensitively it is possible for Canada to build a national identity infrastructure unparalleled in its usefulness and in its foundation of trust and respect for rights.

The Five Tests

Throughout the gestation of an identity infrastructure, that is an identity policy and resulting identity system, there will inevitably be a number of core aspects that should be continually monitored and assessed. These "tests" will help ensure that the scheme is secure, cost effective, robust, trusted and fit for purpose.

Clarity of purpose. An identity infrastructure must have a clearly defined purpose. The most successful identity systems in the world are those that have specific objectives around which the architecture can be securely developed.

Capability. Can an envisioned identity system be built with an assurance of reliability and security? Is the technology robust and stable? Are the purposes set out for it achievable within the current technological capacity and can the relevant partners in its delivery provide guarantees that there is no significant gulf between aspiration and reality?

Alternative measures. Particularly with regard to elements that are costly, controversial, complex or risky, have alternatives to particular aspects and objectives of the identity infrastructure been adequately scrutinized? Are there better ways to achieve the objectives set out for the identity infrastructure that may have nothing whatever to do with identity provisions?

Consultation. Have the views of all stakeholders been genuinely and honestly solicited and considered? Have opposing voices been seen as "critical friends" or merely as "dissenters"? Has the full spectrum of ideas and feedback been adequately and transparently taken into account?

Respect for rights. Has the infrastructure been designed to take into account all aspects of rights and freedoms? Has the architecture been designed with privacy at its core, or as a conditional bolt-

on? Has privacy-friendly technology been engaged to ensure that potential abuses are eliminated or minimized?

Importance of Process

It is fair to say that some identity policies are successful while others are not. It is always important to remember the ideas presented by Denis Coderre when he was advocating a national ID card, ideas that were repeated by Tony Blair in his own defence of the UK card, and in other countries without identity cards: most countries have identity cards so clearly they work

But to just divide identity policies into success and failures is insufficient. One of the key 'tests' is the consultation process surrounding identity policies. There are some identity policy processes that are just and open, and there are others that are not. Returning to the points raised in this report, the political challenges and costs to introducing identity policy change is one of the key challenges for governments and organisations that embark on this path. Identity policy affects individuals as citizens and consumers, and their buy-in is essential to the likely success of the policy.

To just focus on citizen and consumer trust is also insufficient. Modern identity policies are complex and we need the best and brightest to be able to feed into the policy development process. Yet so many modern identity policy processes end up being closed, with limited opportunities for participation and feedback. This not only results in less popular schemes, but when there is no open review we end up with ill-conceived proposals. Because governments have been so unwilling to engage, countless times the various government projects covered in this report had to go 'back to the drawing board'. The results were not only costly, and lengthy delays, but also diminished trust.

The creation of public trust in an identity system depends on a sensitive, cautious and cooperative approach involving all key stakeholder groups. Public trust thrives in an environment of transparency and within a framework of legal rights. Importantly, trust is also achieved when an identity system is reliable and stable, and operates in conditions that provide genuine value and benefit to the individual.

These conditions will not easily be created. They must evolve through a clear, genuine and thoughtful policy process.

Our view, based on the international evidence, is that a appropriate identity policy for Canada would be one based on a foundation of public trust and user demand rather than one based solely on enforcement. The goal of public trust would be made possible, in part, through the use of reliable and secure technologies and the creation of a flexible "citizen centered" model. A citizen-centred model does not mean that the citizen placed under the scope of every government department in Canada, but instead the goal of the system is to enhance the ability of the citizen to choose for himself and

herself the nature of the information and identity exchanges with government departments across Canada.

Any successful, trusted, complex and sensitive policy requires five elements of process: Discourse, Deliberation, Decision, Design and Delivery – each of which is interconnected.

Discourse comprises the vital first stage in the policy process during which policy makers and key experts determine the objectives, necessity and the frame of reference for a potential policy initiative. This stage is crucial in that it establishes an intellectual, legal and moral foundation that will form reference points for subsequent stages.

Deliberation encompasses the majority of the public consultation along with stakeholder engagement and any necessary research work. A consultation process in a domain as potentially sensitive as identity should generate discussion, feed into the policy process, make individuals aware that they are part of the decision-making process and improve the quality of the policy through the solicitation of a wide spectrum of ideas, opinions, and facts. A true consultation process would solicit alternative views, schemes and architectures.

Decision is the weak link in most policy processes. A truly genuine and effective decision stage involves a structured approach similar to the ideal Discourse environment. It should involve the systematic consideration of all output from previous stages rather than using those stages as a mere device to justify a pre-ordained policy.

Design should be undertaken with regard to all previous stages, and encompasses a more clinical approach to the achievement of goals, targets and objectives. The Design stage should, wherever possible, be transparent and accountable.

Delivery is the final stage, and should be foreshadowed as frequently as possible in the Design phase. It is within this crucial element of the process that goals such as trust and broad take-up can be achieved, or where of course they may fail, setting the entire policy process back to phase one.

An analysis of effective identity policies across the world reveals that these five elements are integral to their very success.

Testing Canada

When we embarked on this research on the Canadian identity landscape, we were optimistic that a Canadian identity policy processes would match these procedural elements. Perhaps naively, we believed that Canadian public policy processes would be open at all stages of the process in order to enhance trust and to see the best input into the policy designs.

Looking at some of the policy initiatives identified in the 'What's Happening In Canada' section of this report, here we assess the status of these initiatives by applying the five tests.

Ontario Smart Card Project	**Assessment**	**Test Results**
Clarity of Purpose	Ambitious and complex initiative, with a wide range of programs and services envisioned.	
Capability	Geographic and bureaucratic challenges pervaded, while an overly ambitious timetable was considered.	
Alternatives considered?	Insistence upon biometrics limited design flexibility.	
Consultation and Process	Little or no consultation. Lack of support across the public. Little information was made available.	
Respect for Rights	Privacy problems within the design, particularly with the proposed data matching for reducing fraud.	

There is little surprise that this project was eventually abandoned.

Alberta's Drivers Licence	**Assessment**	**Test Results**
Clarity of Purpose	Drive to reduce fraud and theft, and to increase document security. Residence status adds ambiguity.	
Capability	Technological and administrative choices require further research.	
Alternatives considered?	Unclear.	
Consultation and Process	Unclear. Exemption from FOI and Privacy Act is problematic.	
Respect for Rights	Database of biometrics with police access is highly problematic, though advanced use of PIAs is promising.	

Similar initiatives to 'update' drivers' licences require much greater openness and consideration of alternative technologies to protect privacy.

BC Ministry of Health	Assessment	Test Results
Clarity of Purpose	Drive to enhance online access to health services, though extensibility to other projects is potentially problematic, though consent driven.	
Capability	Using available technologies and techniques.	
Alternatives considered?	Ministry is considering a variety of plans.	
Consultation and Process	Discussions are at early stages and some outreach has started.	
Respect for Rights	Non-compulsory, consent-based, though limited to citizens.	

The BC work is promising not only because it is still at the early stages, but because they have also considered a voluntary regime that can be ramped up to include other services, through consent.

WHTI 'Border Card' System	Assessment	Test Results
Clarity of Purpose	Purpose shifts from terrorism to national security to border management. Unclear how scheme will manage variety of border tasks.	
Capability	Registration and administration of the scheme is highly complex.	
Alternatives considered?	Dangerously no alternatives have been considered because the process is opaque.	
Consultation and Process	Disingenuous consultation. Little consideration in design.	

Respect for Rights	No consideration of civil liberties, trade considerations.	

This is one of the more problematic policy processes because so little is made public other than declarations of needs, but there appears to be even less consideration going into the design – process is driven by political expediency and bravura. This project should not continue without being more open.

Biometric Passport	**Assessment**	**Test Results**
Clarity of Purpose	Driven by foreign influences, though some participation by Passports Canada. Appears limited to use at borders.	
Capability	Unknown and unclear.	
Alternatives considered?	Unknown and unclear.	
Consultation and Process	None. Canadian officials were deeply involved in the international negotiations but communicated little with public.	
Respect for Rights	Unknown and unclear.	

For a policy that is practically owned by Canadian policy-makers, the lack of public discussion is alarming and unacceptable. This project should not continue without being more open.

Treasury Board Secretariat IDM	**Assessment**	**Test Results**
Clarity of Purpose	Clear though how it goes beyond use by specific government departments requires further clarification.	
Capability	A realistic and measured approach, but consideration of implementation and assessment is still required.	

Alternatives considered?	Unknown and unclear.	
Consultation and Process	More consultation beyond government departments is required.	
Respect for Rights	Some consideration but clearer notions of when 'identity' is actually required would help advance trust.	

The TBS work is advanced in thinking but also in its development process. We would have expected more public engagement by this point in its development stage.

Industry Canada	**Assessment**	**Test Results**
Clarity of Purpose	Clearly defined.	
Capability	Clearly defined.	
Alternatives considered?	Extensive deliberation took place.	
Consultation and Process	Extensive deliberation took place.	
Respect for Rights	Extensive deliberation took place and privacy has been given a key position in framework.	

The consultation work by Industry Canada should serve as an international model for dealing with this topic at an early stage and by interacting with all stakeholders across Canada and internationally.

StatsCan National Routing System	**Assessment**	**Test Results**
Clarity of Purpose	Unclear the boundaries of this work.	

Capability	Ambitious goal of datasharing is questionable across the multitude of government systems.	
Alternatives considered?	Unclear.	
Consultation and Process	None.	
Respect for Rights	No indication that privacy has even been considered.	

The amount of public information on this project is quite limited. From experiences in other countries, this could serve to create a massive data-sharing infrastructure with serious privacy concerns, along with data integrity and infrastructure challenges. This project should not continue without being more democratically accountable.

Concluding Remarks

In reviewing and analysing our research on Canadian identity policy initiatives, we are alarmed by the current state of affairs. In the rush and excitement to implement new identity policies, Canadian government departments at the federal and provincial levels are not only considering hazardous identity policy designs, but they are failing to open up the process of deliberation. In so doing they risk developing failing initiatives, or worse, damaging the precious trust relationship between the citizen and government.

In many ways Canada is perhaps failing worse than other countries with even more invasive policies because of the unwillingness to actually start a national dialogue. Of course the quality of dialogues may differ across the world, but it at least opens up the policy-making process. Instead what we have in Canada is an opaque policy process establishing technologies and techniques that are beyond our control. For a policy that is so important, where the stakes are so high, this situation is unacceptable and worse yet, inexcusable.

About this project

This report is the result of an 8-month joint research project between the Faculty of Information Studies at the University of Toronto and the Policy Engagement Network at the London School of Economics and Political Science. This research was funded by the Office of the Privacy Commissioner of Canada, as part of the Contributions Program. This research is an independent study and so should not be interpreted as reflecting the opinions of the OPC.

It builds on our prior work on technology policy issues around the world. In particular we have been independently researching and conducting campaigns on identity policy for more than twenty years. At various stages in our research processes we reached out to colleagues with expertise in areas beyond our own to inform our understandings of this complex field.

Within this project we ran two workshops with participants drawn from various government departments, industry sectors, stakeholders, and experts, bringing their experiences to frame discussion on the issue of identity policy. A discussion paper was circulated at each workshop with our initial findings and statements of challenges and opportunities. Following short presentations from the project team members we heard from participants in formal and informal presentations throughout the 5-hour sessions.

A Vancouver workshop was organized in association with the British Columbia Civil Liberties Association and the American Civil Liberties Union. The event was held at Simon Fraser University's Harbour Centre campus. The goals of this workshop were to:

- Understand the plans for new border controls and the practical implications.
- Grasp the challenges introduced by REAL ID and other new identity standards.
- Assess the economic and cultural repercussions of changing legal conditions.
- Explore the privacy, security, and technological challenges to these new developments.

There were over twenty participants in this workshop, ranging from academia, civil liberties organisations, offices of provincial privacy commissioners, and provincial ministries from Alberta and British Columbia.

The Ottawa workshop was organized in association with the Canadian Internet Policy and Public Interest Clinic at the University of Ottawa. This workshop focused more on the activities of the Canadian Federal Government, and the goals of this workshop were to:

- Analyse the drivers for a national identity policy.

- Understand the changes to the Canadian Passport and explore changes to other travel and immigration documents.
- Build on the work of Industry Canada on authentication principles.
- Explore the challenges and risks in increased data-sharing.
- Discuss the privacy, security, and technological challenges to these new developments.

There were nearly thirty participants in this workshop, ranging from academia, civil liberties organisations, provincial privacy commission representatives, and federal ministry officials.

These workshops played integral roles in informing our research and shaping the outcome of this report, but we do not claim to represent the ideas and opinions of those who participated in our events. We do present the accumulated findings of the workshops in a later section of this report.

The intended audience of this report includes policy-makers, industry officials, non-governmental organisations, academics, and the wider public. The purpose of the report is to explain the dynamics behind identity policy. We hope to show to the reader that identity policy is not as simple as calling for identity cards for all Canadians. Nor is it something that must be avoided at all costs for fear of infringing personal privacy. Identity policy can and must be considered openly, instead of the fragmented and closed manner in which we are altering the relationship between the citizen and the state.

About the FIS research team

The Information Policy Research Program [IPRP] at the Faculty of Information Studies is an on-going program of research examining key public policy issues, notably access, privacy and governance. It is co-ordinated by Prof. Andrew Clement, who is also Director of the Collaborative Graduate Program in Knowledge Media Design. Starting in 1995, IPRP has been serving as the organizational hub for a series of Canadian policy research projects, each with its own research focus, team members and funders. Most relevant to this proposal is the Digital Identity Construction project, which was funded in 2003 by SSHRC's Initiative for the New Economy program. Its aim is to study how the accumulated digital records of individuals' attributes, preferences and prior behaviour increasingly mediate peoples' interactions among themselves and with organizations though a series of case studies including government smart ID cards, call centres, and wearable computers in mobile technicians. Other research the project has supported includes examinations of national ID card debates in Canada, e-passports, and biometrics.

Our work in this area began by investigating the Ontario Smart Card Project, which was proposed in 1999 and quietly cancelled in December 2001. To study this initiative, given the dearth of public information, we initiated a broad series of access to information requests. These records were used

in Krista Boa's masters thesis “Smart Card, Weak Effort? Public Consultation in the Ontario Smart Card Project” (2003) to map and analyse the project’s planning and decision-making trajectory, as well as its public consultation strategy. The thesis also put forward a framework for developing an effective and genuine consultation strategies regarding identity schemes that have implications for privacy. Research has continued to follow proposals for smart ID cards and e-passports and the public debates and deliberations about them, including submission to the public consultation about a National ID card for Canadians in 2003. A predominant issue is the absence of information in the public domain and government’s tight control on how the debate is framed. Professor Clement has been invited to present his work on national identity systems in many countries, including Australia, Finland, UK, France, and the US.

In addition to her ongoing doctoral research on identity systems, identity technologies, and concepts of privacy, anonymity, and identity, Boa is currently conducting information policy research for the OPC on identity management, to obtain information and records for later analysis about various identity management initiatives using ATI. From July 2004 to April 2005, she was senior policy advisor for information management and policy for the Post-secondary Education Review in Ontario (Rae Review), which gave her first hand experience in a government consultation process.

Another doctoral student working in on the Digital Identity Construction project is Joseph Ferenbok, who is studying the development of facial recognition technology and its role in biometric identity documents.

Another recent relevant IPRP project was entitled Implementing PIPEDA. It was funded by the Privacy Commission's Contributions Program in 2004-05 and conducted in partnership with the Centre for Innovation Law and Policy in the Faculty of Law at UofT. This project evaluated the implementation of PIPED Act by reviewing privacy statements posted on the Internet by companies in the telecommunications, airlines, banking and retail sectors.

IPRP research work can be found at http://www3.fis.utoronto.ca/research/iprp/

About the LSE research team

The London School of Economics and Political Science's Policy Engagement Network was established in 2006 to build on the work from the LSE's Identity Project, which in turn built on years of work by leading researchers in the field of identity systems, privacy, and public policy. The LSE team began its research into authentication and identification systems in the 1990s. In 2003 it began research to inform policy deliberation on biometric identification systems in the United Kingdom and subsequently, we launched a concerted initiative to inform the debate on the proposed identity card, first by hosting a number of public meetings on the then “entitlement card”, then convening meetings with industry leaders and government departments. In 2005 this research activity culminated in the LSE's 'Identity Project'.

The first report of the project drew upon the work of over a hundred researchers and experts in technology and policy. The first result was a three-hundred page report with over six-hundred references and footnotes that analysed the policy landscape in the United Kingdom, as well as providing a comparative study of the identity requirements in other countries. In response to policy developments we also released two further reports as well as numerous All-Party briefings for Parliamentarians.

The LSE's output became central to the public debate and political deliberations in the United Kingdom. The reports received a high level of interest from Parliamentarians, industry representatives, technology and policy experts, the media, and members of the general public in the UK and around the world. Subsequent work has been conducted to advise Her Majesty's Treasury on identity policy opportunities.

Our work to date can be found at http://identityproject.lse.ac.uk

The two mentors on the UK Identity Project, Simon Davies and Gus Hosein, have previous and extensive experience in identity systems in other contexts. As members of Privacy International they have organized and led debates on identity systems around the world through research and analysis.

Appendix A: Privacy Protection in Canadian Charter Jurisprudence

Highlights:

- Section 8 of the *Charter of Rights and Freedoms*, which is the main section under which privacy interests are adjudicated, protects against unreasonable search and seizure by the state. There seems to be an interest in understanding privacy in the context of the fundamental rights protected under section 7.[112]
- The two main cases that relate to identity policy are *Hunter v. Southam Inc*. (1984) and *R. v. Plant* (1993), and to a lesser extent *R. v. Tessling* (2004) and *R. v. Edwards* (1996).
- S.8 protects a "reasonable expectation of privacy", from *Hunter v. Southam Inc*. 1984
- Privacy under s.8 "protects people not places", also from *Hunter v. Southam Inc*. 1984.
- Privacy protects a "biographical core" of personal information, that "which tends to reveal intimate details of the lifestyle and personal choices" the individual and is "of a 'personal and confidential' nature".[113]
- The Quebec *Charter of Human Rights and Freedoms* lists privacy, more specifically, "respect for [one's] private life" (s.5) in the fundamental right section, there is no equivalent privacy-focused right protected in *Charter of Rights and Freedoms.*

In this section we review some key cases dealing with privacy in Canadian *Charter of Rights and Freedoms* jurisprudence. It briefly describes the circumstances of each case and highlights the elements (definitions, tests, etc.) that case introduces for privacy jurisprudence. The cases presented here are ordered according to their (likely) relevance to this report and the CAN-ID project.

It is important to remember that the cases discussed here are s.8 *Charter* cases. Section 8 of the *Charter* is the main section under which privacy issues arise. Section 8 states,

> "Everyone has the right to be secure against unreasonable search or seizure."

Therefore, this right applies to law enforcement powers, surveillance, and the collection of evidence without a warrant. There has also been some interest in developing a privacy interest inherent to section 7 of the Charter, which deals with fundamental rights. It states,

112 C.f. *Ruby v. Canada (Solicitor General)* 2002

113 *R. v. Plant* 1993, para. 20

> "Everyone has the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice."

What we provide below is not a complete survey of s.8 cases addressing privacy or an historical analysis of the development of conceptualizations of privacy in *Charter* jurisprudence. Rather we identify a number of key cases and the issues most likely to be relevant to the CAN-ID project. Since s.8 relates to unreasonable search and seizure, some of this case law is tangentially related to identity. However, it does paint a picture of how privacy is understood at the Supreme Court of Canada.

The main privacy cases in s.8 *Charter* jurisprudence[114] are:

Key Cases for this report's purposes:

- Hunter v. Southam Inc., [1984] 2 S.C.R. 145
- R. v. Plant, [1993] 3 S.C.R. 281
- R. v. Tessling, [2004] 3 S.C.R. 432, 2004 SCC 67
- R. v. Edwards, [1996] 1 S.C.R. 128

Connecting privacy to fundamental rights:

- R. v. Mills, [1999] 3 S.C.R 668

Privacy interests in particular spaces (not private homes)

- R. v. Buhay, [2003] 1 S.C.R. 631, 2003 SCC 30

Dealing with bodily privacy

- R. v. Dyment, [1988] 2 S.C.R. 417
- R. v. Arp, [1998] 2 S.C.R. 339

Cases not discussed here but of possible interest (see conclusion):

- R. v. Duarte, [1990] 1 S.C.R. 30
- R. v. Wong, [1990] 3 S.C.R. 36
- R. v. Wise, [1992] 1 S.C.R. 527

114 All these decisions are available online at the following sites: Judgments of the Supreme Court of Canada: http://scc.lexum.umontreal.ca/en/, and CanLii: http://www.canlii.org/en/index.html.

There are also two other Supreme Court cases of interest with respect to privacy that do not fall under s.8 jurisprudence:

- Aubry v. Éditions Vice-Versa, [1998] 1 S.C.R 591, a civil rights case tried under Quebec *Charter*
- Ruby v. Canada (Solicitor General), [2002] 4 S.C.R. 3, 2002 SCC 75, an attempt to determine a privacy right under the *Charter* s.7

Section 8 Cases

Hunter v. Southam Inc., [1984] 2 S.C.R. 145

Hunter v. Southam Inc. is the first case dealing with privacy in Canadian *Charter* jurisprudence. It deals with a search conducted on the premises of the *Edmonton Journal* and the case questions the warrant for this search as being overly broad and not being granted by a sufficiently neutral and impartial arbiter. It is essentially questioning "a statute authorizing a search and seizure" (para. 14).

Hunter v. Southam Inc.'s main contribution to privacy is the introduction of the notion of a "reasonable expectation of privacy" into s.8 *Charter* jurisprudence (at para. 25). In addition, the judgment sets out two other important aspects of privacy protection in this context. First, privacy protects "people, not places" (para. 23), following from U.S. Supreme Court jurisprudence in *Katz v. United States* (1967). The judgment is clear that s.8's protection is not

> "restricted to the protections of property or to associate it with the law of trespass. It guarantees a broad and general right to be secure from unreasonable search and seizure" (para. 22).

Finally, "the proper approach to the interpretation of the *Charter of Rights and Freedoms* is a purposive one" (para. 20). This involves determining what values privacy is meant to protect in a particular case. It also involves balancing an individual's privacy interest with the needs of the state.

The remainder of the judgment focuses on the question of how to assess the particular situations when the public's interest in being left alone by government must give way to the government's interest in intruding on the individual's privacy in order to advance its goals, notably law enforcement (para. 25). The proper way to approach this question is purposive (para. 26).

R. v. Plant, [1993] 3 S.C.R. 281

This is one of the many s.8 *Charter* cases that deal with growing marijuana. The police received a tip that marijuana was being grown in a particular house. They investigated by doing a perimeter search but could not see into the house or find any evidence outside. They then examined the electrical

records for that house[115] and upon determining that the electricity consumption was significantly higher than comparable properties (4 times higher) the police used this fact to obtain a warrant to search the house. The main question is whether a warrant should have been obtained for the 'search' of the electrical records: Is it a search in the meaning of s.8?

The central idea introduced in *Plant* is the concept of the *biographical core*, which has been used recently as in *R. v. Tessling* (2004) to deny Mr. Tessling a privacy interest in heat patterns escaping from his home captured by FLIR technology.

The biographical core perspective is a narrow conceptualization of privacy, deeply informed by traditional notions of privacy. In *Plant*, Justice Sopinka defines the area of privacy protection as follows:

> "In fostering the underlying values of dignity, integrity, and autonomy, it is fitting that s.8 of the Charter should seek to protect a biographical core of personal information, which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual" (para. 20),[116] and
>
> The information protected "must be of a 'personal and confidential' nature" (para. 20).

The biographical core, therefore, excludes a wide range of personal information that is neither traditionally 'personal' nor confidential, but which nonetheless, if exposed or collected might in other approaches be deemed to fall under privacy, particularly if inferences are drawn from that information.

In addition, this is an interesting case because it draws on the nature of the relationship between Mr. Plant and the electrical utility, which is not a relationship defined by confidentiality, a traditional zone of privacy protection. Interestingly, Justice McLachlin (now Chief Justice) in her dissent disagrees with the classification of the type of information held by the utility and argues that a warrant should have been obtained.

R. v. Tessling, [2004] 3 S.C.R. 432

The issue in *Tessling* is whether images gathered of heat patterns captured by a Forward Looking Infra-Red camera on an airplane are admissible evidence if obtained without a warrant. *Kyllo v. United States* (2001) deals with the same technology and its application. The cases, however, have different results. *Tessling* finds that there is no reasonable expectation of privacy in these images,

115 The facts of the case describe the officer "us[ing] a terminal linked to the electrical utility's computer that allowed officers to check electrical consumption at a specified address after entering a password" (p. 2)

116 This is not to be interpreted as exhaustive (see e.g., *Tessling* 2004, para 26).

while *Kyllo* finds there is. *Kyllo* focuses on the location of this surveillance being an individual's home and therefore afforded a high degree of privacy protection. A central question in *Tessling* is whether the technology allows law enforcement to see "inside" the home. The court finds it does not: Using FLIR is "not equivalent to entry" (preamble, p. 3).

A couple important things come up in *Tessling*. First, the court relies on the biographical core, from *Plant* and finds that the information revealed in FLIR images does not meet this standard. Throughout the judgment alludes to a type of hierarchy of privacy interests with bodily privacy and territorial privacy being at the top. In addition, the reasoning in *Tessling* emphasizes the current state of the technology – what it reveals and what inferences may be drawn from that information (para 35). The court believes "currently" the technology does not invade a reasonable expectation of privacy (para 36). The decision does, however, leave the door open to re-evaluate this technology at some later date when it is more advanced. Finally, the case uses a slightly modified "totality of circumstances" test from *Edwards* (1996). The modifications are only such that the questions relate to the facts of this case.

R. v. Edwards, [1996] 1 S.C.R. 128

The main element to come out of *Edwards* is the "totality of circumstances" test to determine whether a reasonable expectation of privacy exists. The judgment lays out the elements of the test as follows:

"The factors to be considered in assessing the totality of the circumstances may include, but are not restricted to, the following:

(i) presence at the time of the search;

(ii) possession or control of the property or place searched;

(iii) ownership of the property or place;

(iv) historical use of the property or item;

(v) the ability to regulate access, including the right to admit or exclude others from the place;

(vi) the existence of a subjective expectation of privacy; and

(vii) the objective reasonableness of the expectation" (para. 45)

R. v. Mills, [1999] 3 S.C.R 668

This case deals with the production of private records, particularly therapeutic records, in criminal cases involving sexual offences. In this case, it is the victim's records that are in question. The accused argues that he cannot make full answer to the charges if this evidence, that the Crown possesses, is not brought forward. The conflict in this case then is between "two principles of fundamental justice … the right to full answer and defence and the right to privacy" (preamble, p. 4).

The link between s.7 and the forced release of therapeutic records is that "security of the person is violated by state action interfering with an individual's mental integrity" (preamble, p.5).

Mills summarizes the areas of privacy protection under that the law, particularly s.8 of the *Charter*, which is closely related to the biographical core. *Mills* describes privacy as a "fundamental human right" (para. 81) and argues privacy protection upholds liberty and the ability to develop and maintain intimate relationships. The *Mills* summary includes: "the right to be let alone" (para. 79), "control of dissemination of confidential information" (para. 80), and confidential relationships. Finally, *Mills* argues that privacy concerns are particularly strong "where aspects of one's individual identity are at stake, such as in the context of information about one's lifestyle, intimate relations or political or religious opinion" (para. 80), much like *Plant's* biographical core.

Regarding *Mills*, the Canlii digest explains, "Given that s.8 protects a person's privacy by prohibiting unreasonable searches or seizures, and given that s.8 addresses a particular application of the principles of fundamental justice, we can infer that a reasonable search or seizure is consistent with the principles of fundamental justice".[117] Thus, *Mills* ties privacy expectations in s.8 to issues of fundamental rights and is cited for having done so in later cases. However, this is not explicitly done by engaging s.7.

R. v. Buhay, [2003] 1 S.C.R. 631

Buhay relates to the seizure of marijuana from a rented locker in the Winnipeg bus station without obtaining a warrant. Apparently, the marijuana could be smelled outside the locker and its existence there was determined by an initial search by station security (which not being agents of the state does engage s.8 protections). The judgment found that the police should have obtained a warrant. It also finds that there is a reasonable expectation of privacy in the contents of a locked locker, despite it being a public place.

The judgment dictates that this sort of adjudication must consider a "totality of circumstances" (which draws on *Edwards*) and follows the reasoning in *R. v. Wong* (1990) insofar as how to frame the question of the case, which must "be framed in broad and neutral terms" (*Wong*, para 50 as cited in *Buhay*, para 19). In Buhay, the question was framed in this way as "whether in a society such as ours persons who store and lock their belongings in a bus depot locker have a reasonable expectation of privacy" (para 19). The judgment focuses on the fact that the items were locked away and expectations of privacy do not only exist in spaces that are owned by individuals – rented spaces are also included.

117 From Canlii Section 8 digest: http://www.canlii.org/en/ca/charter_digest/s-7.html

R. v. Arp, [1998] 2 S.C.R. 339

Arp raises the issues of informed consent and the duration of consent. While in this case the "information" is bodily samples taken in the investigation of two murders, parallels can certainly be drawn with issues of information privacy, to the collection use, disclose, and destruction of information. It also raises the issue of secondary uses.

During the investigation of the first murder, Mr. Arp provided hair samples, but was not charged. While investigating the second murder, DNA was collected from cigarette butts and used to charge Mr. Arp. That DNA sample was then compared to the hairs collected in the first murder investigation and lead to a second murder charge for the first murder. The essential question (for privacy purposes) in this case is "did the admission into evidence of hair samples obtained by consent in one police investigations and used in connection with the separate later investigation offend the accused's right to be free from unreasonable search and seizure granted in ss. 7 and 8 of the *Charter*?" (preamble, p. 3). Essentially the question before the court was whether there are acceptable secondary uses to data that is collected.

One of the main contributions of this case deals with properly instructing the jury when connections between cases are made. The other main element addressed is the consent issue. The summary in the preamble reads:

> "If consent to the provision of bodily samples is to be valid it must be an informed consent. Yet if neither the police nor the consenting person limit the use which may be made of the evidence then, as a general rule, no limitation or restriction should be placed on the use of that evidence. The obligation imposed on the police in obtaining a valid consent extends only to the disclosure of those anticipated purposes known to the police at the time the consent was given. In the absence of any limitation placed by the police or the consenting party on the use to be made of the hair sample, there is nothing inherently unfair or illegal about the police retaining evidence obtained in connection with one investigation and using it in connection with a later investigation which was not anticipated by the police at the time the consent was given. Once the accused's hair samples were taken by the police with his unconditional and reasonably informed consent, he ceased to have any expectation of privacy in them. It was not necessary to consider whether the accused may have had a subsisting privacy interest in the samples or in the information that could be obtained from them after he gave his unconditional consent to the authorities to take the samples" (preamble, p.8).

The findings turn on the fact that Mr. Arp was told when the initial hair samples were collected that "any evidence as a result of the hair sample, it would be used in court" (preamble, p.2), which is interpreted to imply an on-going consent for future uses.

R. v. Dyment, [1988] 2 S.C.R. 417

Dyment also relates to the collection and use of bodily samples, blood evidence in this case. It is also a case of secondary uses of data collected. Following a car accident, Mr. Dyment's "free-flowing" blood was collected for medical purposes at the hospital. Following further conversation in which Mr. Dyment indicated that he had consumed alcohol and medication, the doctor passed the vial of blood to the police, who tested it and charged Mr. Dyment with impaired driving. The main question of this case is whether the collection blood for medical purposes, without the knowledge of consent of Mr. Dyment and then passed to police engages s.8.

The judgment finds that the police acceptance of the blood, collected for medical purposes by a doctor does constitute a seizure under s.8 and its collection should have been governed by a warrant. Bodily samples cannot be taken without consent, nor can samples collected for one purpose (medical tests) be passed to the police and used for another purpose (see also *R. v. Stillman* 1997,[118] which also finds that bodily samples cannot be taken without consent unless governed by a warrant). The case also addresses the confidentiality-based relationship between doctor and patient and thus accords a higher degree of privacy protection to the sample in this case because of how it was collected.

This case also privileges the sanctity of the body as a zone of particular privacy protection. The judgment draws on the language of *R. v. Pohoretsky* (1987), which states "a violation of the sanctity of a person's body is more serious than that of his office or even his home…" *Dyment* goes further stating, "The sense of privacy transcends the physical. The dignity of the human being is equally seriously violated when use is made of bodily substances taken from others …". Further the judgment privileges the body stating, "The use of a person's body without his consent to obtain information about him, invades an area of personal privacy essential to the maintenance of his human dignity" (para 27).

Non-Section 8 Cases

Aubry v. Éditions Vice-Versa, [1998] 1 S.C.R 591

Aubry is a case tried under the Quebec *Charter of Human Rights and Freedoms*, s. 5, which states, "Every person has a right to respect for his private life." In this case, Ms. Aubry was photographed without her consent while sitting on the steps of a public building. This photograph was then published in *Éditions Vice-Versa*, without her knowledge or consent. She argued that her privacy had been violated.

118 This case is not summarized here since it is similar to Dyment and does not seem to add anything of particular interest to the CAN-ID project.

It is understood that "the right to one's image is an element of the right to privacy under s.5 of the Quebec *Charter*" (preamble, p. 3).

Ms Aubry won her Supreme Court challenge and was awarded $2000 in damages plus costs. The case turned on whether "prejudice was sustained" as a result of the actions of *Éditions Vice-Versa* in publishing the photo. The judgment found that while there was a conflict between freedom of expression and the right to control one's image, "there is an infringement of a person's right to his or her image and, therefore, fault as soon as the image is published without consent and enables the person be identified" (preamble, p, 3).

Ruby v. Canada (Solicitor General), [2002] 4 S.C.R. 3

Ruby v. Canada deals with ss. 7 and 8 of the *Charter* as well as the right of access to one's own personal information under the *Privacy Act* and its exemptions, particularly for national security and interactions with foreign governments. Ruby requested his CSIS file and CSIS refused to acknowledge whether or not it exists, cited the above exemptions to releasing information. The specifics of this case are quite legalistic and the exact issues being tried are procedural. What is relevant for the purposes of the CAN-ID project is the relationship between privacy (as a right) and the fundamental rights under s.7 of the *Charter* "life, liberty and security of the person".

The judgment does not deal with the issues under s.8. It argues that they are "entirely subsumed under s.7" for the purposes of this judgment (para 30). Ruby's argument is

> "the right to security of the person protected by s. 7 of the *Charter* protects the right to privacy in a biographical core of information to which an individual would wish to control access. This biographical core of information includes information which tends to reveal intimate details of lifestyle and individual personal or political choices. This right to privacy is said to include a concomitant right of access to personal information in the hands of government in order that an individual may know what information the government possesses. This, in turn, will ensure that government action in the collection of personal information can be scrutinized and inaccuracies in the information collected may be corrected. Any limit on this right to access must accord with the principles of fundamental justice" (para 31).

The judgment also describes the Federal Court decision in the case (the previous stage prior to going to the Supreme Court), which observed that

> "that there is an emerging view that the liberty interest in s. 7 of the *Charter* protects an individual's right to privacy. They accepted the appellant's view that in order for the right to informational privacy to have any substantive meaning it must be concerned both with the acquisition and the subsequent use of personal information. Recognizing that one has a legitimate interest in ensuring that information has been properly collected and is

being used for the proper purpose, the Court of Appeal held that the right to privacy includes the ability to control the dissemination of personal information obtained by the government" (para 32).

However, the Supreme Court finds that "it is unnecessary to the disposition of this case to decide whether a right to privacy comprising a corollary right of access to personal information triggers the application of s. 7 of the *Charter*" (para 32). Therefore, the Supreme Court has not yet determined the connection between privacy and the fundamental rights granted in s.7 of the Charter.

Conclusions

Essentially the notion of privacy protected under the reasonable expectations tests and definitions found throughout the case law is quite traditional – it focuses on the home, things and information that are kept secret, and confidentiality. While the case law does make a point of clarifying that privacy interests it is not limited to homes – privacy "protects people not places" – understandings like the biographical core (*R. v. Plant*) reduce the possibility of a privacy interest in non-traditional spaces or with respect to information not traditionally understood to be private.

Three cases of potential interest not discussed here contain some interesting arguments by Justice LaForest (*R. v. Duarte* 1990, *R. v. Wong* 1990, and dissenting in *R. v. Wise* 1992). La Forest argues for a broader understanding of privacy based on the understanding that technologies, particularly surveillance technologies are a "different order of magnitude" in their power to infringe what was previously protected by use of less sophisticated technology. While these cases are interesting and LaForest's reasoning powerful from a pro-privacy perspective, they have not been discussed at length here because his position seems to have been superseded in surveillance cases with the decision in *Wise*, and now in *Tessling*.

Supreme Court privacy jurisprudence under the *Charter* occurs almost wholly within the provisions of Section 8 protections against unreasonable search and seizure. This context makes much of the jurisprudence only tangentially relevant to questions of identity and personal information. Aside from the notions privacy found in *Hunter & Southam Inc*. (1984), which introduces the "reasonable expectation of privacy" test and clarifies that privacy is intended to protect people and not only places, and *R. v. Plant*'s (1993) "biographical core", which transcend the context of search and seizure, most of the case law is difficult to separate from the context of law enforcement practices and search and seizure. This decreases to some extent the ability of this case law to inform questions of identity. However, it does reveal the Supreme Court's approach to privacy, which is one that privileges traditional notions of zones of privacy, name the property, secrecy and confidentiality, and the body. While these are indeed worthy of significant protection, they do little to help in determining the existence of privacy interests in contexts where personal information is gathered from "public" sources, is transactional data, and is connected to identities stored in central databases

or registries to develop fuller digital identities. The notions that appear in the case law make it more difficult to find privacy interests in these sorts of information and could make it more difficult to identify the harms associated with these practices.

Both Dyment and Arp deal with issues of consent and secondary uses of information collected. While the context here is law enforcement, these cases also relate to broader issues of secondary uses of information and consent. The court found that Mr. Arp did not limit his consent and neither did the police so it was still valid for secondary uses. There is a problem here that also exists in the realm of personal information – the data subject is not necessarily in a position of sufficient power to negotiate the terms of consent.

Finally, a number of the cases discussed here link privacy to fundamental rights. While there is no definitive decision that makes this connection to section 7 *Charter* rights, there seems to be movement in this direction. Understanding privacy in the context of section 7 might be more beneficial for issues of identity and privacy than the rights established in section 8 in that it would remove privacy from the narrower context of intrusion by the state for the purposes of law enforcement. However, the degree of benefit would depend on how privacy is conceptualized. If the Court relies on the reasoning found in *Plant* and a traditionally informed notion of privacy like the "biographical core," the benefit of using s.7 might not be as great.

Appendix B: Sources for Identity Principles

7 Laws of Identity (Microsoft)

http://www.identityblog.com/?page_id=354

7 Laws of Identity The Case for Privacy Embedded Laws of Identity in the Digital Age (Information and Privacy Commissioner, Ontario, 2006)

http://www.ipc.on.ca

Principles for Electronic Authentication (Industry Canada)

http://strategis.ic.gc.ca/authen

Cross Jurisdictional Working Group on Identity Authentication and Authorization

http://www.iccs-isac.org/eng/pubs/iaa/IAA_TOR_final.pdf

Identity Authentication and Authorization in Electronic Service Delivery - An Ontario Perspective (Discussion Paper, V1.2, May 5, 2003), Government of Ontario

http://www.accessandprivacy.gov.on.ca/english/pub/iaa.pdf

CSA Privacy Principles in Summary

http://www.csa.ca/standards/privacy/code/Default.asp?articleID=5286&language=english

Federal/Provincial/Territorial Identity Council Principles

"Identity in Canada: A Policy Framework" (2002) (not available online)

CBSA Identity Principles (Internal CBSA document)

HRSD/SDC Identity Policy Principles (Internal HRSD document)

Identity Project Report (London School of Economics)

http://identityproject.lse.ac.uk/

National Electronic Commerce Co-ordinating Council Consultation of Electronic Authentication. (US)

Identity Management report http://www.ec3.org/Downloads/2002/id_management.pdf

Australian Privacy Commissioner, Proof of ID Required? Getting Identity Management Right

http://www.privacy.gov.au/news/speeches/sp1_04p.html

Identity Management for Australian Government Employees (IMAGE)

http://www.agimo.gov.au/__data/assets/pdf_file/51358/IMAGE_Privacy_Management_Strategy_1_0__2_.pdf

New Zealand Evidence of Identity Framework

http://www.ethnicaffairs.govt.nz/diawebsite.nsf/wpg_URL/Resource-material-Evidence-of-Identity-Standard-Evidence-of-Identity-Standard-(html-version)?OpenDocument