A National ID Card by Stealth?

The BC Services Card

Privacy Risks, Opportunities
and Alternatives

by Kate Milberry &
Christopher Parsons

In partnership with
The British Columbia Civil Liberties Association for
The Office of the Privacy Commissioner of Canada
Contributions Program

Table of Contents

Summary 5

1. Introduction 7

2. The Importance of Identity Policy 13

3. Identity Policy in British Columbia 19
    The Evolution of "Government 2.0" 20
        BC's e-Health Initiative 20
        Information Sharing and the e-Health Act 22
        Information Access Layer 23
    Identity and Information Management 24
    Terrible Track Record on Big IT Projects 26

4. Transforming Identity and Information Management in BC 31
    Drivers and Inhibitors 32
        Identity Theft and Health Care Fraud 33
        Cost/Savings 34
        Security 35
        Better Service Delivery/Improved Patient Safety 36
        Privacy Professionals 36
        BC Information and Privacy Commissioner 38
        Legislative Changes 39

5. (Lack of) Transparency 43

6. The BC Services Card 47
    Physical Attributes, Technical Specifications and Database Architecture 47
    Biometrics/Facial Recognition Technology 49
    Near Field Communication 50
    Database Architecture 50

7. SecureKey Technologies: Wrapping up Canada? 55

8. Privacy Risks and Security Vulnerabilities 57
Enrolment 58
Physical Card Protections 59
Data Management and Security 60
NFC Chips 61
Mobile Migration & Personal Computing 62
Function Creep 64

9. A National ID Card for Canada? 67
The Birth of a Pan-Canadian Identity System 68
Drivers 69
"Barriers" and Challenges 69
Identity Principles 71
Privacy and Security 74
Cyber-Authentication Renewal Project 75
Private Vendor Credential Brokering 77
The Trouble with Federated Authentication 78
From Identity Authentication to Identity Assurance 80
The Card Cartel 82
Federal and Provincial Privacy Commissioners 84

10. Alternatives 87
Considering the User 87
What is a User-Centric Approach 88
A User-Centric Approach Meets Identity Requirements 88
The Comparative Merits of the User-Centric Model 90
Meeting the 'High-Water' Standard of Identity Privacy 92

11. Recommendations 95
Normative Recommendations 95
Policy Recommendations 98
Technical Recommendations 100
Conclusion 102

SUMMARY

For the last several years, British Columbia has been developing the technical infrastructure and legal framework for a comprehensive integrated identity system as part of its "technology and transformation" approach to governance. Otherwise known as "Government 2.0" or e-government, this approach will aggregate the personal information of citizens in order to link and share this data across government bodies. The BC Services Card is the latest in a series of major information technology projects that is part of the Government 2.0 mandate. It is a mandatory provincial ID card that enables access to a range of government services, beginning with health care and driver licencing. The BC Services Card is a key element of unprecedented changes in the way the province collects, accesses and shares personal information, including highly sensitive health information, amongst departments, agencies and even private contractors.

The card is just part of BC's wide-ranging vision for integrated identity and information management—a vision that scales and interoperates on a federal level. Indeed, the system is not only envisioned to extend to other provinces, in essence forming a pan-Canadian identity architecture, but the ID card is expressly intended to provide authentication conducted by the private sector and facilitation of commercial transactions governed by PIPEDA and applicable provincial private sector privacy legislation. The importance of developments with the BC card for national identity management cannot be overstated: the BC Services Card model is interoperable with the federal system, and thus a (proto) Canadian ID card, and is also meant to be used for commercial and e-commerce transactions. Thus, developments in BC have critically important implications for ID systems provincially and federally, and involve both the public and private sector.

This report examines the normative, technical and policy implications of the BC Services Card and the federal and commercial implications of the technical systems underlying the Services Card. Throughout the report, the ID system is examined from the perspectives of security, privacy and civil liberties, and generally echoes the Information and Privacy Commissioner for BC's call for broad and meaningful public consultation before Phase II of the card program is implemented. Emergent from the analysis of the Services Card is a call for the Office of the Privacy Commissioner of Canada to work with provincial privacy commissioners to issue a joint resolution on the applicable privacy and security standards for the provincial systems on the basis that they will ultimately compose the national federated system. The report concludes with provincial and federal recommendations for designing an identity system that is secure, privacy-protective, trusted and fit for purpose.

1. Introduction

In our increasingly digital age, the prevalence of social media, ubiquitous computing and mobile work/play environments has prompted government efforts to leverage the convenience and efficiency promised by computer networks. Canadians are using digital tools in their daily lives with growing frequency. The government of Canada wants to develop an approach to identity management that will facilitate online access to government services and e-commerce, and is working in concert with private sector interests like the payment card industry to accomplish this goal. After failing to develop a centralized system, the federal government is now set on the goal of a harmonized, federated identity system that involves enrolling provincial and potentially municipal jurisdictions. British Columbia has stepped up to be the de facto first major provincial pilot for such a federated identity system. For this reason, developments in British Columbia are crucially important and need urgently to be discussed in a broader national context.

The government of BC has been attempting to position itself as a leader in "transformation and technology" strategies. To that end, the government announced that it would reinvent how the province manages the personal information of its residents. This project, dubbed "Government 2.0" is a speculative—rather than evidence-based—strategy driven by a logic that upholds technology as the solution to social problems. Moreover, Government 2.0 is motivated by goals of technocratic efficiency—cost-savings for government and convenience for citizens—as well as the desire for "modernization".

The "transformation and technology" approach depends on government-wide collaboration that is meant to provide online service delivery via integrated, interoperable databases. While "Government 2.0" is described as a technical "upgrade", it actually demands a radical restructuring of identity management and information sharing practices. In the original paradigm, government areas like Health, Justice, Social Development and Child and Family Development each held residents' information in localized electronic databases that were not linked to other government databases. Moreover, there were limited technical means of connecting stored information internally across government or externally with government agents or service providers. These discrete databases created "silos" that acted as natural impediments or "road bumps" to the inappropriate sharing of personal information, whether accidental or contrived.

In the BC government's view, these silos interfere with the timely and efficient delivery of services, and constitute barriers that ought to be removed to provide citizens with "seamless" service delivery. Government 2.0—or "joined up" government—thus seeks

to ensure the free flow of citizens' personal information across government ministries, accessible via hundreds or thousands of portals. As such, it contrasts starkly with the way Canadian governments have traditionally handled citizens' personal information. Indeed, Government 2.0 abandons some of the universally accepted privacy principles in favour of a technological solution to privacy protection. This approach is worrisome given that such "solutions" may be overcome through policy, legislation or technical failure. Such failures take on heightened importance given the known security vulnerabilities that attend the digital identity management system that is being deployed in British Columbia, and the impetus towards disseminating the BC model to other jurisdictions to form the integrated federal system.

Within the e-government framework, computer networked data sharing and data linking comprise the foundation of the new paradigm for the province of BC's identity and information management (IdIM) system. The BC Services Card is a lynchpin in this scheme insofar as it provides the technical capacity to link citizens' personal information stored in disparate government databases. Introduced in February 2013, the card replaces the "outdated" health CareCard, which the government claims was insecure and the cause of untold losses due to medical fraud. It is the inclusion of an embedded computer chip, however, that transforms the Services Card from a relatively limited access or entitlement token into a potentially more significant surveillance device. Inside the computer chip is an ID tag, or "unique identifier" that facilitates linking the cardholder's personal information across a range of government services. In essence, the card is the physical instantiation of a digital "master key" to personal identity information held by the province. The card is mandatory, with all BC residents required to enroll by 2018. At the moment, it is optional for citizens to marry their driver's licence to the BC Services Card, creating a "combo" or hybrid card. The province has pledged that more government services will be "bound up" with the card in the future and the technical requirement that the BC Services Card be interoperable with the federal system evidences the intent that federal government services will ultimately be accessible through the use of the Services Card as well.

British Columbia's transformative approach to identity and information management policy raises a host of concerns, as well as questions. Concerns around privacy, identity integrity and democratic governance are commonly associated with "joined up" and card-based identity systems. First among the questions is: why do we need the card? This question has not yet been fully canvassed by the government, although the card is now operational. Neither has it been put to British Columbians: to date, there has been no public consultation on the issue of an electronic provincial ID card, nor debate around the merits and risks of the associated integrated identity management infrastructure. BC's Information and Privacy Commissioner has been unequivocal in

calling for a “fulsome public consultation” before the government proceeds to Phase II of the BC Services Card program.

Indeed, a distinct lack of transparency has characterized the design and development process of the BC Services Card, despite the fact that it enacts a new way of dealing with citizens’ personal information. Very little information about the card was publicly available prior to its launch, though since then the government has posted some documentation online. Requests by researchers on this project to interview the Minister of Health, the Minister of Citizen Services and Open Government, and the Chief Information Officer, representatives of the three key government agencies involved, were ignored or denied. A representative in the Office of the Chief Information Officer (OCIO) agreed to an interview, but would not allow it to be recorded. Freedom of information requests made by the BC Civil Liberties Association and the BC Freedom of Information and Privacy Association met lengthy delays or were returned with “no responsive records”.

The government’s secrecy and apparent obfuscation raise another question: what is being hidden? Such a lack of openness breeds suspicion and tests the public’s confidence in government. In the absence of transparency, there can be no public accountability, which is fundamental to democratic governance. If members of the public and experts outside of government cannot scrutinize “transformative” programs like the BC Services Card then there are few assurances that the government is acting in the best interests of its residents.

Citizens are compelled to trust that their government appropriately handles their most sensitive personal information. The province acknowledges that Government 2.0 will “require citizens and the public service to trust that steps can be taken to improve access to government without jeopardizing safety and security”.[1] So far, however, this has been a blind trust on the part of BC’s residents. In prioritizing the technical and administrative needs of the province’s integrated identity infrastructure, and excluding residents from the process, the government risks losing the trust of the people. Public debate, consultation and participation in policy making are essential when dealing with as consequential and complex an initiative as an identity system. Their absence in the implementation of the BC Services Card points to larger issues and concerns are exacerbated by the broader scope of the project, which is a national federated system,

1 BC Public Service. nd. *Citizens at the Centre: BC Government 2.0.* Victoria, BC: Government of British Columbia, www.gov.bc.ca/citz/citizens_engagement/index.html.

extending beyond the bounds of provincial jurisdiction and extending very deliberately into the private sector as well.

In addition to questions regarding the necessity of the BC Services Card and the lack of transparency and public consultation, there are serious concerns raised by the unprecedented data linking enabled by the technical infrastructure underlying the card. Accompanying such linking is the potential for government and its private sector technology providers to track, monitor or profile system users. This is an inherent threat to citizens' privacy, particularly as the temptation to "make use" of the vast amounts of data generated through online service delivery encourages function creep, or the use of systems for more and different purposes than originally intended or approved. Such function creep might threaten the life chances of users who could be denied services or entitlement due to profiling or other cumulative assessments made by the identity system. The shift from a reliance on legislation and fair information and identity principles to ensure privacy, toward a prioritizing of technology to safeguard residents' personal information is troubling, particularly given the known human and technical weaknesses associated with computer networked systems and e-government more generally.

Closely connected with concerns about privacy are security vulnerabilities that attend most sophisticated information technology (IT) projects. The access to personal information repositories or data portfolios via the unique identifier, called a Personal Account Number (PAN), embedded in the BC Services Card raises data security and confidentiality concerns.

The more linkages within the system and the more portals there are to access that system, the greater the "attack surface"—or range of ways that hackers, cybercriminals or other "bad actors" might enter, exploit, or otherwise compromise the card's data infrastructure. The full range of attack surfaces is as yet unknown: the BC Services Card proposes an untold number of services, portals and backend users, making the range of ways a bad actor might try to undermine the system challenging to empirically gauge. The government promotes the card as "secure" and describes its technical infrastructure as privacy protective, but has not demonstrated this to be the case.

In what follows we describe the BC Services Card in as much detail as possible, given the limited primary documentary evidence. We highlight civil liberties concerns associated with the card, such as those related to transparency, privacy and security, situating these in the broader context of the province's plans for an integrated, interoperable identity system.

This report maps, analyses and makes recommendations about the current identity policy landscape in British Columbia, locating it firmly within the national context. It

considers how the BC Services Card could function as a de facto provincial ID card and how it aligns with plans for a federated national identity system. Given the historical unpopularity of a national identity card for Canada, we ask the question: is the BC Services Card a national ID card by stealth—the prototype for a card-based identity system at the federal level that is being slipped in through a provincial back door?

British Columbia has just begun implementing a novel identity system which will impact the privacy and security of highly sensitive personal information and likely influence the adoption of similar or identical systems in other provinces and territories. As a result, BC's decisions have the potential to significantly shape how the federated federal system is developed and implemented. While the government includes the language of privacy protection in its promotional material, it is unclear that this is a priority, with other goals—like presumed cost savings and efficiency—taking precedence.

But the province has not reached the point of no return in this identity system. The computer chip, which contains the key to residents' data portfolios, is not yet activated. The data linking infrastructure envisioned by the government is not fully deployed, and integration with the Services Card will not occur for five years. As such, this is a rare second chance, an opportunity to get identity policy in British Columbia "right" and to introduce an appropriate and workable model for broader national dissemination.

Throughout this report we have adopted a more expansive definition of identity than the one guiding policy development at the federal and provincial levels. Thus, we include residents perspectives, ultimately recommending a digital identity management system that would limit some of the potential data mining enabled by these programs and associated system. In the expanded definition, the imperative for the citizen is the preservation of status and entitlement within the identity system, and thus does not focus exclusively on the government-centred objective of ascertaining identity to provide streamlined services.

Chapter 2 outlines the importance of identity policy, noting Canada's brief flirtation with a national ID card, and the evolution of federal policy toward an integrated model of digital identity management. In Chapter 3 the lens focalizes on identity policy in British Columbia, describing the policy's foundation in the province's e-Health mandate and noting that the government's terrible track record on major information technology projects has not seemed to slow the implementation of the BC Services Card. Building upon this foundation, Chapter 4 examines the drivers and inhibitors of the transformation of identity and information management in BC. Chapter 5 addresses the lack of transparency that has characterized the Services Card since its

inception. Chapter 6 focuses on the physical and technical attributes of the BC Services Card itself; this is followed by a discussion of the role of SecureKey Technologies, the main vendor in the design and development phase, in Chapter 7. Chapter 8 outlines the associated privacy risks and security vulnerabilities. Chapter 9 articulates the case for a national ID card for Canada, tracing the evolution of policy development in this direction, while Chapter 10 examines a privacy protective alternative to the technical system that underlies the BC Services Card. The report concludes with Chapter 11, which offers a series of recommendations for a more secure, privacy protective and democratic identity infrastructure for identity management in Canada.

2. The Importance of Identity Policy

Identity policies are emerging at all levels of government, driven in part by a sense of urgency to keep up with new realities wrought by ubiquitous computing and "always on" internet access. These policies, which are meant to integrate "unconnected" electronic systems for identity and information management (IdIM), have sometimes glossed over the attendant privacy and security risks. Crafting an identity policy that meets the needs of diverse populations as well as the administrative functions of government is no small task. Identity initiatives are particularly complex when they are predicated on the inherent tension between ready access to data stores and the imperative to safeguard this data from unauthorized access. In light of this tension, identity policies can take significant amounts of time and resources to craft, critique, remediate and deploy.

Identity policies, especially those that incorporate ID cards, pose classic civil liberties and privacy risks. Often called entitlement cards, ID cards can function as 'disenfranchisement cards' for those without them. There are other components of contemporary identity policies that present civil liberties concerns: a common administrative infrastructure designed to retain and access residents' personal information; mandatory registration; compulsion to carry the card and/or identify oneself on demand; and over-use and re-use of personal information and biometrics contained on the card. Audit-logs trigger the fear of surveillance, that our daily lives will be mapped in detail. While this mapping may be to prevent abuse of the system, it could also be used to create profiles that could inform future entitlement decisions.

Card-based identity systems exist primarily at the national level. Countries have taken different approaches to dealing with the negative implications of ID cards, with varying degrees of success in protecting privacy.[2] Regardless of their differences, national ID cards share a common role in constructing identities and can affect the cardholder's life chances. It is on the basis of how identities are constructed, disclosed, and accepted or rejected that most concerns arise: who establishes a person's identity, under what conditions is an identity recorded or used to authenticate a person, and what are the consequences of "failing" to properly authenticate? National ID cards also share common themes or drivers, such as efficiency, security, or modernization (e-government). Vendors are often unsurprising supporters of ID proposals, given that they stand to gain lengthy government contracts related to identity projects. States and vendors, together with standards bodies, are sometimes said to

2 For a discussion of this see Boa, Krista, Clement, Andrew, Davies, Simon & Hosein, Gus. 2007. *CAN ID? Visions for Canada's Identity Policy. Understanding Identity Policy and Policy Alternatives*. Report submitted to the Office of the Privacy Commissioner of Canada, www.priv.gc.ca/resource/cp/2006-2007/p_200607_10_e.asp.

compose a "card cartel".[3] Problematically for democracy, this cartel—not the citizen or resident—establishes the terms of what constitutes an identity, an identity proof, and the administrative and technical processes that underlie card-based identity systems.

Opposition to ID cards and their technical infrastructure typically emerges on both practical and principled levels. On a practical level, security, cost, efficiency, and effectiveness inform arguments against a card-based identity system, on the basis that the stated benefits of these cards are actually misleading. Function creep is also invoked insofar as the card system may facilitate broader sharing of people's information over time. Critiques based on principle draw upon a civil liberties frame, highlighting how card-based identity systems facilitate increased state surveillance or offend constitutional or moral dignities. Recent examples from the US (*REAL ID Act*)[4] and Britain (*Identity Cards Act*)[5] illustrate how critics can successfully oppose ID cards even after legislation is passed. However, civil society advocacy alone appears to be insufficient: successful oppositions have drawn in other political partners. Some ID cards, such as the European Health Insurance Card, meet little resistance *if and only if* they are introduced as being relatively non-invasive, minimally involved in data collection, and have a low barrier of entry. Together these features limit civil liberties concerns, though such cards can still serve as a potential foundation for later, more invasive identity schemes.

Canadians have little experience with identity cards compared to some European countries, and other less democratic nations around the world. According to Jennifer Stoddart, Privacy Commissioner of Canada, "Canadians place a high value on their personal information and don't want it broadcast, bartered, and bandied about without their knowledge and consent".[6] In 2002, Minister for Citizenship and Immigration Denis Coderre proposed a national ID card. The idea was in part a response to "new national security requirements" that emerged after the September 11 terrorist attacks,[7] including the United States' demand for "secure" travel documents. Coderre struck a standing committee to investigate the matter. The committee's report found that "a national ID card was a challenging policy issue with the

3 Lyon, David. 2009. *Identifying Citizens: ID Cards as Surveillance*, Cambridge: Polity Press. See also McPhail, Brenda, Parsons, Christopher, Ferenbok, Joseph, Smith, Karen and Clement, Andrew. (Forthcoming). Identifying Canadians at the Border: ePassports and the 9/11 legacy. *Canadian Journal of Law and Society*.

4 Bohm, Allie. 2012. Yes, the States Reject Real ID. *American Civil Liberties Union Blog*, www.aclu.org/blog/technology-and-liberty/yes-states-really-reject-real-id.

5 Travis, Alan. 2010. ID Cards Scheme to be Scrapped within 100 Days. *The Guardian*, www.guardian.co.uk/politics/2010/may/27/theresa-may-scrapping-id-cards.

6 Stoddart, Jennifer. 2012. *Privacy and Communications in Changing Times: Remarks at IABC 2012 Canada Business Communicators Summit*. Ottawa, ON: Office of the Privacy Commissioner of Canada, www.priv.gc.ca/media/sp-d/2012/sp-d_20121102_e.asp.

7 Marleau, Robert. 2003. *Why We Should Resist A National ID Card for Canada: Submission of the Office of the Privacy Commissioner of Canada to the Standing Committee on Citizenship and Immigration*. Ottawa, ON: Office of the Privacy Commissioner of Canada, www.priv.gc.ca/media/nr-c/2003/submission_nid_030918_e.pdf.

potential of serious ramifications" requiring broad public review and debate.[8] Overall, the report did not support a national ID card, and the idea was dropped. It made a brief reappearance in 2006, when Public Safety Minister Stockwell Day made public statements that a national ID card was "inevitable". The last public mention of a national ID card was in 2007, when a poll indicated that 72 percent of Canadians agreed with "implementing a national identification card for all Canadians".[9] Since then, lack of further interest coupled with complex policy challenges have prevented the federal government from seriously contemplating a national ID card.

Canada's privacy commissioners and advocates, as well as academics, have voiced their strong opposition to a national ID card and the identity system that would necessarily accompany it. Former Privacy Commissioner of Canada Robert Marleau noted "substantial" privacy risks associated with a national ID card—especially a mandatory, multi-use card".[10] British Columbia's former Information and Privacy Commissioner David Loukidelis underscored the real possibility of function creep, with personal information collected for one purpose migrating to other uses "that extend and intensify surveillance and invasions of privacy beyond what was originally understood and considered socially, ethically and legally acceptable".[11] A report from the Public Interest Advocacy Centre affirmed that although national ID cards are promoted as a means to bolster national security and combat identity theft, they remain an "ineffective solution" to both problems.[12] The BC Civil Liberties Association called a national ID card program "nothing but fool's gold" that could introduce more problems than it solves, including building a technical infrastructure that makes data mining and profiling "irresistible" and thereby create "tremendous incentives" to use the card in both the public and private sector.[13] Critics further noted the technical immaturity and unreliability of biometrics, which are typically included in ID cards, as well as the threat they pose to democracy: "'Proof of status' surveillance technologies such as biometric national ID

8 Boa et al, 2007, p. 89.

9 Clement, Andrew, Boa, Krista, Davies, Simon and Hosein, Gus. 2008. Towards a National ID Card for Canada? External Drivers and Internal Complexities. In Colin J. Bennett and David Lyon (eds.) *Playing the Identity Card: Surveillance, Security and Identity in Global Perspective*. New York: Routledge, p. 235.

10 Marleau, Robert, 2003.

11 Loukidelis, David. 2002. *Submission on a National Identity Card. Victoria, BC: Office of the Information and Privacy Commissioner for British Columbia*, www.oipc.bc.ca.

12 Palihapitya, Hasini. 2006. *National Identity Cards, Biometrics and the Consumer: Displacing the Personal from the Person*. Ottawa, ON: Public Interest Advocacy Centre, www.piac.ca/privacy/piac_report_national_identity_cards_biometrics_and_the_consumer_displacing_ the_personal_from_the_person.

13 British Columbia Civil Liberties Association. 2003. *A National ID Card for All Canadians? Fools' Gold or the Mother Lode of All Databases?* http://bccla.org/our_work/a-national-id-card-for-all-canadians-fools-gold-or-the-mother-lode-of-all-databases-2.

cards threaten the very core of the citizenship provisions that are supposed to be sacred in liberal democracies".[14]

While there has been no concerted effort toward a national ID card for Canada, there has been significant work around developing a national identity system that interoperates on a provincial and even municipal level. The vision for this system is guided by the foundational document, *A Pan-Canadian Strategy for Identity Management and Authentication*, published in 2007. Since then, there has been significant development towards a "joined up" model for online government service delivery dependent on integrated identity management and information sharing. Despite this model being at fairly advanced stages of high level planning there has been no public deliberation on the matter to date. It appears that British Columbia may be the first province to link into the national identity framework—also without consulting its residents.

Getting identity policy "right" is clearly among the key challenges facing the promotion, enhancement and protection of privacy in an increasingly digital age. A well designed identity system can limit the collection, aggregation and sharing of personal information across government jurisdictions and with the private sector while still attending to the business of government. British Columbia is at a crossroads with its identity policy: it is still possible to create a system that satisfies the imperatives of government while addressing important civil liberties concerns, and maintaining a healthy relationship between the citizen and the state. Because there is an express intention that the BC system serve as the prototype for a federated pan-Canadian identity system, it is urgent that this matter be brought forward for public deliberation at the federal level, lest the federal policy (essentially) be implemented by stealth. A broad public airing is necessary because it is unclear to citizens and their political representatives that the provincial systems will provide the de facto building blocks of the federal system.

In the next chapter we trace the history of identity policy in British Columbia as it has evolved to accommodate the emerging e-government model. The promotion of data sharing under the guise of "convenience" occurred first with the enhanced driver's licence (EDL)—once thought to be a precursor to a national ID card—but quickly shifted to the province's e-Health mandate. It is within the health sector that BC's identity and information management (IdIM) program took root, with the notion of harmonized access to residents' highly sensitive information driving its development. The BC Services Card is a key component of the province's IdIM plan, expanding the data linking initiatives of the health sector to other government services and jurisdictions. But privacy advocates have warned that insufficient work has been done on the e-Health infrastructure to ensure the protection and integrity of residents' personal information; thus using it as the foundation of the province's wider IdIM plan is ill advised. Given the government's poor track record on safeguarding privacy within

complex IT projects, questions naturally arise about the ability to properly manage the BC Services Card.

14 Walby, Kevin and Hier, Sean. 2005. *Risk Technologies and the Securitization of Post-9/11 Citizenship: The Case of National ID Cards in Canada. Socialist Studies (1)*2, www.socialiststudies.com/index.php/sss/article/viewArticle/44.

3. Identity Policy in British Columbia

For about a decade, British Columbia has been developing its identity policy based on a "Government 2.0" model intended to move government services online to automate them—or in government parlance, expand "opportunities for citizen self-service".[15] Although the growth of e-government has mainly occurred in the health sector, one of the first efforts under the Government 2.0 rubric was the province's enhanced driver's licence (EDL). Although the notion of a national identity card for Canada failed to gather much support, the introduction of the EDL briefly raised the possibility once again. The enhanced licence was a direct response to the Western Hemisphere Travel Initiative (WHTI), a post-9/11 US initiative to securitize its borders. The WHTI requires Canadians present "trusted travel documents" or a "secured" driver's licence equipped with radio frequency identification (RFID) and biometric data when entering the US by land or sea. British Columbia was the first province to comply with the WHTI, and launched its enhanced driver's licence pilot project in 2008, followed by Quebec (March 2009), Ontario (June 2009) and Manitoba (January 2010).

The federal government promoted the EDL as a way to facilitate "convenient" cross-border travel that would "encourage closer social ties with the US" and "support economic growth on both sides of the border".[16] However, civil liberties groups, academics, and Canada's information and privacy commissioners and ombudspersons raised concerns about the enhanced driver's licence[17]—not least that it could provide the foundation for a national identity program. Especially problematic was the fact that foreign legislation drove the EDL instead of an independent initiative of the Canadian government to serve its citizens' needs. As such, the promotion of EDLs appeared "to be a soft-sell, backdoor approach toward national ID schemes that are harmonized across all of North America".[18]

The Canadian government ignored serious concerns around the card's technical insecurity and tracking capability, leading some critics to believe it was designed to serve wider surveillance and information sharing purposes. Despite significant resistance, the US continues to push ahead with its controversial *REAL ID Act*, which requires all states to develop interoperable licencing documents and linked databases containing the personal information of licence holders. Privacy watchdogs and critics, including Canada's Privacy

15 BC Public Service, nd, p. 13.

16 Public Safety Canada. 2008. *Canada's First Enhanced Driver's Licence Launches in BC.* Ottawa, ON: Government of Canada, www.publicsafety.gc.ca/media/nr/2008/nr20080121-eng.aspx.

17 Office of the Privacy Commissioner of Canada. 2008. *Enhanced Driver's Licences Concern Canada's Privacy Guardians*, www.priv.gc.ca/media/nr-c/2008/nr-c_080205_e.asp.

18 Clement, Andrew and Bennett, Colin. 2008. Enhanced Driver's Licence or National Identity Card? *The Toronto Star*, www.thestar.com/opinion/2008/11/17/enhanced_drivers_licence_or_national_identity_card.html.

Commissioner, have called the REAL ID card "a type of national identity card", suggesting that in Canada, the EDL might have been intended to align with American identity policy.[19] In the context of bilateral discussions regarding a "one-card" solution to travel security that took place in the mid 2000s, the EDL appeared more broadly as a North American identity card.[20]

The Evolution of "Government 2.0"

Despite vigorous promotion, the uptake of enhanced driver's licences across Canada has been limited, substantially allaying concerns that the EDL could become a de facto national ID card. As national security faded as a rationale for a pan-Canadian identity policy, it was replaced by e-government, with its focus on online service delivery, as the main driver of identity policy in Canada. Over the last decade, British Columbia has been developing its e-government strategy—dubbed "Government 2.0"–in keeping with the federal vision outlined in a 2007 policy document titled *The Pan-Canadian Strategy for Identity and Management and Authentication*.

Government 2.0 seeks to "transform" the province's approach to technology and the management of identity and information, largely corresponding with the pan-Canadian identity framework. Indeed, BC's Office of the Chief Information Officer (OCIO) has participated in high level federal discussions concerning national identity management, authentication and assurance strategy. Housed in the Ministry of Citizen Services and Open Government, the OCIO oversees the province's identity and information initiatives and is the lead government agency responsible for the BC Services Card. The OCIO has been a key provincial partner in shaping the vision of a national identity system and has contributed to important policy documents, including the *Pan-Canadian Strategy for IdM&A* and the *Pan-Canadian Assurance Model*. From the outset, it appears as if BC has aligned its Government 2.0 plans with a broader national vision of an integrated model for online service delivery based on unprecedented data linking and sharing.

BC's e-Health Initiative

BC's e-government strategy is comprehensive, incorporating a number of departments and services. Much of the initial focus, however, has been in the health sector. In 2008, the provincial government passed the *e-Health (Personal Health Information Access and*

19 *The Vancouver Province*. 2008. Watchdogs are Wary of New Licences, www.canada.com/theprovince/news/story.html?id=81fe8029-20d4-419d-b800-1d7900adfd14&k=77025.

20 Legislative Assembly of Ontario. 2008. *Committee Transcripts: Standing Committee on General Government - October 20, 2008 - Bill 85, Photo Card Act, 200*, www.ontla.on.ca/web/committee-proceedings/committee_transcripts_details.do?locale=en&Date=2008-10-20&ParlCommID=8856&BillID=2026&Business=&DocumentID=23343.

Protection of Privacy) Act, which created the legal foundation for the online delivery of health services. The objective for e-Health is an integrated, province-wide computer network that provides easier access to patient data by a wide range of health system participants, including caregivers, managers and bureaucrats.[21] BC's e-Health initiative is partially funded by Canada Health Infoway, a federally supported non-profit corporation that has promoted the centralization of electronic health records (EHR) for all Canadians since 2001.

Canada Health Infoway and BC's Ministry of Health share responsibility for implementing EHR systems: Infoway promotes the development and uptake of interoperable systems across Canada while BC works to create a provincial EHR system compatible with the national standards.[22] An EHR is meant to be a secure and private record of an individual's health history and care that is amassed over a person's lifetime. Purported benefits of digitally stored and linked health information include reduced costs and increased efficiencies in health care delivery. Infoway's Electronic Health Record Solution (EHRS) envisions a healthcare system supported by an "infostructure"—an interoperable technical architecture that provides "a shared foundation of hardware, software and communication technologies" to facilitate the "uninterrupted flow of information".[23]

Experts critical of the "shared record" model promoted by Infoway describe it as an "over-centralized approach based on a top-down vision of a 'federated set' of 'health information data warehouses' with highly centralized access to shared records".[24] They point out that this model has already been discredited and discarded in the United Kingdom due to information insecurity and privacy problems. Indeed, there appears to be little evidence to support Infoway's claim that "linked up" electronic health records are the "saviour of Canadian health care", improving efficiency, patient safety and longterm sustainability.[25] To the contrary, there is "rapidly growing evidence that these immensely expensive systems fail to deliver promised benefits and facilitate violations of medical confidentiality on a scale never before seen".[26]

---

21 British Columbia Freedom of Information and Privacy Association. 2009. e-*Health in BC*, http://fipa.bc.ca/help/Civil-Liberties/e-Health-in-BC.php.

22 Doyle, John. 2010. *Electronic Health Record Implementation in British Columbia*. Victoria, BC: Office of the Auditor General, www.bcauditor.com/pubs/2010/report9/electronic-health-record-implementation-british-columbia.

23 Canada Health Infoway. 2006. *EHRS Blueprint: An Interoperable EHR framework. Executive Overview*, p. 7, https://www2.infoway-inforoute.ca/Documents/EHRS-Blueprint-v2-Exec-Overview.pdf.

24 Webster, Paul Christopher and Kondro, Wayne. 2011. Medical Data Debates: Big is Better? Small is Beautiful? *Canadian Medical Association Journal*, www.cmaj.ca/content/early/2011/02/22/cmaj.109-799.full.pdf+html?maxtoshow=&hits=10&RESULTFORMAT=&fulltext=webster&searchid=1&FIRSTINDEX=0&sortspec=date&resourcetype=HWCIT.

25 Vonn, Michael. 2009. The Real Impact of e-Health. *The Advocate*. Vol 67, part 6, p. 753.

26 Vonn, 2009, p.753.

Information Sharing and the e-Health Act

The *e-Health Act* authorizes the creation of linked databases called Health Information Banks (HIBs). HIBs collect personally identifiable patient information from both private and public sector sources. Privacy advocates have flagged the threat to patient confidentiality posed by an integrated network of health databases; the information stored in HIBs may eventually be "used for purposes in addition to the provision of health care to the patient".[27] The *e-Health Act* represents a significant change in how personal health information is handled in British Columbia. While doctors, nurses and others within a patient's "circle of care" are sworn to protect the confidentiality of personal health care information, government authorities have no such obligation.

When private sector information is transferred into HIBs, it is no longer governed by the *Personal Information Protection Act* (PIPA), which requires express consent for the disclosure of personal information outside the circle of care. Once information is in government custody, it is subject to the *Freedom of Information and Protection of Privacy Act* (*FOIPPA*). *FOIPPA* does not require patient consent for use or disclosure of personal health information. Furthermore, FOIPPA allows for the wide sharing of data throughout government. Privacy advocates describe this as "a critical violation of patients' right to control their health information and a loss of control by health care professionals, who are legally and ethically obliged to safeguard patient confidentiality".[28] The *e-Health Act* designated eight HIBs, but so far only the Provincial Laboratory Information Solution (PLIS) containing diagnostic laboratory test results is operational.

In his audit of electronic health record implementation, BC Auditor General John Doyle flagged the lack of clarity regarding privacy and security measures.[29] The Canadian Medical Association is very clear regarding the privacy weakness inherent in EHRs. The Association's policy, documented in *Principles for the Protection of Patients' Personal Health Information*, advises that "patients should be informed that the treating physician cannot control access and guarantee confidentiality for an electronic health record system".[30] Counsel for Canada's Privacy Commissioner observed that e-Health's "privacy challenges, though not necessarily insurmountable, have yet to be fully and broadly understood and coordinated across jurisdictional boundaries".[31] Advocacy groups have noted that despite government assurances

27 BCFIPA, 2009.

28 Vonn, 2009, p. 754.

29 Doyle, 2010, p. 22.

30 Canadian Medical Association. 2011. *Principles for the Protection of Patient.* www.policybase.cma.ca/dbtw-wpd/Policypdf/PD11-03.pdf.

31 Kosseim, Patricia. 2005. *The Advent of Electronic Health Records (EHRs) in the Current Legal and Policy Context*. Ottawa, ON: Office of the Privacy Commissioner of Canada, www.priv.gc.ca/media/sp-d/2005/sp-d_051130_pk_e.asp.

of protecting patient privacy "it appears that the systems are being built *before* the privacy rules have been properly defined".[32] All of Canada's privacy commissioners have called for standards that allow patients to "set rules for who should or should not be allowed to see their own personal health information, express their wishes for how their health information is used by health researchers and others, receive privacy and security breach notification alerts [and] see who has accessed their records".[33] Thus far, these citizen-centric standards do not appear to have been incorporated into BC's e-Health plans.

In addition to e-Health's "devastating impact on health privacy", critics point to the inherent insecurity of such data linking schemes: "The centralization of electronic health records jeopardizes the security of data in ways that cannot be mitigated. A linked database system of this kind cannot be made secure".[34] Indeed, an Ontario review of the privacy and security conceptual architecture for Canada Health Infoway's pan-Canadian health "infostructure", which serves as a development and implementation guide for jurisdictions like BC, identified a host of failings. Specifically, the review found that the architecture "oversimplifies many aspects of the identified security services" making implementation appear deceptively simple when in fact "identity management, authentication, authorization, access management and effective audit all pose enormous challenges to large organizations that try to implement them".[35] The review concluded that a national architecture might not be feasible or affordable, and that the technology being considered had not been proven.

Information Access Layer

The health sector is at the heart of Government 2.0 and British Columbia's identity and information management "transformation". The e-Health infrastructure is the largest area of investment for information systems in BC and is being built with the intention of extending it across the public service sector. According to the Office of the Chief Information Officer (OCIO), "the province is using the development of the electronic health infrastructure to establish the technical standards and services for the whole system".[36] The e-Health initiative at once pioneers and anchors the province's massive information integration program called the Information Access Layer (IAL). The IAL is a multi-million dollar project of the OCIO. It embodies an information sharing vision in which "provincial information services that

32 BCFIPA, 2009.

33 Office of the Privacy Commissioner of Canada. 2009. *The Promise of Personal Health Records. Resolution of Canada's Privacy Commissioners and Privacy Enforcement Officials*, www.priv.gc.ca/media/nr-c/2009/res_090910_eh_e.asp.

34 Vonn, 2009, p. 756.

35 Ontario Privacy and Security Architecture Working Group. 2006. *Infoway EHRi Privacy and Security Conceptual Architecture v1.1: Review and Recommendation Report to the Ontario Health Informatics Standards Council*, p. 7.

36 BCFIPA, 2009.

already exist within each ministry of the provincial government are connected...".[37] The "problem" that the IAL seeks to address is that "BC ministries often create information and process silos that limit sharing and reuse".[38] As mentioned, these information silos provide a natural barrier to inappropriate and excessive sharing of personal information. The "problem" being addressed, therefore, is the lack of connection and interoperability among provincial databases; these "inefficiencies" naturally secure the privacy of British Columbians' personal information that is spread across innumerable government databases.

The Information Access Layer acts as a sort of gatekeeper; it sits between provincial information services, which authenticate identity, and the frontline systems, where citizens request online services. In its role, the IAL "provides a critical layer enabling information sharing between online government service providers across the public sector and their private sector partners for a wide variety of provincial information services".[39] The IAL is part of the government's Integration Infrastructure Program (IIP), which is meant to support a province-wide electronic information sharing model. The IAL encompasses the full range of social services in BC with the goal of linking information about BC residents from the Ministries of Children and Family Development, Employment and Income Assistance, Health, Education, and Justice, as well as their private-sector contractors. It supports the OCIO's motto of "Information Sharing for Better Outcomes" by letting staff "better serve citizens by collaborating and securely sharing information while maximizing privacy...".[40] Despite such assurances, there are few details on how privacy is ensured in the Government 2.0 model.

Identity and Information Management

British Columbia's Identity Information Management (IdIM) plan is key to the province's e-government transformation and is part of the larger Information Management/Information Technology (IM/IT) framework. This framework aims to "improve information sharing to better achieve citizen outcomes" across the public sector.[41] The IdIM plan posits a scalable, secure and "privacy-protective" identity service that is geared towards facilitating the

37 Office of the Chief Information Officer. 2009a. *Information Access Layer Architecture Summary*, www.cio.gov.bc.ca/local/cio/standards/documents/architecture/ial_arch_summary.pdf.

38 Office of the Chief Information Officer. 2011. *IM/IT Enablers Strategy for Citizens @ the Centre: BC Government 2.0*, p. 38, www.gov.bc.ca/citz/citizens_engagement/it_strategy.pdf.

39 Office of the Chief Information Officer. 2009b. *IM/IT Strategic Initiatives and Infrastructure: Guidance for Procurement Staff and Solution Developers*, p. 6. www.cio.gov.bc.ca/local/cio/standards/documents/strategic_initiatives.pdf. www.cio.gov.bc.ca/local/cio/about/documents/it_strategy.pdf.

40 Office of the Chief Information Officer. nd. *Identity Information Management*, www.cio.gov.bc.ca/cio/idim/ial_project.page.

41 OCIO. 2009c. *IDIM Business Context and Requirements*. Victoria, BC: Government of British Columbia, www.cio.gov.bc.ca/local/cio/idim/documents/idim_business_context_requirements.pdf.

delivery of government services online. Its objective is to establish trusted identities online by confirming roles, privileges and entitlements for both BC residents and service providers, as well as issuing authentication credentials. According to the Office of the Chief Information Officer (OCIO), the province is on the cutting edge of online government services using "high assurance digital identities". Also called BCeID *Next Generation* (BCeIDng), the initiative is responsible for "the infrastructure and services that enable registration, identification, authentication, federation and access management for employees, contractors, businesses, professionals and citizens accessing electronic public services".[42]

Currently, British Columbians can log in to BCeID.ca to access a variety of government services online, after completing an online and in-person registration process. Available services presently include revenue management (pay government bills online), court services (search and file civil court cases and documents), mineral titles (administration), commerce centre (receive notifications of business opportunities) and transportation (vehicle inspection reports). The intent of BCeID *Next Generation*, which does not appear to be fully deployed, is "to consolidate new concepts, emerging technologies and solutions to create a next generation identity management service".[43] Linking BCeIDng to the Information Access Layer project has let British Columbians access their medical laboratory results housed in the only operational Health Information Bank—PLIS database—via the *My eHealth* portal.

According to the Chief Information Officer's website, the IdIM architecture uses a "claims based" approach, which means that the architecture separates "the presentation of claims from the provability of the link to a real world object".[44] In a claims based identity system, the user makes certain claims to a service provider (relying party) that she is allowed to access its services. She presents an identity token or credential that the relying party accepts or rejects based on the trustworthiness of the credential issuer (authorizing party). A claims based system tends to use a single sign on process. Such a process lets users authenticate to the system once, after which they can access a range of government services. The BC Government promotes a claims based approach as "a privacy-friendly way for citizens to control the use of their identity information in the online world, and do so in a way that is backed by trusted authorities".[45]

The status of the BCeID *Next Generation* project is unclear. Although government planning documents support a user-centric claims based identity information management framework,

42 OCIO, 2009b, p. 3.

43 OCIO. nd.

44 Cameron, Kim. 2005. *The Laws of Identity*, http://msdn.microsoft.com/en-us/library/ms996456.aspx.

45 BC Public Service. nd.

these plans have yet to be realized in practice. The BC Services Card, as the most recent major Government 2.0 project, has taken a rather different direction than what is outlined on the Office of the Chief Information Officer's website.[46] It is difficult to compare the card program with the currently functioning identity and information system, however. This difficulty arises because the government has not publicized important documents regarding the BC Services Card's policies and standards for information sharing, nor the privacy mechanisms used to ensure the appropriate, secure sharing of information.

Privacy advocates have already warned that not enough work has been done on the e-Health infrastructure to adequately protect personal information or give people sufficient control over their highly sensitive health information. "In light of the BC government's intention to use the e-Health infrastructure for its broader social services integration, many question the effectiveness of the privacy safeguards which are now, or will be, in place".[47] While a claims based approach can afford the user some control of how her information is used when accessing services online, it does not govern how or what personal information is collected, stored or shared across government, which is at the core of concerns with the BC Services Card and IdIM plans more generally.

Over the last decade, identity policy in British Columbia has evolved to propel a technology "transformation" based on increased data linking and sharing. As we have seen, the birth of the e-government model was in the health sector where the e-Health initiative served as a foundation for the expansion of Government 2.0 across the province. In the following section, we describe the government's poor track record on implementing major information technology projects that are part of the Government 2.0 vision.

Terrible Track Record on Big IT Projects

As the province proceeds with its e-government "transformation" and its flagship project, the BC Services Card, it leaves behind a trail of failed or seriously flawed large information technology (IT) projects. In 2011, BC's Auditor General found that despite advising the government "of control issues with IT year after year, IT deficiencies accounted for 30 percent of the audit issues" reported by government ministries and organizations.[48] As the province rolls out its new identity card initiative, supported by an unproven data linking architecture, it is instructive to look at the government's track record on major IT projects.

---

46 *An Introduction to Identity and Information Management*, www.cio.gov.bc.ca/local/cio/idim/IDIM_Module/BC_IM.htm.

47 Levine, Sara A. nd. *Privacy Handbook*, http://bccla.org/privacy-handbook/main-menu/privacy6contents/privacy6-12.

48 Doyle, John. 2012. *The Status of IT Controls in British Columbia's Public Sector: An Analysis of Audit Findings. Report #3.* Victoria, BC: Office of the Auditor General of British Columbia, www.bcauditor.com/pubs/2012/report3/status-it-controls-british-columbias-public-sector-analys.

The province's electronic student information system, BCeSIS, is slated for replacement after the government spent almost $100 million on it.[49] Designed for teachers and administrators, the system tracked students' information, such as grades and attendance. Early reports from system users criticized it as unreliable and difficult to use. A consultant concluded in 2011 that the system was "not meeting the business, technical or operational needs of BC and is not a viable future alternative".[50] Critics were unsatisfied with the database's poor performance as well as its design as a top-down system of control "aimed at system-wide information for administrative decisions and purposes and only secondarily—at best— providing information for educational development of the individual student".[51] The government agreed to replace the system, though acknowledged this was not likely to happen before 2014.

In 2013, the Auditor General highlighted "serious security flaws" in JUSTIN, the Ministry of Justice's integrated electronic system for managing and administering the criminal justice process.[52] His audit found that the system, which contains extremely sensitive personal information, was not properly protected from internal or external threats. Excessive user access, lack of audit trails, and the inability to detect unauthorized access compounded these threats. The JUSTIN report followed a 2008 audit of CORNET, the BC Corrections case management system, which also identified security weaknesses regarding internal access to sensitive information. According to Auditor General Doyle, the government should have applied the recommendations from the CORNET audit to its other IT systems: "This failure to act, and the very fact that significant security weaknesses were allowed to exist at all, leads us to question the quality of IT leadership and governance around criminal justice information".[53]

The $182 million Integrated Case Management (ICM) system is another technology project beset by apparent mismanagement, technical malfunction and high profile criticism. Based on expansive information sharing, ICM is part of the larger Social Service Sector Integrated Information Management Project led by the Office of the Chief Information Officer. ICM is the first component of this broader project to be implemented and as such, serves as the

---

49 Hoekstra, Gordon. 2011. BC Schools to Scrap $89m Records Software. *The Vancouver Sun*, www.globaltvbc.com/bc+schools+to +scrap+89m+records+software/6442484776/story.html.

50 Gartner Inc. 2011. *A Report for BC Ministry of Education: Review of Student Information System*, www.vancouversun.com/pdf/ bc_education_final_report.pdf.

51 Kuehn, Larry. 2012. *BCeSIS—Going, But Still Not Gone: A 2012 Update.* BC Teachers' Federation. www.bctf.ca/AboutUs/ EmploymentOpportunities.aspx.

52 Doyle, John. 2013. *Securing the Justice System: Access and Security Audit at the Ministry of Justice*. Victoria, BC: Office of the Auditor General of British Columbia, www.bcauditor.com/pubs/2013/report9/securing-justin-system-access-and-security-audit-ministry.

53 Office of the Auditor General of British Columbia. 2013. *News Release: Auditor General outlines serious flaws with B.C.'s criminal justice security system*, www.bcauditor.com/pubs/2013/report9/securing-justin-system-access-and-security-audit-ministry.

foundation for future information sharing across the social services sector. The objective of ICM is to "enable the connecting of clients, services, contracts and outcomes"[54] in the delivery of social programs like the BC Employment and Assistance Program and the Child Care Subsidy Program.[55]

ICM has raised red flags with privacy advocates from its inception.[56] This is because the system collects and shares across government "comprehensive personal data from hundreds of independent community service organizations, which are contracted to provide government services, in order to create a database of unprecedented scope and detail about citizens' lives, including their participation in health care, education, family services and other government services".[57] In addition to an architecture that connects, shares and discloses the personal information of British Columbians who are clients of independent community service agencies, ICM lets government officials reveal that information to a wide range of parties without the consent of the clients or the agencies. "The ramifications for such an unprecedented proliferation of data disclosures between the government and the private sector are vast and deeply troubling".[58] Former BC Information and Privacy Commissioner David Loukidelis recommended that the government "should not proceed with any more data sharing initiatives until a meaningful public consultation process has occurred, and the outcome of that process is an enforceable code of practice for data sharing programs".[59] Calls for government transparency and public debate in advance of the system's launch went unheeded, however.

ICM's Phase 2 implementation moved forward without public consultation in April 2012. By July of that year, BC's Representative for Children and Youth Mary Ellen Turpel-Lafond issued a scathing critique of the system, questioning its effectiveness, security and reliability and stating that the volume of technical problems left real doubt as to whether "child safety can be assured through the use of ICM".[60] Serious system flaws caused a number of civil society organizations to call for a public inquiry. The Ministry of Child and Family

54 Ministry of Children and Family Development. nd. *Information Resource Management Plan*, www.mcf.gov.bc.ca/about_us/irmp.htm.

55 Levine, nd. *Privacy Handbook*, http://bccla.org/privacy-handbook/main-menu/privacy6contents/privacy6-1-3.

56 British Columbia Freedom of Information and Privacy Association. 2010a. *Culture of Care or Culture of Surveillance?* http://fipa.bc.ca/library/Reports_and_Submissions/Culture_of_Care_or_Culture_of_Surveillance_March_2010.pdf.

57 British Columbia Freedom of Information and Privacy Association. 2010b. *Privacy Research: Personal Privacy and the BC Government's Integrated Case Management System*, https://privacyresearch.wordpress.com.

58 BCFIPA, 2010a.

59 Office of the Information and Privacy Commissioner for British Columbia. 2010. *Submission of the Information and Privacy Commissioner to the Special Committee to Review the Freedom of Information and Protection of Privacy Act*, www.leg.bc.ca/foi/.../Information_ and_Privacy_Commissioner.pdf.

60 Turpel-Lafond, Mary Ellen. 2012. *Statement. July 12, 2012*. Victoria, BC: Office of the BC Representative for Children and Youth, www.rcybc.ca/Images/PDFs/Statements/ICM%20Statement%20July%202012%20FINAL.pdf.

Development hired a consultant to investigate the problem-plagued system while taking remedial steps "to stabilize the solution and allow time for more robust review of suitability".[61] The consultant's report, issued in November 2012, found fault in a wide range of areas, from procurement, governance and training to technical design and implementation. It said that ministry officials failed to adequately monitor the development of the ICM and to ensure the system was designed to properly support child-care work. Turpel-Lafond said the report confirmed her earlier warning, calling the findings "brutal" and the ICM "a colossal failure".[62]

From this brief overview, we can see how identity policy in BC evolved to accommodate an e-government agenda, beginning with the e-Health mandate. The government's troubled track record on complex IT projects founded on data collection and sharing casts serious doubt on the ability to successfully deploy the BC Services Card. In Chapter 4, we examine how British Columbia is transforming its approach to identity and information management, focusing on the factors that motivate as well as inhibit the development of an IdIM "solution", of which the Services Card is an integral part.

61 Queenswood Consulting Group Ltd. 2012. *MCFD-Integrated Case Management System: Interim Assessment Report*, www.integratedcase management.gov.bc.ca/documents/icm-mcfd-iar.pdf.

62 Kines, Lindsay. 2013. Watchdog Says Computer System for Social Workers a "Colossal Failure." *The Victoria Times-Colonist*, www.timescolonist.com/news/local/children-s-watchdog-says-computer-system-for-social-workers-a-colossal-failure-1.56291.

4. Transforming Identity and Information Management in BC

The BC Services Card Business Transformation Project is responsible for implementing the province's new multi-purpose identity card. The project promotes the BC Services Card as a "solution to support the enhancement of identity and authentication of eligible health beneficiaries across the health services sector".[63] It is a large, complex initiative that includes the Ministry of Health, Ministry of Finance, Public Safety and Solicitor General, Citizens Services and Open Government, Health Authorities, health care providers and private facilities providers. It is expected "to continue to evolve and expand to include other ministries and agencies where appropriate".[64] Considered a "high priority", the Project is overseen by a board of 12 Deputy Ministers and Assistant Deputy Ministers, referred to as the Committee on Transformation. According to Kim Henderson, Deputy Minister of Citizens' Services, the committee "provides the governance on how we're able to drive BC agendas like open government and the BC Services Card. These 12 high profile deputies have helped drive the strategy and enable us as the central agency to get cross-government buy-in on lots of our programs".[65]

In early 2010 a governmental working group began evaluating the merits of a photo health card for government services. Dubbed the "CareCard Initiative", the group involved the Ministry of Health (MoH), Ministry of Citizen Services, and the Insurance Corporation of British Columbia (ICBC), as well as private sector corporations, including IBM, VISA and SecureKey Technologies. Together they established a foundation for e-government—the province's move toward electronic service delivery based on integrated identity and information management. Plans for the new card originated from MoH. ICBC was quickly enrolled as a partner because of its existing facial recognition database as well as card production and identity proofing capacity. ICBC's identity proofing process, which includes the ability to detect and manage the investigation of potentially fraudulent identity information, was considered helpful: "The BC Services Card project will extend these processes to support those who identity proof for BC Services Cards and extend established fraud reporting processes between ICBC and the Ministry of Health".[66]

63 Ministry of Health. nd. *Position Description: Director, Business Transformation and Policy.*

64 Ibid.

65 Fyfe Toby. 2012. Open Government: Turning Past Practice on its Head. *Canadian Government Executive*, www.canadiangovernmentexecutive.ca/article/?nav_id=1044.

66 BC Ministry of Health FOI Request HTH-2012-00156.

ICBC is responsible for the practical implementation of the BC Services Card program, including issuing the stand-alone health card and the hybrid driver's licence/health card. The Corporation is also responsible for verifying client information by searching its database for existing client records and performing biometric comparisons of renewals or new applications against existing images. "Fraud detection functions are integrated with the counter service, identity proofing, and card production processes".[67] ICBC then passes the required data on to the government's Identity Information Service (IIS). For people applying for a health card only, ICBC captures the data required, including a digital photograph that is used to develop the "biometric templates" needed for subsequent facial recognition analysis, and sends them to IIS. ICBC does not collect fees for the health card, and information collected for health card purposes is not stored by ICBC, nor is it used as ICBC client data. Although ICBC handles the daily operation of the BC Services Card program, the Office of the Chief Information Officer designed and operates the technical architecture through which all personal information accessed by the card flows.

In May 2011, MoH publicly announced the BC Services Card as a replacement to the "outdated" health CareCard. The government promised a more secure "smart" card designed to enable the future onboarding of other government services, including, potentially, electronic voting.[68] A five-year phase-in of the BC Services Card was set to begin on November 30, 2012, but the launch was delayed until February 15, 2013.[69] BC residents have the option of combining their driver's licence (or BC ID card for non-drivers) with the new health card, an offer they will receive upon renewing their licence. While the hybrid driver's licence/health card is optional at present, after the initial five-year phase-in, the stand-alone BC Services Card will be mandatory for all residents enrolled in the Medical Services Plan. The government projects that most eligible citizens will have the hybrid driver's licence/health card by 2018.

Drivers and Inhibitors

There are common drivers and inhibitors associated with identity systems and ID cards, and the BC Services Card shares many of them. The BC Government has identified a range of drivers—all intended benefits to be derived from the card, including reduced identity theft and medical fraud, cost savings, enhanced security, streamlined service delivery, and

67 ICBC FOI Request F197019.

68 Shaw, Rob. 2012. Internet Voting Gets Close Look in BC. *The Victoria Times Colonist*, www.timescolonist.com/news/internet-voting-gets-close-look-in-b-c-1.13184.

69 MoH blamed a labour dispute at ICBC in which employees threatened to derail the plan to transfer the BC Services Card program from Health Insurance BC. Hager, Mike. 2012. ICBC Employees Aim to Stall Transfer of Care Card Program. *The Vancouver Sun*, www.vancouversun.com/business/ICBC+employees+stall+transfer+Care+Card+program/6920069/story.html.

improved patient safety. Most inhibitors to data linking identity management programs are related to privacy—notably restrictions imposed by privacy legislation and opposition from privacy professionals and advocates. In what follows we discuss the drivers and inhibitors that have played a role in the development of the BC Services Card program.

Identity Theft and Health Care Fraud

The Ministry of Health initially presented the BC Services Card as a technological fix for the perceived problems of identity theft and medical fraud. The government highlighted the card's increased security benefits, including biometric photograph, anti-forgery features and computer chip, although to date few details have been provided. The government has also failed to provide empirically valid statistics concerning medical-related identity theft in the province, thus preventing an analysis of the evidence-based need to address this "problem". Nevertheless, BC Solicitor General Shirley Bond offered vague assurances that the "new more secure card will make it tougher for people to steal your identity".[70] The Ministry of Health also promised the new card would reduce fraud, claiming that there are "about 9.1 million BC CareCards in circulation for a population of about 4.5 million people".[71] A closer inspection of the numbers found in documents received through a freedom of information request revealed that the majority of "extra" cards were legitimately issued as replacements, updates or new enrolments. Although fraud was one of the original rationales for the BC Services Card, it was a confusing and potentially misleading one, as this statement from MoH confirms:

> We have never said there are 4.6 million fraudulent cards in circulation. We have said that there are slightly more than 4.6 million more cards than persons covered under MSP. We fully expect some have been properly destroyed by their owners when they received a replacement card, or when their account became inactive (upon leaving the province for example). We fully expect some are kept at a person's residence.[72]

The government further admitted that it did not know how many CareCards were misused or used fraudulently because it had no mechanism to track this. In the absence of a "credit and debit" style ledger, there is no indication of how many active cards are in circulation, or how many *should* be in circulation.[73]

---

70 Zielinski, Jennifer. 2011. *New Care Card for BC*. Castanet, www.castanet.net/news/BC/62148/New-care-card-for-B-C.

71 Ministry of Health. 2011. *BC Paves Way for New Card to Replace CareCard*, www.newsroom.gov.bc.ca/2011/05/bc-paves-way-for-new-card-to-replace-carecard.html.

72 Ibid.

73 Parsons, Christopher. 2013. Checking the Numbers behind BC CareCard Fraud. *Technology, Thoughts, and Trinkets*, www.christopher-parsons.com/blog/checking-the-numbers-behind-bc-care-card-fraud.

Ontario's health ministry conducted a data security audit when it tried to learn the extent of card-related medical fraud in that province. The audit led to the cancellation of invalid cards. It also led to the introduction of new security measures, including legislation that required health care providers to report suspected fraud and retain invalid cards, as well as the establishment of a special police unit to investigate health fraud. As a result, the number of extra cards in circulation in Ontario dropped. But, as its Health Fraud Investigation Unit acknowledges, the majority of medical fraud involves "fraudulent billings by physicians, pharmacists and vendors of medical equipment" and not individuals misusing health cards.[74] Independent research that evaluated the BC situation made a number of recommendations that the province should implement *before* introducing a new health card, including an audit similar to Ontario's to ascertain the real extent of health care card fraud.[75]

Although the scope of health care card fraud in British Columbia is unknown, MoH suggests it causes the province to lose about $260 million a year. This number comes from vague estimates from the Canadian Anti-Health Care Fraud Association, which in turn gets its numbers from American think tanks focused on fraud in the US health care system. The kinds of medical fraud referred to include a broad range of unlawful activities—again largely originating from health care and service delivery providers rather than individuals. When asked to quantify losses due to health care fraud, Health Minister Margaret MacDiarmid answered: "We don't know the extent of it".[76] She went on to list the different ways the government *believes* the old health card was being abused. If hundreds of millions of dollars have been lost to fraud in BC's health care system annually, it is inexplicable that the government has neither initiated an audit function nor followed the best practices established by Ontario. Regardless, the BC Services Card is not designed to address the wide range of fraudulent activities that occur under the broad umbrella of medical fraud and thus cannot assist in reducing all of them. Although the evidence points to systematic mismanagement of card issuance—a problem solvable by other means than a wholesale change in the way the province handles personal identity information—the government continues to promote the new card as a key solution to the "fraud problem".

Cost/Savings

The BC Government has not provided a clear explanation of the potential savings associated with the BC Services Card, nor of other costs it will likely incur. Rather, the province has

74 Dumfries, John. 2012. *Health Care Fraud and Medical Identity Theft in Canada and USA.* Presentation to Internal Auditors Association of Canada, October 9, 2012, www.wsuccess.com/iia/healthcare_fraud_bw.pdf.

75 Ibid.

76 On the Coast. 2011. *Goodbye Care Card, Hello BC Services Card.* CBC Radio, www.cbc.ca/onthecoast/episodes/2013/01/07/goodbye-care-card-hello-bc-services-card.

simply stated that the card will cost $150 million over five years, without indicating whether that figure comprises some—or all—of the cost of hardware (e.g. card readers), software, private vendor contracts (e.g. SecureKey, IBM), staff training, and public education. It is also unclear whether this amount includes the cost of setting up or running the business processes linked to the card. Prior to March 2013, and a response from the Ministry of Citizen Services to a freedom of information request, there was no publicly available information on the cost of issuing 4.5 million new cards over the next five years. There are no guarantees that the technical architecture—largely untested before card launch—will operate smoothly and will not require remediation, as happened with the Integrated Case Management System (ICM), or a complete overhaul, as with the electronic student information system (BCeSIS). In aggregate, then, the public has no demonstrable evidence that the program will "only" cost $150 million. It has no idea of what additional costs might be projected. And it has no guarantees that the BC Services Card and associated infrastructure will not suffer the same technical and bureaucratic mismanagement linked with earlier large-scale provincial information technology projects.[77]

Security

The government has also promoted improved security as an important new feature of the BC Services Card, and the key to reducing identity theft and medical fraud while accruing savings. The old CareCard had been unchanged since its debut in 1989. Its security features included the cardholder's name, signature and Personal Health Number (PHN), as well as a magnetic stripe containing that same information in machine-readable format. Although there was password functionality, very few health care providers were aware of it and it was not in widespread use.[78] The BC Services Card is more secure insofar as its anti-fraud and anti-forgery features will help reduce the issuance of multiple unique cards to the same person. This will not stop fake issuance entirely nor prevent medical fraud, which, in the Canadian context, does not seem to be largely driven by patients so much as by health service providers.

While security associated with the BC Services Card is meant to reduce fraud, neither the card nor its associated technical infrastructure appear to have received robust technical analysis by government or external experts. Consequently, claims that the Services Card

77 It is important to note that one of the main reasons for the eventual rejection of Britain's national ID card in 2011 was ballooning costs. The British government's initial estimates of the cost of the massive identity scheme were vague and eventually revealed to cover only a portion of the overall cost. In abolishing the ID card five years after its introduction, the key benefit for Britons (in addition to reversing the "erosion of civil liberties") was cost savings. The British Prime Minister's Office. 2011. *Queen's Speech – Identity Documents Bill*, www.number10.gov.uk/news/queens-speech-identity-documents-bill.

78 Lazaruk, Susan. Thief Uses Stolen CareCard. *The Province*, www.canada.com/health/Thief+uses+stolen+CareCard/7794706/story.html.

enhances security are questionable; such questions are compounded insofar as it's unclear what degree of security testing the province's IdIM "solution" has received. Without conducting in-depth, externally-driven and publicly released security audits, assurances that the card is secure must be regarded with caution.

Better Service Delivery/Improved Patient Safety

The prospect of improved service delivery and patient safety are drivers that anchor the government's promotional material concerning the BC Services Card. While these are legitimate and laudable goals, they must be accompanied by supporting evidence that indicates how these outcomes will be achieved through the new card. The government has not shown how either service provision or patient safety will be improved, what these deliverables would look like, nor how they were compromised under the CareCard system. It is particularly important for the province to clearly identify how the cards will improve service in light of how past IT projects have borne out. As just one example, the ICM increased workloads and created new risks for children. The architecture underpinning the BC Services Card is entirely new, virtually untested and exists nowhere else in the country. Consequently, the ability to gauge the benefits of the Services Card is predicated on actuarial assumptions instead of empirically demonstrable proof. Taken together, the lack of support for the claim of improved patient safety, and the province's poor track record on successfully deploying large IT projects do not inspire confidence that the BC Services Card will improve service delivery or health outcomes.

Privacy Professionals

Privacy professionals, civil society privacy advocates and privacy legislation are the usual inhibitors of expansive data and information sharing programs. Privacy and Freedom of Information advisors at ICBC were the first to question the privacy implications—and the legality—of the BC Services Card initiative. They flagged the Ministry of Health's early proposal to use the research provision in the *Freedom of Information and Protection of Privacy Act (FOIPPA)* to gain access to ICBC client information to run a data matching pilot test. Section 35 of *FOIPPA* lets a public body disclose information under its control for a "research purpose".[79] "I'm not sure this is really research in the traditional sense," wrote one manager.[80] ICBC employees had other privacy concerns, including putting a chip on the

79 Government of British Columbia. 2011 *Freedom of Information and Protection of Privacy Act*, www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/96165_00.

80 ICBC's Privacy & FOI Advisor eventually signed off on the agreement, writing in June 2010 that she was "completely satisfied" that the research agreement satisfied *FOIPPA* requirements for disclosing information for research purposes. ICBC FOI Request F197019.

driver's licence "that will store a bunch of information that will be irrelevant to a driver license".[81]

While the chip embedded in the BC Services Card does not store health or driver records, it does contain a personalized ID tag that stores the cardholder's Personal Account Number (PAN). The PAN is used to initiate a host of number linking processes, with the end goal of accessing specific government services (e.g. online health records, tax information). As we explain in Chapter 6, this linking process creates an extensive data trail that could connect the PAN to particular users and the government services they are accessing. Under Canadian privacy law, such unique identifiers are considered personal information: section 3 of the *Privacy Act* defines personal information as information about an identifiable individual that is recorded in any form, including "any identifying number, symbol or other particular assigned to the individual".[82]

ICBC's privacy team was troubled by the privacy implications of visibly locating the personal health number (PHN) on the BC Services Card along with driver's licence information. More generally, they worried about how the partnership with the Ministry of Health would affect the integrity of their clients' data, including personal information and photograph, noting that this data was not collected for the purposes that MoH intended to use it. Under *FOIPPA*, a public body must ensure that personal information under its control is used only for the purpose for which it was collected or a consistent purpose, unless it obtains the consent of the individual for the new use(s).

Another concern was that ICBC had not received a privacy impact assessment (PIA) from MoH. When the Corporation finally received the assessment in April 2011, it was a "conceptual" plan that left many questions. "The document is really an overview of the BC Services Card project since no assessment from a [*FOIPPA]* perspective has been done", wrote one manager. "[A] lot of the items in the PIA are clearly relevant and instead they have chosen to not address them at this time. I had hoped for more of an assessment and a clear indication of all the personal data to be collected and used...".[83] Another wrote: "Mostly I'm shocked at how many things they put N/A about, when I think they're very applicable. The concept of a 'conceptual PIA' seems to be exploited to mean that they don't think they need to provide much detail".[84]

81 ICBC FOI Request F197019.

82 Government of Canada. 1985. *Privacy Act,* http://laws-lois.justice.gc.ca/eng/acts/P-21/page-1.html#h-3.

83 ICBC FOI Request F197019.

84 Ibid.

The BC Information and Privacy Commissioner

BC's Office of the Information and Privacy Commissioner, which provides oversight and enforcement of BC's information access and privacy laws, was regarded as another inhibitor. When ICBC privacy advisors expressed concern about data sharing with the Ministry of Health in 2010, MoH explicitly prohibited ICBC from communicating with the Information and Privacy Commissioner, Elizabeth Denham. More than a year into the planning of the BC Services Card, one ICBC manager observed that the "Privacy Commissioner has not been involved in Government decisions. Unresolved privacy issues could impact the project scope, schedule, and budget".[85] After submitting its conceptual PIA to Denham in early 2011, MoH purported to have had the document "approved"— "approved" even though the Privacy Commissioner does not have a mandate to approve PIAs.[86] Just five weeks before the card's launch, Denham said that her office was "still awaiting information from the relevant ministries and government agencies" in order to finish evaluating the system architecture as it related to security and privacy issues.[87] Denham's review of the BC Services Card, issued one week before launch, only covered Phase I of the project. It affirmed that "the BC Services Card program raises significant concerns regarding misuse of personal data, such as unauthorized access, profiling, and function creep".[88]

Denham further stated she was "deeply concerned" that the government had not consulted the public: "Given the program's profound reach and the amount and type of personal information involved, it is critical that citizens are included in the dialogue". She recommended that the government conduct a "fulsome public consultation" in which it must, at minimum, "explain its long-term vision for the card, the potential benefits to be gained as well as the risks".[89] Denham's statement neatly sums up the lack of transparency and public debate on the BC Services Card since its inception. Because government ministries have not provided relevant documents, a full public accounting of how these institutions perceive privacy and security risks is impossible. Since transparency is essential to holding government to account, it is uncertain how the public can know that the BC Services Card provides suitable privacy and security protections or that the card can or will achieve its stated goals. Addressing the need for transparency, Denham recommended that the "solutions the government proposes to address these risks should be subject to scrutiny by both the

85 ICBC FOI Request F197019.

86 Ibid.

87 Denham, Elizabeth. 2013a. *Statement from BC Information and Privacy Commissioner on the BC Services Card*. Victoria, BC: Office of the Information and Privacy Commissioner for British Columbia, www.oipc.bc.ca.

88 Ibid.

89 Denham, Elizabeth. 2013b. *BC Services Card Phase 1 Review.* Victoria, BC: Office of the Information and Privacy Commissioner for British Columbia, www.oipc.bc.ca.

public at large and by those with technical knowledge in the field".[90] This is directly contrary to the government's position thus far, which has justified keeping information about the technical architecture of the BC Services Card secret so as to protect the infrastructure against system attackers and to protect the proprietary interests of private sector partners.[91]

Legislative Changes

Legislation is a common inhibitor of digital identity management schemes. The need for "legal alignment" is mentioned throughout the *Pan-Canadian Strategy for Identity Management and Authentication*, one of the guiding documents for the data linking architecture underpinning the BC Services Card. The province was keenly aware that the cross-jurisdictional and extra-governmental information sharing required to implement its IdIM "solution" faced legal obstacles. One government document noted that "existing privacy legislation creates some barriers to implementing identity management solutions".[92] Certainly the BC Services Card would not have been possible without several legislative changes, which eliminated these barriers and gave the province new data linking authority. In what follows, we outline the changes to provincial legislation that paved the way for the Services Card and thus enhancing intra- and extra-governmental data sharing and linking.

The first changes authorized information sharing between ICBC and the Medical Services Commission (MSC). ICBC privacy advisors were concerned early on about the legality of sharing their clients' biometric photographs with the Ministry of Health. In May 2011, however, the BC Government introduced *Bill 13, Miscellaneous Statutes Amendment Act (No. 2), 2011*. This omnibus bill amended both the *Medicare Protection Act* and the *Motor Vehicle Act* and thus authorized previously prohibited information sharing where before it had been prohibited. Specifically, *Bill 13* lets ICBC enter an information sharing agreement with the Medical Services Commission for the "purposes of collecting, using and disclosing personal information necessary for the administration" of both acts.[93] Similarly, the Medical Services Commission, after entering an information-sharing agreement, can "collect and use personal information from, and disclose personal information to the party with whom the agreement was made". The amendments let MSC and ICBC exchange client information with one another, including the biometric images ICBC collects and stores for its driver's licence program.

90 Denham, 2013b, p. 5.

91 Author telephone conversation with a representative of the Office of the Chief Information Officer, November 1, 2012.

92 BC Public Service. nd. p. 7.

93 Government of British Columbia. 2011. *Bill 13—2011: Miscellaneous Statutes Amendment Act (no. 2), 2011*, www.leg.bc.ca/39th3rd/3rd_read/gov13-3.htm.

There were other legislative barriers to the BC Services Card and the province's IdIM program more broadly. As one ICBC employee observed, "Citizen Services is looking at changing *FOIPPA* to allow them to implement their identity assurance service".[94] In October of 2011, the government introduced *Bill 3, Freedom of Information and Protection of Privacy Amendments Act*. The stated rationale of the proposed amendments was to "modernize an act that came into force in 1992, when the majority of citizens had not even heard of the Internet".[95] The "sweeping rewrite" was "one of the most significant changes" to *FOIPPA* since its enactment.[96] In brief, the amendments authorized the digitization, aggregation, collation and exchange of personal information across formerly discrete government databases, and enshrined BC's policy direction on province-wide integrated identity management into law.

According to the Ministry of Citizen Services, the *FOIPPA* changes were meant, among other things, to enable the development of a provincial identity and information management system that would provide "secure online government identification", allow information sharing across government "in specific circumstances where programs touch multiple ministries", and facilitate "data linking".[97] Data linking refers to the combining of personal information in one database with that in other databases if the purpose of the combination is different from "the purpose for which the information in each database was originally obtained or complied...".[98] This could include "data mining and data profiling for both research and administrative use of personal information".[99]

By introducing new provisions that expand the collection, use and disclosure of personal information, *Bill 3* also introduces new risks for privacy and access rights. One legal analysis notes that the amendments shift the intent and mandate of *FOIPPA* from privacy protection and accountability "to a much more open regime of access to personal information".[100] It concludes that "if the intent of these amendments is to create a more extensive data pool for data linking purposes that have no relationship to the original needs and goals of public

94 ICBC FOI Request F197019.

95 Ministry of Labour, Citizen Services and Open Government. 2011. *News Release: Amendments Introduced to Strengthen Privacy Act*, www2.news.gov.bc.ca/news_releases_2009-2013/2011LCITZ0019-001255.htm.

96 Shaw, Rob. 2011. BC Overhauling Privacy Laws. *The Victoria Times Colonist*, www2.canada.com/victoriatimescolonist/news/story.html?id=be56c096-b1de-44d3-89fa-0cd0008a1fed.

97 Ministry of Labour, Citizen Services and Open Government, 2011.

98 Government of British Columbia. 2011. *Bill 3-2011, Freedom of Information and Protection of Privacy Amendments Act, 2011*, www.leg.bc.ca/39th4th/1st_read/gov03-1.htm.

99 Scott, Jill. 2012. Bill 3 and Privacy Implications. *Canadian Journal of Administrative Law and Practice(23)* 5, p. 42.

100 Scott, 2012, p. 76.

bodies, the potential harm to privacy is considerable".[101] Insofar as they increase data sharing and linking across government sectors, bodies and agencies, the new provisions seem at odds with *FOIPPA's* mandate to regulate privacy in the public sector. The bill adds "a confusing array of new powers for collection, use and disclosure of 'personal identity information'[102] by the ID Services Provider", that is, the Office of the Chief Information Officer. Moreover, these new powers could govern vast quantities of personal information "without independent stewardship and ethics review or any guarantee of transparency".[103] In general, the amendments to *FOIPPA* reduce residents' control over their personal information and limit transparency and accountability while expanding how and for what reasons their personal information can be shared.

An all-party special committee struck in 2009 to review *FOIPPA* consulted a range of stakeholder groups, including provincial and local public bodies, professional organizations, advocacy groups, unions and citizens. Key among the 118 submissions was the one from Paul Fraser, former Acting BC Information and Privacy Commissioner. Fraser warned against compromising privacy protections in the name of bureaucratic efficiency: "We are adamant that no legislative amendments...are needed to authorize data sharing and data matching activities within government, and would strongly oppose any weakening of the existing right to privacy".[104] Fraser further advised that "government should not proceed with any more data sharing initiatives until a meaningful public consultation process has occurred, and the outcome of that process is an enforceable code of practice for data sharing programs".[105] Among the recommendations in the committee's report, released in 2010, was public consultation on the new data sharing proposals.[106]

The government did not consult the public on the data sharing initiatives proposed for *FOIPPA*. It did, however, conduct a confidential process on the *FOIPPA* amendments, the results of which have not been publicized. The BC Civil Liberties Association and BC Freedom of Information and Privacy Association, two key privacy advocacy groups in the province, declined to participate due to the confidentiality requirement. Instead, they submitted joint comments to the Ministry of Citizen Services, roundly condemning *Bill 3* as a

101 Ibid, p. 42.

102 According to Schedule 1 of *FOIPPA*, "personal identity information" is "any personal information commonly used, alone or in combination with other information, to identify or purport to identify an individual."

103 Scott, 2012, p. 48.

104 Reynolds, Keith. 2011. BC Government Claims New Power Over Personal Information. Public Comment Didelined. *Policy Note*, www.policynote.ca/bc-government-claims-new-power-over-personal-information-public-comment-sidelined.

105 Ibid.

106 Special Committee to Review the Freedom of Information and Protection of Privacy Act. 2010. *Report. Second Session. Thirty Ninth Parliament.* British Columbia: Legislative Assembly, www.leg.bc.ca/cmt/39thparl/session-2/foi/reports/PDF/Rpt-FOI-39-2-Rpt-2010-MAY-31.pdf.

costly, wasteful violation of privacy rights that "trades citizens' essential privacy rights for administrative efficiency". They further asserted that the amended act "will move the province closer than any other in Canada to being the 'surveillance state' that privacy commissioners across Canada and around the world have warned about".[107]

Despite the strong misgivings of privacy advocates, BC's Information and Privacy Commissioner Elizabeth Denham generally approved of *Bill 3,* especially the "significant new oversight powers", including that data sharing initiatives will come "under the scrutiny" of the commissioner. There are no formalized rules to govern the broader identity and information management system (IdIM) system, however. Rather, the *FOIPPA* amendments "leave much to the discretion of the Minister with respect to setting the direction of the IdIM system, privacy impact assessments and data linking".[108] Although Commissioner Denham will provide oversight of PIAs and new data linking initiatives, not all initiatives will be subject to review.

From this review of legislative amendments, it is clear how the government sought to change the law to align with its integrated identity and information management "solution". It did so by creating new legal provisions for the multi-directional flow of the personal identity information of almost every British Columbian. The result is a dramatic transformation of the province's identity infrastructure and privacy law. As we discuss below, however, this transformation has taken place in relative secrecy.

107 British Columbia Freedom of Information and Privacy Association & British Columbia Civil Liberties Association. 2012. *Re: Consultation on amendments to the regulation to the Freedom of Information and Protection of Privacy Act,* http://fipa.bc.ca/library/Reports_and_Submissions/FIPA-BCCLA_Submission%20_on_FOIPP_Act_Regulations--March_2012.pdf.

108 Scott, 2012, p. 61.

5. (Lack of) Transparency

The BC Services Card is the latest major IT project to be unveiled as part of British Columbia's Government 2.0 strategy. It is a key component of the broader identity and information management (IdIM) infrastructure that is meant to link personal information across government information silos to "better achieve outcomes".[109] Because of the government's depiction of its IdIM program as a transformative and new approach to linking BC residents' data there should be public documentation of the government's plans. This has not been the case, however: even today, a year after this project began, relatively few documents are available to explain the intricacies of how the IdIM or BC Services Card infrastructures will function.

When this research project began in July 2012, there were very few publicly available documents pertaining to the BC Services Card, although there was much seemingly outdated information on BC's identity management strategy. Researchers on this project had difficulty obtaining information directly from pertinent government ministries and representatives. Requests for interviews with the Minister of Health, Minister of Citizen Services and Open Government, and the Chief Information Officer received no response. Five freedom of information (FOI) requests filed by the BC Civil Liberties Association to ICBC, Ministry of Health and Ministry of Citizen Services resulted in no documentation. Two of those requests are still pending, although the process was started in September 2012. The BC Freedom of Information and Privacy Association (BC FIPA) also filed five FOI requests.

In November 2011, BC FIPA received 600 heavily redacted and duplicated pages from ICBC related to the early planning of the "CareCard Initiative". More than a year later, in March 2013, BC FIPA received 350 redacted pages of information from Citizen Services containing details about vendor involvement in the planning process and some financial data. That is the extent of information received from the province on the BC Services Card through FOI requests. The government justified one denial of information by invoking several sections of the *Freedom of Information and Protection of Privacy Act*, including section 12, which allows a provincial public body to withhold information on the grounds that it would reveal cabinet confidences, and section 13, which allows a public body to withhold advice or recommendations. Other government responses to FOI requests simply said there were no records related to the requests. Still other requests were transferred amongst the three government departments—OCIO, MoH and Citizen Services—starting the process anew,

109 Architecture and Standards Branch. 2009. *Identity Information Management Architecture Summary.* Victoria, BC: Office of the Chief Information Officer, www.cio.gov.bc.ca/local/cio/standards/documents/architecture/idim_arch_summary.pdf.

including new deadlines and automatic extension periods. This is the reason that the BC Civil Liberties Association has yet to receive any responses to its FOI requests.

Organization	FOI Request #	Made by	Submitted	Received	Response
ICBC	F197019	BC FIPA	May 24, 2011	November 25 2011	600 redacted pages
Ministry of Health	HTH-2011-00034	BC FIPA	May 24, 2011	Dec. 5 & 6, 2011	Invoked sections 12, 13 & 17 of FOIPPA
Ministry of Health	HTH-2012-00124	BC FIPA	July 12, 2012	Aug. 8, 2012	Awaiting response
Ministry of Citizen Services	CTZ-2012-00107	BC FIPA	Aug. 3, 2012	Sept. 7, 2012	No responsive records
Ministry of Citizen Services	CTZ-2012-00117	BC FIPA	Sept. 6, 2012	March 20, 2013	350 redacted pages
ICBC	F213959	BCCLA	Sept. 29, 2012	Oct. 18, 2012	Transferred to CTZ & HTH
Ministry of Health	HTH-2012-00212	BCCLA	Oct. 18, 2012	Closed Jan. 8, 2013	Partial transfer from ICBC
Ministry of Citizen Services	CTZ-2012-00166	BCCLA	Oct. 18, 2012	Pending	Partial transfer from ICBC
Ministry of Health	HTH-2013-00009	BCCLA	Jan. 8, 2013	Jan. 24, 2013	Transferred to CTZ
Ministry of Citizen Services	CTZ-2013-00033	BCCLA	Jan. 24, 2013	Pending	Transfer from HTH

Figure 1 Freedom of Information Requests

One representative from the OCIO eventually agreed to be interviewed, but would not allow the interview to be recorded. When asked why government officials associated with the BC Services Card project were so reluctant to speak with our research team or provide information, this representative explained that people "were afraid". On October 2, 2012, BC's Chief Information Officer (CIO) Dave Nikolejsin, the face of identity management transformation in the province, was quietly removed from his post and transferred to the Ministry of Environment. There was no explanation for Nikolejsin's abrupt transfer, barely two months before the Services Card was originally set to launch. After more than a year, Citizen Services returned an FOI request for all correspondence between Nikolejsin and SecureKey Technologies, the lead vendor for the Services Card project, with "no responsive records".

It is inexplicable that there should be no correspondence between BC's Chief Information Officer, whose office is the lead government organization on the BC Services Card project, and the main vendor partner in the project, SecureKey Technologies. This is even more baffling considering SecureKey's significant involvement in the planning and development of the card program, as evidenced by government documents. The *Masters Services Agreement* between the province and SecureKey, dated April 2012, indicates that Nikolejsin was on the Joint Executive Committee for the BC Services Card, along with two SecureKey representatives. The committee was to meet monthly during the implementation of the card, and quarterly during its operation. Among other things, the committee was to "provide executive oversight and strategic direction" and "set priorities for guiding the relationship

between the Parties".[110] This seems to suggest a primary relationship between the CIO and SecureKey.

The lack of email or other written correspondence between Nikolejsin and SecureKey seems to point to what BC's Information and Privacy Commissioner calls "oral government". This is the practice of government business "undertaken verbally and in a records-free way" and includes the use of private email accounts.[111] In her investigation into a complaint filed by BC FIPA about an increase of "no responsive records," Commissioner Denham affirmed that "without a duty to document, government can effectively avoid disclosure and public scrutiny as to the basis and reasons for its actions".[112] Denham considered the practice of oral government problematic enough to warrant entrenching a "duty to document" in provincial privacy legislation. Such a duty would require that public officials document their decisions, deliberations, their proffered or received advice, or other professional activities. The lengthy delays in releasing information to researchers and advocates, combined with apparent government obfuscation and little more public information than a promotional campaign about the BC Services Card, are cause for concern in terms of good governance and government accountability. In addition to this serious lack of government transparency, there are other concerns with the BC Services Card itself, which are the focus of the next chapter.

110 SecureKey Technologies and Province of British Columbia. 2012. *Master Service Agreement with SecureKey Technologies*, www.cio.gov.bc.ca/local/cio/strategic_partnerships/v13-Master_Services_Agreement%28redacted%29.pdf, p. 60.

111 Denham, Elizabeth. 2013. *Investigation Report F13-01. Increase in No Responsive Records to General Access to Information Requests: Government of British Columbia*. Victoria, BC: Office of the Information and Privacy Officer for British Columbia, p. 3, www.oipc.bc.ca.

112 Ibid.

6. The BC Services Card

Despite the lack of transparency around the planning and development process of the BC Services Card, the government was nevertheless clear about its intention to "transform the way [the Province of BC] does business." This is driven, in part, by the government's insistence on "leveraging technological solutions and innovation" in the drive towards digital record keeping and increased electronic service delivery.[113] The rationales that appear to drive other ID card-based identity systems, such as national security agendas (e.g. REAL ID in the US) and ideological imperatives like immigration reform (e.g. national ID card in Britain) are largely absent with the BC Services Card. Instead, the primary motivation for a card-based integrated identity system in British Columbia appears to be attaining efficiencies by investing in technology, reducing costs and streamlining service delivery. These drivers are linked to secondary rationales, such as convenience and improved patient outcomes. In this technocratic approach, the acquisition of more information (through data linking) by government on the one hand, and the downloading of service delivery to the citizenry (through increased "self-service") on the other are essential to achieving these efficiencies. However, clear plans to link the card into a national identity system, by ensuring that it is interoperable on a federal level, suggest that the drive for efficiencies aligns with objectives set by the Government of Canada. The drive towards efficiencies can be based on other data as well: as an example, private sector partners, including VISA, have been part of the 2010 working group that has evaluated the merits of a photo health card for government services. That the working group was not solely focused on health care entitlement makes clear that a broad range of uses have been envisioned for the identity system since its earliest development stages. To understand where the privacy, security and civil liberties issues arise with this model of ID management, we now turn to a more in depth examination of the card itself.

Physical Attributes, Technical Specifications and Database Architecture

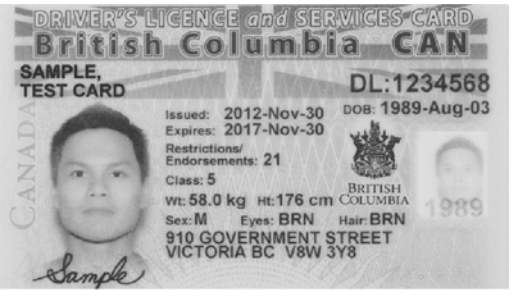

Figure 2 **Sample BC Services card**

Phase I of the BC Services Card is operational. The Provincial Identity Information Services Provider (PIISP) runs the Identity Assurance Service (IAS) on behalf of the Office of the Chief Information Officer. The PIISP collects and stores the personal identity information of BC residents enrolled in the card program. In the first part of Phase 1, this collection is limited to the personal information of those who are enrolled in the

113 Office of the Chief Information Officer. 2010. *IM/IT Enablers Strategy for Citizens@The Centre: BC Government 2.0*, p. I, www.gov.bc.ca/citz/citizens_engagement/it_strategy.pdf.

Medical Services Plan (MSP). By November 2014, however, scheduled amendments to the *Motor Vehicle Act* Identification Card Regulation will expand BC Services Card enrolment to include non-recipients of MSP.[114] By 2018, the BC Services Card will be mandatory for all BC residents, effectively enrolling the entire population into the province's identity system. Phase II, which comprises the activation of the embedded computer chip, is set to commence in 2018.

The BC Services Card comes in three versions:

- **A stand-alone health/ID card**
  - Displays name, sex, address, date of birth, photograph, signature, Personal Health Number and expiry date of Medical Services Plan coverage
  - Contains a "contactless" computer chip with a unique ID tag featuring the Personal Account Number
  - Utilizes ICBC's front-counter identity-proofing services and facial recognition technology
- **A hybrid health card/driver's licence**
  - Displays name, sex, address, date of birth, photograph, signature, Personal Health Number and expiry date of Medical Services Plan coverage
  - Additionally displays the same personal identity information as the driver's licence: eye and hair colour, weight, height and whether corrective lenses are required
  - Contains a "contactless" computer chip with a unique ID tag featuring the Personal Account Number
  - Utilizes ICBC's front-counter identity-proofing services and facial recognition technology
- **A non-photo card**
  - Issued by Health Insurance BC
  - For people under 19 and over 75
  - Contains a "contactless" computer chip with a unique ID tag featuring the Personal Account Number
  - Does not contain a photograph

114 Denham, Elizabeth. 2013b. *BC Services Card Phase I Review*. Victoria, BC: Office of the Information and Privacy Commissioner for BC, www.gov.bc.ca/citz/down/letter_E_Denham_Re_BC_Services_Card_Phase_1_Review.pdf.

The BC Services Card is manufactured and its chip personalized by Iris Corporation, a Malaysian firm, and is engraved by IBM, a longtime provincial technology provider. The card's physical attributes include layered polycarbonate plastic with embedded holography and laser engraved markings for photo and text images. These are security features intended to provide a "high assurance" that the cards are not forged.[115] The card is based on EMV, the payment card industry standard for security and global interoperability. It has a magnetic stripe, which contains all the information visible on the card in machine readable format.[116] In an attempt to adopt a more secure means of transferring data, the card is embedded with a Near Communication Field (NFC) computer chip that provides cryptographic proofing functions. The chip is "contactless", meaning that it can be read by waving the card at a reader. It contains a unique ID tag inscribed with a personal account number (PAN) that is associated with a government database containing a "meaningless but unique identifier" (MBUN). An MBUN is linked to each card issued to a cardholder at enrolment and is held by the Office of the Chief Information Officer. The MBUN is used as part of the authentication process; it is a global identifier that is used to "look up" service specific identity credentials. In short, the PAN on the chip is used to identify the MBUN which, in turn, is used to look up specific credentials for various government services.

Biometrics/Facial Recognition Technology

The BC Services Card uses ICBC's existing facial recognition technology (FRT) systems. At enrolment, applicants have their photographs taken and converted into biometric templates that are subsequently matched against the existing ICBC databases to ensure a single person is not registered under more than one identity. This matching functionality entails extending the Corporation's FRT capacity to "support the ability to recognize matches and unexpected mismatches between health card images and [driver licence] images".[117] Operationally, this requires establishing processes for evaluating mismatches. According to ICBC, "facial recognition will be done against all photos captured by ICBC's image capture process...to support Personal Health Number (PHN) fraud investigation."[118] In the case of "hits" either ICBC or the Ministry of Health will be responsible for auditing for accuracy, depending on whether the image was taken for driver's license or health card issuance.[119] The overall

115 Government of British Columbia. 2009. *News Release: High Tech Driver's Licence to Help Stop ID Theft, Frau,* www2.news.gov.bc.ca/news_releases_2005-2009/2009PSSG0012-000157.htm.

116 Interview with a representative of the Office of the Chief Information Officer on November 13, 2012.

117 *Government Care Card Initiative: ICBC Program Model, Version 2.6,* 2010, p. 27, ICBC FOI Request F197019.

118 ICBC FOI Request F197019, p. 14.

119 Ibid, p. 12.

efficacy of the imaging process, however, remains unclear as ICBC has not provided any significant information concerning the statistical accuracy of its evaluation system.[120]

Near Field Communication

The communications protocol between the contactless chip in the BC Services Card and the card reader relies on near field communication (NFC), a set of technical standards governing communications protocol (and data exchange) based on radio frequency identification (RFID) technology. The BC Services Card will use the ISO 14443 standard, which is meant to be read up to 10cm away. NFC is increasingly used for identification and payment purposes around the world. In Japan, for example, student IDs are sometimes stored on NFC chipped cards to facilitate class registration, food purchase, and other commercial uses; in South Korea, NFC is used for mobile payments.[121] Researchers received conflicting information regarding whether the NFC chip on the Services Card is encrypted, preventing it being read or "skimmed" by unauthorized parties. Skimming, in an electronic environment, refers to the capture of information by an unauthorized third-party. A pre-smartcard example is the capturing of data from a bank card's magnetic stripe when run through a compromised banking machine. Documents obtained through a freedom of information request show ICBC's concern, early in the planning process, about the card having a non-encrypted chip. According to those documents, ICBC's privacy team received assurances that the chip would indeed by encrypted, thus safeguarding the ID tag containing the personal account number (PAN) stored there. Interviews with the Office of the Chief Information Officer in 2012, however, suggested that the PAN would not be encrypted, though the chip would perform cryptographic proofing to guarantee that the chip – and PAN – were active and valid.

Database Architecture

Amendments to the *Freedom of Information and Protection of Privacy Act* in 2011 authorized the changes to information sharing required by the BC Services Card. These amendments also included creating a Provincial Identity Information Services Provider (PIISP) to provide identity and information management services for the province. In July 2012, the Minister of Citizens' Services designated its own ministry as the provider. Within the Ministry of Citizen Services, the Office of the Chief Information Officer (OCIO) operates the PIISP, which in turn provides the Provincial Authentication Application (PAA). The following describes the

120 Parsons, Christopher and Molnar, Adam. 2012. *The BC Services Card: Drivers, Architectures, Risks,* www.bccla.org.

121 Paus, Annika. 2007. *Near Field Communications in Cell Phones,* www.emsec.ruhr-uni-bochum.de/media/crypto/attachments/files/2011/04/near_field_communication_in_cell_phones.pdf.

database architecture with key standards identified as well as SecureKey's prominent role in authenticating identities throughout the Services Card initiative.

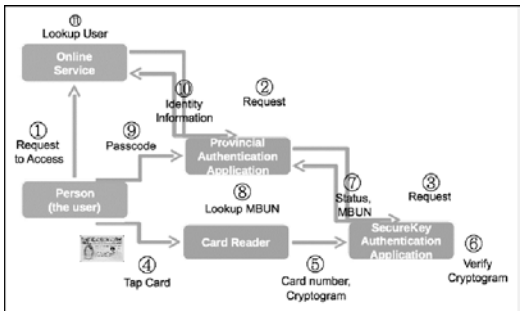

Figure 3 **BC Services Card data flow architecture**

When a person presents her BC Services Card at a point of service such as a doctor's office or medical laboratory, the authentication process is initiated by tapping the card on a card reader linked to an office or laboratory computer. The reader invokes the SecureKey software to communicate with the NFC chipped card, accessing the card's Personal Account Number (PAN) and cryptogram.[122] The SecureKey Application communicates with the Office of the Chief Information Officer (OCIO) through its Provincial Authentication Application after verifying the authenticity of the cryptogram. SecureKey verifies that the PAN is still active. The chip validation process looks like the following:

Validating the NFC Chip

Stage 1: Card → USB reader

- A cryptogram is created to confirm chip authenticity.

Stage 2: USB reader → SecureKey

- SecureKey interacts with reader to evaluate the cryptogram generated in Stage 1. This interaction confirms that an authentic card is present and, if so, sends the cryptogram to the SecureKey Application.

Stage 3: SecureKey → OCIO

- After confirming the authenticity of the cryptogram, SecureKey communicates with the OCIO to confirm that the PAN remains active.[123]

Upon confirming that the PAN is active the OCIO will release a meaningless but unique number (MBUN) specific to the user and provide it to SecureKey. Given that the PAN is confirmed active, the reader at the point of service and SecureKey application securely exchange session tokens using OAuth 2.0, an open standard for authentication. The SecureKey server then transforms the MBUN into a Persistent Anonymous Identifier (PAI) relevant to the service being requested (i.e. cardholders will have one PAI for Health, another

122 It remains unclear to us how this proof is guaranteed or what cryptographic methods are used in arriving at card-present verification.

123 Note that the PHN itself does not appear to be transmitted given this is a triple-blind process.

for Citizen Services, and so on). The PAI is then transmitted to the point of service. This can be visualized as follows:

Validating the Cardholder

Stage 4: OCIO → SecureKey
- Transmits MBUN.

Stage 5: POS ←→ SecureKey
- Since card was authenticated in Stage 3, an encrypted OAuth 2.0 session is established.

Stage 6: SecureKey + MBUN = PAI
- SecureKey translates MBUN to PAI.

Stage 7: SecureKey → POS
- SecureKey sends the PAI to point of service.

In the case of accessing health services, when the point of service has acquired the persistent anonymous identifier (PAI) that is specific to the Ministry of Health (i.e. MoH has one PAI linked to an individual, whereas another ministry will have a different PAI linked to the same individual) it has to be translated into Personal Health Number (PHN) because the government's Electronic Health Record applications only "understand" the PHN. To translate the PAI, MoH will look up the PAI, correlate it with the PHN associated with the individual, and pass that to the point of service.

Translating the PAI

Stage 8: POS → Ministry of Health client registry
- Point of service sends the persistent anonymous identifier to MoH to look up the linked Personal Health Number.

Stage 9: MoH client registry → POS
- MoH transmits the PHN to the point of service.

This concludes the electronic transactions and will have verified the cryptographic validity of the NFC chip, transmitted information between the Ministry of Health and the Office of the Chief Information Officer to verify that the BC Services Card is still active, and enabled the counter staff to retrieve the associated record(s). Ultimately, in this process the point of service just needs to cryptographically verify and access the personal health number (PHN) associated with the card. Since the cardholder is physically present, visual evaluation can be performed to check that the card in question belongs to the individual requesting service. Our research suggests that neither the OCIO nor MoH have adequately prepared for this process: the OCIO admits it is unable to explain "definitively" how in-person card transactions (the only transactions the card is capable of until the chip is activated) "will work at this time".[124]

124 Email communication between author and senior OCIO official, April 4, 2013.

Although the card has been available to the public since February 2013, the OCIO continues to have “several options under consideration”.

Where online services operate as the point of service, a slightly different process and set of standards applies. The following outlines an online situation, available during Phase II of the BC Services Card program: When a cardholder visits the Ministry of Health’s website to look up her prescription history, protocols based on the Security Assertion Markup Language (SAML) are used to facilitate single sign on. MoH directs the user to the Office of the Chief Information Officer’s website for authentication. The website initiates the SecureKey Application residing on the cardholder’s computer and prompts her to tap her card. SecureKey validates the chip with the OCIO (see Stages 1-3) and provides the MBUN (Stage 4). The core difference arises during the OAuth process (Stage 5), where a two-factor authentication process is used. This means that a user is prompted to enter their passcode before the session is established. After successfully entering the passcode, data flows according to Stages 6-9, with the difference being that instead of a MoH point of service being served data, it is the web-enabled client that is served the information.

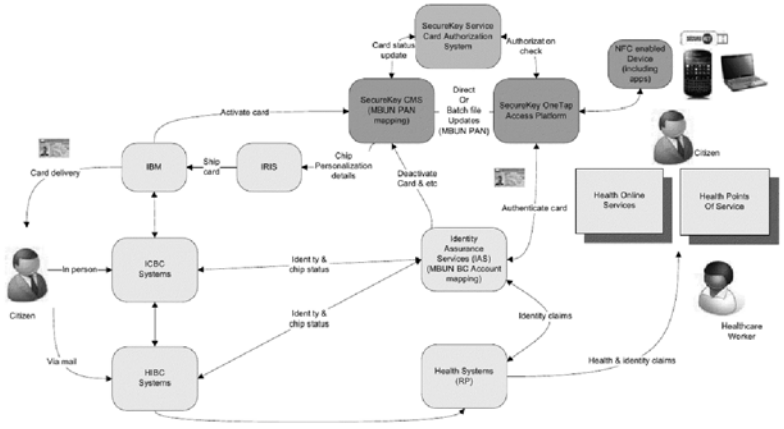

Figure 4 User centric data flow architecture

7. SecureKey Technologies: Wrapping up Canada?

Private vendors have played a significant role in designing and developing the BC Services Card. In particular, SecureKey Technologies has been heavily involved in developing, testing, and leading vendor integration efforts. Per government documents, key officials have turned to the company to explain how the system would function, and have relied on SecureKey to provide "expert" advice in the areas of card production and issuance.

British Columbia directly awarded the $20 million contract for credential and authentication services to SecureKey in January 2012. The province justified its failure to tender the six-year contract on the basis that the federal government had already hired SecureKey to provide a national credential brokering service. One of the province's requirements for its new identity card was that it "work with, interoperate with and [be] compatible with Canada's credential broker service".[125]

SecureKey's stated goal is a "pan-Canadian public-private digital identity and authentication regime" that includes all the provinces and enrols the banking and telecommunications sectors to provide credential authentication.[126] In 2011, SecureKey partnered with three major Canadian banks and in 2013 it reached agreements with three of Canada's telecommunications providers—Bell, Rogers and Telus—to install its authentication technology on mobile phones.[127]

André Boysen, the company's Executive Vice President, describes how four key actors—federal and provincial governments, banks and telecommunications companies—participate in the SecureKey model:

> The *federal government* can set standards and leverage its buying power in a way that individual provinces can't. The *provinces* are the source of identity—birth certificates and the licenses we carry around in our wallets. But the problem is that we don't deal with the province very often; it's rare that we have to talk with them and this makes it hard to authenticate online...This is where the *banks* come in. They have a very tight relationship with 98 percent of Canadians. What the *telcos*—bring to this is something that Canadians always have in their pockets—their phones.[128]

---

125 Minister of Labour, Citizens' Services and Open Government and Insurance Corporation of British Columbia. 2012. *Notice of Intent #SATP-290*, http://bccla.org/wp-content/uploads/2012/10/20120101-BC-Services-Card-notice-of-intent.pdf.

126 SecureKey Technologies Inc. 2012. *Consultation Submission from SecureKey Technologies Inc. in response to Strengthening Canada's Anti-Money Laundering and Anti-Terrorist Regime*, www.fin.gc.ca/consultresp/pdf-pcmltfa-lrpcfat/023-SecureKey-eng.pdf.

127 *SecureIDNews*. Canadians to Get Mobile Authentication, www.secureidnews.com/2013/02/21/canadians-to-get-mobile-authentication/?source=rss.

128 Code Technology. 2012. *SecureKey–The Interview*, https://codetechnology.wordpress.com/2012/09/24/securekey-the-interview.

British Columbia is SecureKey's first provincial client, apparently part of its sweeping vision that encompasses "financial institutions, health care providers, government organizations and others". According to Boysen, "'wrapping up Canada' (all remaining provinces) is the current goal".

SecureKey has signed a "confidentiality covenant" with the province that includes screening employees and requires its employees to sign confidentiality agreements. The covenant requires that SecureKey "create and maintain detailed Records logging the activities of all Service Workers in relation to their access to Sensitive Information".[129/130] It also requires that the company establish strong access controls that adhere to a "documented process for limiting access to Sensitive Information to those persons who are authorized to have that access and for the purposes for which they are authorized, which process must include measures to verify the identity of those persons".[131]

While expansive, the confidentiality covenant may not protect against internal bad actors or attackers. This is because the technical design of the data flow architecture does not prevent SecureKey from "seeing" what services a cardholder is accessing, thus enabling user profiling. As a trusted partner in the BC Services Card program, SecureKey's position in the technical infrastructure means that it could be used to correlate those identifiers that, independently, are meant to enhance citizen privacy.

This capability is significant because SecureKey markets its service as highly privacy protective. As we detail in Chapter 6, however, there are concerns associated with its data linkage infrastructure: while the company says its uses a triple-blind system whereby no individual party can ever know who is accessing what service, we suggest this is really a "triple-blind lite" system. The "lite" version does permit data linkage to learn who is accessing what service at a technical, if not a policy or legislative level. In effect, SecureKey's position in the data flow architecture does not necessarily prevent it from re-identifying citizens and linking them to the services they are accessing. Thus, while the authentication process is billed as a triple-blind system, the technical dimensions do not appear to have fully implemented such a system. This is because under a fully-functioning triple-blind system, there should be no technical capacity to engage in re-identification processes. In the following chapter, we discuss in greater detail the privacy and security problems associated with this model.

---

129 Province of British Columbia. 2012.

130 In the *Master Service Agreement*, "sensitive information" is "personal information" as defined in the *Freedom of Information and Protection of Privacy Act*.

131 Province of British Columbia, 2012.

8. Privacy Risks and Security Vulnerabilities

It is difficult to separate privacy and security issues when discussing a technical system that is designed for maximum information sharing. Security vulnerabilities tend to invite privacy risks. Such risks can be defrayed, however, by developing strong security infrastructures that incorporate "privacy enhancing technologies" (PETs). Together, strong security and PETs can ensure that technical systems adhere to the spirit, as well as letter, of privacy law. In what follows, we first outline the risks linked to the privacy and security characteristics of the BC Services Card initiative. This is followed by a more detailed accounting of the specific types of vulnerabilities that may lurk within the card's corresponding technical infrastructure, and the significance for citizens' privacy.

Privacy does not appear to have been thoroughly designed into the Services Card. While consistently referencing privacy protections, the government has poorly explained how the card will leverage technology to keep citizens' personal information secure, their identity safe and their privacy intact. Rather, it describes the card in the language of technological determinism: its "high-level identity proofing" marks "the first service utilizing identity information management services to move higher value services online".[132] Broad claims are made regarding the card's security and privacy features, including that the card will "help keep everyone's personal information more secure and help prevent fraud, like identity theft or misuse of government services".[133] Such protection will be accomplished by "using state-of-the-art technology and upgrading information systems" as well as by embedding "enhanced security features to help protect personal information and prevent fraud".[134] The efficacy of these security features remains unknown: publicly available documents, as we discuss below, in fact seem to challenge these broad assertions.

The same holds true for statements about the privacy protective elements of the card. After assuring that the BC Services Card program adheres to the *Freedom of Information and Protection of Privacy Act* (which was changed specifically to accommodate the card's data linking infrastructure), citizens were assured that "new technology" built into the card will secure personal information and ensure that "services are delivered to the right person". Further, the government states that personal information collected when applying for the card will only be used to confirm identity and service eligibility. It affirms that personal information will only be disclosed to government agencies at the time citizens use the card,

132 OCIO, 2011, p. 10.

133 Government of British Columbia. nd. *Families & Residents: Privacy & Security,* www2.gov.bc.ca/gov/topic.page?id=F694A0A3880B4499BFAF0FAAE32C5F17.

134 Ibid.

and then only by role-based access. “Unless it’s authorized by law, your records will not be shared across agencies providing services”.[135] Such statements provide little reassurance, however, given the government’s readiness to change laws to meet new policy objectives. Moreover, irrespective of legislation, the government’s track record of safeguarding the privacy of British Columbians advises caution. Scathing reports from BC’s Auditor General about serious flaws in large IT projects suggest that citizens’ deeply sensitive personal information is often inappropriately accessed and shared, and generally poorly protected.

Government messaging notwithstanding, there are core risks and vulnerabilities that could be associated with the BC Services Card. Given the relative scarcity of primary source documents about the project, however, many of the concerns discussed identify the *kinds* of questions that need to be answered and the *types* of vulnerabilities that such data systems possess. Importantly, when considering the security of the card, “what matters is how the system might fail when used by someone intent on subverting that system: how it fails naturally, how it can be made to fail, and how failures might be exploited”.[136]

Potential weaknesses in the BC Services Card arise around card issuance and forgery, data management and security processes, the NFC chip, and function creep. As part of this research we conducted an in depth security analysis complete with recommendations, the results of which are published separately. What follows is a summary of the findings.[137]

Enrolment

It is well understood that the security of identity documents begins—and often ends—with the strength of enrolment processes. Enrolment is dependent on root or foundation documents, such as birth certificates. If these are obtained fraudulently, then all subsequent identity credentials will be fraudulent. Further, there are a number of mechanisms that could be leveraged to attack the point of service (POS)—the ICBC counter—where the enrolment process takes place. The POS is critical because it establishes the authenticity of the root documents. This means that counter staff must be able to detect false root documents that fraudsters use to apply for legitimate cards. Moreover, staff members must be “good” actors and not attackers, or complicit in attacks to generate identity credentials based on fraudulent foundation documents. Any secondary evaluation process—such as biometric facial recognition systems, or post-enrolment screening—similarly need to be tested for accuracy

135 Government of British Columbia. nd. *Families & Residents. Privacy*, www2.gov.bc.ca/gov/topic.page?id=56E8F986C75947AD87845E4E0D2E3332.

136 Schneier, Bruce. 2004. *A National ID Card Wouldn’t Make Us Safer*, https://www.schneier.com/essay-034.html.

137 Parsons, Christopher and Molnar, Adam. 2012. *The BC Services Card: Drivers, Architectures and Risks*, www.bccla.org.

and free from attackers. These kinds of problems are endemic to *any* identity credential system.[138]

Physical Card Protections

The BC Services Card adopts a series of defence-in-depth strategies. In addition to making substrate modification difficult, the card uses specialized holographic images and province-specific imagery. However, the means of card tampering vary and well-resourced attackers have defeated card security mechanisms time after time.[139]

> Even though manufacturers work hard to improve "smart" card tamper-resistance, mass produced smart cards will likely never be able to withstand invasive physical attacks for more than a few years following their release. New sophisticated attack apparatus will appear, and existing apparatus is being improved all the time. Organized crime will hire expertise comparable to government experts, and sophisticated tools are increasingly accessible to hackers and undergraduate students at technical universities.[140]

Defeating physical-layer protections occurs at a social, rather than technical level insofar as modifications to ID cards must be "authorized" by real people who visually or physically inspect the document. Consequently, successful presentation of fraudulent identity documents tends to be "about fooling people, not beating hardware".[141]

Smartcard chips often succumb to tampering when motivated attackers have sufficient resources. Problematically, audits of smartcard chips have been limited, though they are improving with major credit companies requiring penetration testing of their issued chips.[142] Such audits are essential to verifying that the cryptographic authentic features of the BC Services Card are actually resistant to being tampered with or fraudulently replicated. It remains unclear what kinds of penetration audits have been performed against the NFC chip contained in the card. There is no reason to expect that attackers will stop innovating as chip-based security measures become increasingly sophisticated: past "unbreakable" chips have been broken.[143] It is in light of such attacks that smartcards, ideally, are designed to be

---

138 Any security system overlaid on existing infrastructure must consider the possibility of the organization/system having *already* been compromised. Thus, new systems should try to develop processes that prevent existing bad actors from expanding their actions to the new service offering(s).

139 See Anderson, Ross. 2007. Physical Tamper Resistance. In *Security Engineering (Second Edition)*. Indianapolis: Wiley.

140 Brands, Stefan. 2000. *Rethinking Public Key Infrastructures and Digital Certificates*. Cambridge, MA: The MIT Press, p. 229.

141 Ross Anderson. 2007. Security and Printing Seals, *Security Engineering (Second Edition)*. Indianapolis: Wiley, p. 454.

142 For more on the poor incentives surrounding security evaluations, see Anderson, 2007.

143 For a brief overview of how smartcards and microcontrollers have been attacked, see Anderson, 2007, pp. 499-514.

capable of securely and reliably authenticating an individual for a government service offering, even if the card has been "cracked". This often requires the technical capability to "rotate" the security proofing associated with the smartcard, in the event that attackers successfully attack its hardware.

Data Management and Security

The technical infrastructure of the BC Services Card is premised on the ability to securely use the public internet to transfer data across government ministries and to SecureKey, relying upon the Transport Layer Security (TLS) encryption protocol.[144] TLS facilitates trust in online communications by cryptographically protecting against eavesdropping and tampering. In the architecture underlying the card, TLS is augmented by Secure Shell (SSH), a cryptographic network protocol that uses public key encryption. There are several ways of attacking the TLS/SSH encryption, as well as broader issues that could affect the data transfer network providing online service delivery in BC. Security experts recognize TLS as a fundamentally broken system,[145] and online cryptographic service delivery tends to suffer from Man-in-the-Middle attacks, "eavesdropping", and Distributed Denial of Service (DDOS) attacks. These challenges are outlined in more detail in our technical analysis of the Services Card.[146]

Additionally, there are, as always, threats associated with bad actors inside the organizations themselves. Internal bad actors drive a vast number of attacks by exploiting their position within the data networks. Role based access controls provide a means of managing user access to complex computer systems, thereby restricting access to personal information to authorized employees. The role is related to a user's job or position within an organization; each role is associated with permissions or privileges within the system. Employees are assigned privileges based on their duties, qualifications or competencies.

Role based access controls are dependent in part on trust. The challenge with role based permissions is that employees have access to a range of records, and specific (not necessarily all) fields associated with any given record. Problems arise when an employee looks up a person's record without authorization. Logging and auditing employees' access to data can

144 According to an email exchange between ICBC employees: "Regarding the transmissions of the information from the ICBC mainframe to the Shared Services mainframe, please be aware that portions of this network are *not considered private* and are *provided by Telus*." (emphasis ours). FOI Request F197019.

145 See e.g. Gallagher, Sean. 2011. New Javascript Hacking Tool Can Intercept Paypal and Other Secure Sessions. *Ars Technica*. Retrieved from http://arstechnica.com/business/2011/09/new-javascript-hacking-tool-can-intercept-paypal-other-secure-sessions/; Arnbak, A. and Van Eijk, N. 2012. *Certificate Authority Collapse*. Draft of paper prepared for TPRC's 40th Research Conference on Communication, Information and Internet Policy, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2031409.

146 Parsons and Molnar, 2012.

alleviate some of the challenges related to the inappropriate accessing of personal information. To successfully govern how employees access data, however, these logs must be monitored and subsequently audited. Such governance can be limited and is only as effective as the ability to certifiably demonstrate that a credential used to access data is positively linked to the individual using the credential itself. Moreover, to be effective, audit systems need the ability to proactively flag unauthorized access.

When bad actors are “in the system” then there can be significant violations of people’s expectations of privacy and confidentiality. The threat of such internal privacy breaches is not novel or theoretical. Despite strict privacy legislation and the existence of logging and auditing functionality, data breaches in hospitals and government institutions regularly occur. In 2011, an Ontario hospital nurse was fired for inappropriately accessing files on almost 6,000 patients over a six-year period.[147] In another recent example, two health authorities in Newfoundland fired or suspended more than a dozen employees for looking up thousands of patient records without authorization. "If somebody with wilful intent is going to break the rules, then it’s pretty hard to stop that," admitted Newfoundland and Labrador Privacy Commissioner Ed Ring.[148]

NFC Chips

Near Field Communication (NFC) is a set of protocols for wireless communication that is gaining popularity across the payment card industry. The primary difference between NFC and previous chips is that it is “contactless”: NFC relies on a communications protocol that uses radio waves to communicate with card readers. Tapping or waving an NFC-chipped card a few centimetres away initiates a small charge that passes between the chip and the reader. This charge activates a data exchange. In the case of the BC Services Card, the reader “will recognize your unique chip and provide your identity information to the service provider”.[149]

Chip-enabled identity documents like the Services Card tend to bolster the perception of privacy. Indeed, the NFC chip embedded within the BC Services Card appears to be central to the government’s security and privacy claims. “Security chips are almost impossible to duplicate,” states a government website promoting the card. “If your card is stolen, the chip can be de-activated to prevent someone else from using it”.[150] It further states that the NFC

147 Wilson, PJ. 2011. Nurse Fired After Breach of Privacy at Hospital. *The North Bay Nugget*, www.nugget.ca/2011/09/06/nurse-fired-after-breach-of-privacy-at-hospital.

148 *CBC News*. 2012. Massive Breach at 2nd Newfoundland Health Authority, www.cbc.ca/news/canada/newfoundland-labrador/story/2012/08/01/nl-western-health-privacy-801.html.

149 Government of British Columbia. nd. *Families & Residents: Privacy & Security*, www2.gov.bc.ca/gov/topic.page?id=F694A0A3880B4499BFAF0FAAE32C5F17.

150 Ibid.

chip does not store any personal information, implying there is nothing of importance to "skim" from the card.

However, the chip's unique ID tag contains the personal account number (PAN) associated with the card/cardholder, an expiry date, a cryptogram and the Application Transaction Counter (a number that records how many times the contactless chip has been used since the last time it synchronized its cryptogram). Because that information is permanently linked to a person's name—which is visible on the card itself along with other biographical data—and is ultimately used to link the card and cardholder to government databases, it constitutes personally identifiable information. As noted, Canadian privacy law holds that "meaningless" numbers like unique identifiers that are associated with individuals' biographic information are considered personal information and as such protected.

Because NFC is increasingly being used for banking and identity authentication purposes there will be more and more motivated attacks against it. The result is that the reader devices—and associated computing environments—used by the BC Services Card infrastructure may also be subject to attack. Further, malicious tags could undermine the security of personally identifiable information stored on NFC-linked mobile or fixed computing systems. Third parties could embed known false NFC chips in the Services Cards to subsequently infect associated computing systems with malware or other attack code. This broader concern with NFC—that it could let third parties compromise computing systems—is troubling in light of the province's formal adoption and advocacy of the technology.

Mobile Migration & Personal Computing

As well as security vulnerabilities associated with card readers, there are concerns related to mobile integration. The Office of the Chief Information Officer is investigating the possibility of using mobile technologies to read the BC Services Card and is currently testing this functionality with a Google Android device.[151] SecureKey's authentication software integrates with consumer-grade NFC-enabled mobile devices and, as mentioned, the company recently partnered with three major Canadian telecommunication companies to put its mobile product on Canadian cellular phones.[152] This report's accompanying technical analysis highlights a number of problems associated with using mobile phones to access government services via the BC Services Card, including opening the phones—and the government network itself—to compromise by malicious or unauthorized third parties.[153]

151 Interview with a representative of the Office of the Chief Information Officer on November 13, 2012.

152 SecureKey. nd. *Strong Authentication*, http://securekey.com/our-solutions/strong-authentication.

153 Parsons and Molnar, 2012.

While BC is testing the functionality of the system on mobile devices, security issues are not receiving the focus they deserve. Security issues require much broader, federal involvement. In essence, the question is: if Canadians are going to be encouraged to access government services on mobile readers, what security conditions must these devices and their associated electronic infrastructure be required to meet? Currently there are no holistic security standards that computing devices must meet before citizens can access government services on personal devices. In light of the recent complaint lodged with the U.S. Federal Trade Commission by the American Civil Liberties Union with respect to Android smartphone security[154] and extensive security problems highlighted by the technology press[155], we need leadership from the federal government in interpreting what minimal legal standards of security are required if governmental services are to be delivered through such channels.

In addition to the vulnerabilities associated with mobile readers, readers built into laptops or attached to desktops should be treated with similar caution. The move to greater online access to government services, significantly facilitated by the BC Services Card, will increase the value of attacking cardholders' computers as yet more sensitive information is made available through these highly insecure computing environments. Even if the cryptographic functions between an NFC-reader, SecureKey, the Office of the Chief Information Officer (Provincial Authorization Application), and particular Ministry databases can be secured, the display medium—the web browser—will remain a leaky and vulnerable piece of software. This has the potential of turning the benefits of single sign on against British Columbians by enabling third party capture (and subsequent use/dissemination) of highly personal information. Moreover, malware with screen capture and data exfiltration capabilities is a common problem in today's PC world and there is no reasonable expectation that such security vulnerabilities will go away in the near future. As late into the planning process as 2012, government officials had concerns that the BC Services Card could be subject to well-known attacks being reported in the popular media. However, in the absence of the government having conducted its own security threat and risk assessment of the card, it turned to SecureKey to prepare a "story" on the credential brokering service's "vulnerability or not...".[156]

154 Wizner, Ben. 2013. *Federal Trade Commission Request for Investigation and Complaint for Injunctive Relief*, www.aclu.org/files/assets/aclu_-_android_ftc_complaint_-_final.pdf.

155 See e.g. Johnston, Casey. 2012. The checkered, slow history of Android handset updates. *Ars Technica*, http://arstechnica.com/gadgets/2012/12/the-checkered-slow-history-of-android-handset-updates/; Lilly, Paul. 2012. Is there anything Google can do to solve the problem of slow Android updates? *Extreme Tech*, www.extremetech.com/computing/131749-is-there-anything-google-can-do-to-solve-the-problem-of-slow-android-updates.

156 FOI Request CTZ-2012-00117, p. 238.

Function Creep

The BC Services Card itself is the result of function creep. As discussed in Chapter 3, ICBC's facial recognition system was initially implemented to meet with American requirements British Columbians to cross land and sea borders into the United States. Since then, and contrary to privacy law, ICBC offered its biometric database to law enforcement in the wake of the 2011 Vancouver Riots. While the Vancouver Police Department did not take up ICBC's offer, BC's Information and Privacy Commissioner launched an investigation and ruled that ICBC could not "lend out" its database.[157] Now other government services want to use the stored biometric templates for purposes other than the reason for which they were initially collected.

The expansion of ICBC's data stores has not gone unnoticed: the Corporation itself has noted function creep-related issues around the dissemination of photographic and tombstone information with other agencies.[158] Function creep is a core aspect of the BC Services Card, with the government calling the layering of additional services onto the card an "obvious next step".[159] As the card is used to gain access to more and more government services, it will be increasingly likely that additional uses will be found for both the card and information associated with cardholders. Further, the change in legislation around data linking and data sharing could increase the number of locations that British Columbians' data is accessed. Moreover, increased amounts of personal information might be collected or created using data mining techniques.

Expansions of the card's scope, including undefined future uses of personal information, could affect people's willingness to use the card to access government services. The reluctance of people to use a service where they lack confidence in the protection of their privacy is well documented. For example, patients are less likely to access critical health care where they cannot be assured of the confidentiality of their sensitive health information, such as sexual history, stored in electronic databases.[160] If citizens are uncertain about whether accessing government services through a Services Card could generate unknown connections and interactions, the response could be limited uptake of the multi-use functionality of the card. Related concerns could arise as other, non-public parties lobby for access to information

---

157 Hui, Stephen. 2011. ICBC Offers Facial-recognition Technology to Vancouver Police's Riot Investigation. *The Georgia Straight*, www.straight.com/article-399779/vancouver/icbc-offers--technology-vancouver-police%E2%80%99s-riot-investigation.

158 ICBC FOI Request F197019.

159 Shaw, Rob. (2012). New CareCards to Combat Fraud. *The Victoria Times Colonist*, www2.canada.com/victoriatimescolonist/news/story.html?id=ab121170-2a70-4acc-9fe0-9cc801fac75a.

160 Vonn, 2009.

linked via the BC Services Card, such as private insurance companies. Given that the government has already changed provincial law to facilitate more expansive information sharing goals, British Columbians might worry that similar legislative amendments could lead to increased sharing between public and private bodies in the future.

9. A National ID Card for Canada?

To fully appreciate the implications of British Columbia's integrated identity and information management (IdIM) "solution", which includes the BC Services Card, it is important to consider the national context. Although plans for a national ID card have not publicly materialized, the push for e-government and digital IdIM "solutions" have continued at the federal level.

The Government of Canada's drive towards a national identity system arguably began with Secure Channel. Secure Channel was a single network for online service delivery with government-wide authentication that represented a shift in thinking about identity management. Specifically, Secure Channel was developed in order to better run the government like "a single giant enterprise".[161] An industry consortium led by Bell Canada designed and operated Secure Channel, whose stated goal was to meet "citizen expectations for client-centric service delivery, security and privacy".[162] Secure Channel was used in conjunction with ePass—"a digital certificate to register with a user ID and password"—that was meant to "ensure confidentiality and security".[163]

While Secure Channel was promoted as secure, a veritable "Fort Knox", computer security experts claimed its public key infrastructure (PKI) made users' personal information vulnerable. In essence, a public key system means that there are two keys to any transaction: a public key that can be shared with anyone and a private key that is retained in confidence by the individual to whom it belongs. Messages can be encrypted by anyone using the public key but only the recipient of the private key can subsequently "unlock" the message. Alternately, an individual can "sign" a message with their private key and the public key can be used to cryptographically verify that a message was signed with the individual's private key. As a result, using a PKI system can both secure a message from being read by an unauthorized third party and also verify that a message was sent by the person who holds the private key.

It is "widely recognized that PKIs are an essential ingredient for secure electronic communications and transactions;"[164] however, they are challenging to implement in a manner that both protects the security and authenticity of communications (encrypts and signs messages) and guarantees anonymity or pseudonymity. These challenges are

161 The Ottawa Citizen. 2007. The Secure Channel Saga. January 23, 2007, www.canada.com/topics/technology/story.html?id=d917e556-f7e7-404d-a8e4-58acb3684029.

162 Chénier, Maurice. 2007. *Secure Channel Services and Long Term Contract*. Ottawa, ON: Public Works and Government Services Canada, p. 5.

163 The Ottawa Citizen, 2007.

164 Brands, 2000, p. 3.

accentuated when all communications and transactions associated with PKI-based transactions can be linked with other personal information. In the case of Secure Channel, it was possible to identify communications with information such as the IP address that was registered when the ePass was issued or by linking the user's name with the "meaningless but unique identifier" (MBUN) that was used in the transaction process.[165] As a result of these technical deficiencies, dossiers or profiles of users' habits, including behaviour, movements, preferences etc., could be developed and automatically linked to the user's identity. The consequence was that, while the communications might be secure they were not anonymous. It is in light of these kinds of challenges that public key cryptographic infrastructures cannot be regarded as a privacy panacea, particularly where external identifying information can be combined with encrypted communications.

Although the idea to get the federal government online via a single, secure high-speed network was suggested as far back as 1999, Secure Channel was plagued by delays, bureaucratic jostling and apparent financial mismanagement by the Treasury Board Secretariat. In 2003, Canada's Auditor-General Sheila Fraser warned that the project would become "an expensive flop" unless the government quickly resolved "technological and management problems".[166] By 2008, Secure Channel was becoming a liability for government, and was described by the media as a "$1 billion boondoggle" and a "technology white elephant".[167] Secure Channel was ultimately scrapped because of rising costs, technological difficulties and departments, including Service Canada and Canada Revenue Agency being reluctant or refusing to use it.[168]

The Birth of a Pan-Canadian Identity System

At the time of Secure Channel's demise, the blueprint for a new national identity system was well underway. This system adopted a decentralized and federated approach that incorporated various departments, agencies and jurisdictions. This meant that instead of Secure Channel's "single channel" of centralized data management, a host of disaggregated systems, databases and information stores could be made accessible without ever creating a centralized database.

---

165 Brands, Stefan. 2007. *Identity Management for Online Government: Challenges and Solutions.* Presentation to Government Technologies Conference and Expo, http://doc.wowgao.com/gtht/2007/presentations/BrandsPPS.pdf.

166 *The Ottawa Citizen*. 2008. Government to Replace $1B online service 'Boondoggle.' October 17, 2008, www.canada.com/ottawacitizen/news/story.html?id=1f99ea2e-3e87-42d9-8f7e-2eb7028d9a41.

167 Ibid.

168 The federal government nevertheless extended the Secure Channel contract an extra two years beyond its original end date of Dec. 30, 2009 according to *Advance Contract Award Notice: Cyber-Authentication. Reference Number 176290. Solicitation Number 9125-09-0002*, www.merx.com. The Secure Channel contract was apparently extended again, until 2013, according to *RFP: Government of Canada Managed Security Service. Reference Number PW-$$XK-100-24691. Solicitation Number 2B0KB-123147/A*, www.merx.com.

In 2006, the Provincial and Territorial Deputy Ministers created a task force to develop "a pan-Canadian strategy, with a plan of action, on identification and authentication in a service delivery context".[169] The Inter-Jurisdictional Identity Management and Authentication (IJIMA) task force, chaired by then-Chief Information Officer of BC Dave Nikolejsin, produced its final report in 2007. Titled *A Pan-Canadian Strategy for Identity Management and Authentication* (IdM&A), it outlined a national vision for an integrated identity system.

This vision encapsulated a longterm goal of "seamless, cross-jurisdictional multi-channel service delivery for all jurisdictions".[170] The pan-Canadian strategy is based on a "joined-up" model of government, which federates or links discrete federal and provincial databases across the country, making disparate data stores available without creating a centralized database. British Columbia appears to be the first province to implement the recommendations of the task force and, as a result, begin to build the infrastructure that could be used to link with federal government and private databases.

Drivers

The IJIMA task force invokes familiar rationales for a national identity system, including "improved service delivery and client engagement through increased accessibility and choice and significant cost reductions."[171] Other drivers, such as combating identity theft and fraud, and improving privacy and information security, also inform the pan-Canadian framework. The final report provides no evidence, however, that "joined-up" government via a federated model can meet these aspirational aims. Indeed, evidence from foreign jurisdictions supports a different conclusion: "The worst example of 'joined-up government' is the United Kingdom" which "has been trying to figure out how to undo years of bureaucratization mismanagement of data collected about citizens. One UK government committee said recently that their system was a 'recipe for rip-off'."[172] In the face of international failures it is imperative that any federated integrated identity program be strongly based on evidence and not on aspirational hopes.

"Barriers" and Challenges

Nevertheless, the pan-Canadian strategy promotes a federated approach to a national identity system that is focused on digital identification and authentication. Unsurprisingly, the

169 Inter-jurisdictional Identity Management and Authentication Task Force. 2007. *A Pan-Canadian Strategy for Identity Management and Authentication: Final Report*, www.cio.gov.bc.ca/local/cio/idim/documents/idma_final_report.pdf.

170 Ibid, p. 59.

171 Ibid, p. 6.

172 BC Civil Liberties Association and BC Freedom of Information and Privacy Association. 2011. *New Bill Means Less Privacy, No Improvement for Ailing FOI Process*, http://bccla.org/news/2011/10/new-bill-means-less-privacy-no-improvement-to-ailing-foi-process.

strategy finds a number of challenges to achieving this goal, including limited expertise and resources, privacy and identity fraud concerns, and insufficient identity assurance processes and providers (identity proofing). Other challenges include the overall technical complexity and novelty of sophisticated identity management and authentication infrastructures. Another obstacle arises from "insufficient data integrity or quality," which is blamed on "the lack of effective linkages within and across jurisdictions for the sharing of identity and vital events information".[173] One of the key recommendations of the IJIMA task force was for "a legislative scan to determine what legislative barriers, if any, exist to sharing identity information".[174] As discussed in Chapter 4, the BC Government amended three Acts to legalize the sharing of identity information for government service provision. These amendments authorized the data linking properties associated with the BC Services Card program. As privacy advocates are quick to point out, however, laws protecting citizens' personal information should not be considered "barriers"; such laws constitute necessary constraints on how governments and the private sector use this information.

Importantly, the pan-Canadian strategy acknowledges that identity management and authentication "has deep implications for privacy" but that it is difficult to reconcile these with competing interests like law enforcement and convenient, efficient service delivery.[175] Due to citizens' legitimate concerns about profiling and tracking, and the lack of available privacy enhancing technologies (PETs), a national strategy should provide citizens "with maximum knowledge of and control over the uses of their identity information".[176] The Pan-Canadian report identifies other key components of alleviating privacy concerns, notably transparency regarding the collection and use of personal information, and limiting the use of identity information to the purposes for which it is collected. It is unclear whether or how much citizens would have control over their own information in the proposed national identity system, nor whether this would address the vulnerabilities that accompany online integrated data sharing systems. While the report points to the dearth of PETs, it concludes that "the industry will essentially build whatever is demanded so if PETs become a requirement of government, industry will respond".[177]

The pan-Canadian strategy highlights the fact that while federal and provincial privacy legislation and policy possess similarities, "there are nevertheless some key differences" that

173 IJIMATF, 2007, 24.

174 Ibid, p 25.

175 Ibid, p. 29.

176 Ibid, p. 32.

177 Ibid, p. 33.

could interfere with the smooth deployment of a national identity scheme.[178] Such differences could create barriers insofar as some government bodies might be unable to share information, either internally or across provincial lines. Additionally, the linking databases across the country to exchange identity data clearly depends "on the reliability and trustworthiness of every single data provider," including provincial and federal ministries, their agents and private contractors.[179] Technological immaturity and cross-system incompatibility comprise a common barrier to interoperability. However, incompatible laws, policies, regulations and standards—including no universal national standard for issuing identity documents, no universally accepted identity proofing standards or processes and no common policy or standard regarding which attributes should be used to identify an individual—are considered potentially larger obstacles.

Identity Principles

Several different sets of identity principles inform the *Pan-Canadian Strategy for IdM&A*, including Cameron's *Laws of Identity*, Cavoukian's *Privacy-embedded Laws of Identity*, and the Treasury Board Secretariat's *Identity Principles.*[180] Cameron, former Architect of Identity for Microsoft, developed his seven laws collaboratively in the blogosphere in an effort to create the (missing) identity layer of the internet.[181] Building on these "technologically-necessary principles of identity management," Ontario Information and Privacy Commissioner Ann Cavoukian crafted a "privacy-embedded" version that mapped "fair information practices over the *7 Laws of Identity* to explicitly extract their privacy-protective features".[182] The Canadian Standards Association created its *Model Code for the Protection of Personal Information (Q830)* based on internationally recognized fair information principles (FIPs). The *Model Code* identifies 10 principles that "balance the privacy rights of individuals and the information requirements of private organizations".[183] These are incorporated into the *Personal Information Protection and Electronic Documents Act (PIPEDA*), the federal privacy law that governs the private sector.

The pan-Canadian strategy identifies the protection of privacy and the "confidentiality, integrity and availability of data"[184] as among the most contentious issues facing the

178 IJIMATF, 2007, p. 36.

179 Ibid, 39.

180 Treasury Board of Canada Secretariat. 2011. *Federating Identity Management in the Government of Canada: A Backgrounder.* Ottawa, ON: Government of Canada, www.tbs-sct.gc.ca/sim-gsi/docs/2011/fimgc-fgigc/fimgc-fgigc04-eng.asp#Toc232927513.

181 Cameron, Kim. 2005. *The Laws of Identity*, www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf.

182 Cavoukian, Ann. 2009. *Privacy By Design*. Toronto, ON: Office of the Information and Privacy Commissioner, Ontario, p. 232.

183 CSA Group. nd. *Privacy Code*, www.csa.ca/cm/ca/en/privacy-code.

184 IJIMATF, 2007, p. 93.

development of a national identity system. “Very strong measures are necessary to ensure that privacy is safeguarded, that confidential business and government information is protected”.[185] It endorses eight identity principles based on the above standards.

1. *Justifiable and Proportionate*

    - The collection, use, retention and disclosure of identity information must be authorized by legislation or policy and be done only when a clear need is demonstrated. The IdM&A process should follow a risk-based approach, considering both external and internal threats to security and privacy of identity information. Finally, the process should reflect the assessed risk, and be proportional to the goals of the program or service, using “the least intrusive method for identification and authentication”.[186]

2. *Client Choice, Consent and Control (User-centric)*

    - Citizens should be able to choose from a variety of service delivery channels (e.g. in person, by telephone or online). The IdM&A process “should only collect, use and disclose identity information with a person’s knowledge and consent,” which should be informed, non-coerced and revocable. People should be empowered to “control to the extent possible their own identity credentials and the transfer of their own identity information between identity providers and service providers”.[187]

3. *Limited Information for a Limited Use (Data minimization) Limited Information for a Limited Use (Data minimization)*

    - A national identity system should “collect, use, retain and disclose the least amount of identity information possible, on a ‘need to know’ basis”. It should limit use of identity information to the stated purpose, with access to such sensitive information restricted to those who have “a necessary and justifiable place in the service delivery transaction”.[188]

---

185 IJIMATF, 2007, p.93.

186 Ibid, p. 72.

187 Ibid.

188 Ibid, p. 73.

4. *Client Focused, Consistent Experience*

    - "Clients should figure prominently in any identity management and authentication process and be integrated and empowered through intuitive processes that respect and address client needs and capacity".[189]

5. *Diversity of Identity Contexts and Systems*

    - The different identities that people simultaneously occupy within and across jurisdictions, such as citizen, employee and employer must be recognized. Further, an identity system should comprise multiple identity systems run by multiple identity providers.

6. *A Trusted and Secure Environment*

    - Citizens should have a mechanism for authenticating service providers, especially when accessing services remotely. Moreover, there should be auditing processes that facilitate rapid detection and response to data breaches. Government agencies should take "every reasonable step" to ensure the accuracy of citizens' personal information. This principle does not go as far as to facilitate people accessing, amending or challenging the accuracy of their information, which is a standard FIP.[190]

7. *Transparency and Accountability*

    - The IdM&A process should be open, transparent and understandable.

8. *Enduring Solution*

    - The IdM&A process should be flexible, modular, technologically neutral and scalable in a way that it can easily accommodate the addition of clients or any other party (jurisdictions, departments, service providers, etc.).[191]

These identity principles are comprehensive but it remains to be seen how effectively they would be applied in the implementation of a national identity system. Perhaps tellingly, these principles are whittled from eight to four in a follow up policy document to *A Pan-Canadian Strategy for Identity and Authentication Management,* entitled *Pan-Canadian Assurance Model*. To date, information released by the BC Government does not indicate that identity principles factored prominently, or even at all, in the development of the BC Services Card.

189 IJIMATF, 2007, p. 73.

190 Ibid, p. 74.

191 Ibid, p. 75.

Privacy and Security

The pan-Canadian strategy for IdM&A acknowledges that "privacy is better built-in than bolted on. Privacy enhancing technologies are most effective when integrated in the design stage".[192] It also highlights notification and consent requirements (Principle 2) as critical to the protection of privacy. Although individuals do not typically have to consent to public bodies collecting their personal information, this reality "is likely to become more of an issue as organizations move towards providing cross-jurisdictional seamless services".[193] This issue arises because, although many government organizations can collect identity information without consent to provide mandated services, they do not necessarily have the authority to share that identity information with other organizations, especially in other jurisdictions, without client consent. As well, because any private sector partners are obligated under *PIPEDA* to obtain client consent to collect and use client information, obtaining consent might be necessary in a federated national identity system.

The *Pan-Canadian Strategy for Identity Management and Authentication* understands data-minimization and the proportionate use of identity information as key to protecting privacy; that is, collecting only what is authorized, as well as needed, and using it only for the purpose stated (Principles 1 and 3). Such data minimization helps prevent function creep by limiting the identity program or process to its original intention. While many aspects of fair information and identity principles are reflected in privacy law, when these are regarded as barriers the policy response is often simply to amend existing legislation or create new laws. As discussed in Chapter 4, British Columbia engineered successful workarounds of "legislative barriers" when rolling out Government 2.0 by passing the *e-Health Act*, and by amending the *Freedom of Information and Protection of Privacy Act*, the *Medical Services Act* and the *Motor Vehicle Act*. Taken together, these changes have let the province more broadly share and link BC residents' personal information across government bodies.

The security component of the pan-Canadian framework draws upon Principle 6 in calling for the creation of "an environment that engenders trust".[194] Essential to this are security threat and risk assessments (STRA) that "must be regularly conducted to identify general business and security risks, to determine the adequacy of security controls...and to mitigate those risks".[195] In BC, the Office of the Chief Information Officer, which is responsible for

192 IJIMATF, 2007, p. 92.

193 Ibid, 2007, p. 86.

194 Ibid, 2007, p. 92.

195 Ibid, 2007, p. 94.

the technical design and implementation of the Services Card, did not conduct a STRA of launching the card and its associated infrastructure.

The authors of the pan-Canadian strategy recommend and identify several pilot projects to begin addressing the "barriers" and verify the applicability of the IdM&A framework and principles. "Early pilots will involve inter-jurisdictional initiatives that lay the foundation for bundled transactions requiring authentication; and implement, and report on, a range of new business processes involving data sharing, and shared or leveraged identity-proofing and authentication processes".[196] Among these was a partnership between British Columbia's electronic identification credentialing program, BCeID, and the federal government's online authentication process. The intent of the pilot was to "test the concept of one jurisdiction (BC) leveraging the identity-proofing process of another jurisdiction (Canada Revenue Agency)".[197] The partnership allowed British Columbians to use their federal Business Number to identify their company when communicating with the province. The project appears to be ongoing, although its success or otherwise is unknown. Nevertheless, this project demonstrates that BC's involvement in developing a national identity system is not limited to authoring policy documents: the province was also involved in early testing of the potential ways that provincial jurisdictions could participate in an interoperable national identity infrastructure.

Cyber-Authentication Renewal Project

The pursuit of a national identity system based on federated identity management and authentication continued with the Cyber-Authentication Renewal Project. The Government of Canada launched this project in 2008, the same year that it abandoned Secure Channel. Described as "a federal interdepartmental initiative that defines a new approach to authentication", it followed on the heels of the *Pan-Canadian Strategy for Identity Management and Authentication*.[198] The goal of the initiative is to "articulate a vision and develop a strategy to move toward a standards-based federated architecture that would allow for the use of other credentials external to government".[199] The government of Canada's approach to identity management now favours a federated multi-channel network with authentication provided by a private credential broker service instead of the (failed) single channel network approach of Secure Channel.

---

196 IJIMATF, 2007, p. 44.

197 Ibid, p. 150.

198 *LOI: Credential and Authentication Services*. Reference Number PW-$$XK-102-18053. Solicitation Number EN869-090305/A, www.merx.com.

199 Treasury Board of Canada Secretariat. nd. *Guideline on Defining Authentication Requirements*, www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26262&section=text.

The Treasury Board Secretariat (TBS) has played an important role in the Cyber-Authentication Renewal initiative.[200] The TBS is a federal body that "establishes and oversees a whole-of-government approach to security and identity management".[201] It developed a guide for creating "seamless and coordinated service delivery across jurisdictions" that built on the *Pan-Canadian Strategy for IdM&A.*[202] The guide, titled *Federating Identity Management in the Government of Canada: A Backgrounder* recommends a federated approach to identity assurance as well as authentication.[203] Significantly, it makes no mention of the pan-Canadian identity principles. Instead, the principles that inform the "federation model for identity management" refer to "consensus," "responsibility," "interoperability" and a "competitive marketplace". The only principle that bears a resemblance to anything in the pan-Canadian framework is the one referring to client choice concerning which identity credentials to use to access government services. The backgrounder underscores the potential of a pan-Canadian approach to bridge departmental, agency and jurisdictional boundaries. Significantly, it goes beyond national federation, highlighting the importance of "ensuring that Canada's approach aligns with those in other countries to support the business of government that extends beyond sovereign borders".[204]

Although there appears to have been little public consultation, the Cyber-Authentication Renewal initiative consulted closely with industry, with "a new cost-effective online authentication solution" the clear objective.[205] As promised, by December 2010, the federal government rolled out a lower cost credential service to replace the ePass across government departments and services. The replacement, Access Key, was described as an "efficient and flexible authentication solution" that would not compromise "the security of services and the protection of personal information". Only two years later, however, Access Key was phased out, replaced by "GC Key," a government-issued credential service. The $29 million contract for GC Key, awarded to information security firm 2Keys, was the result of the Cyber-Authentication Renewal Project's ongoing effort to find a replacement for Canada's "current online authentication services".[206]

---

200 Treasury Board of Canada Secretariat. 2012. *Policy on Government Security*. Ottawa, ON: Government of Canada, www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578&section=text.

201 Ibid.

202 Treasury Board of Canada Secretariat, 2011.

203 Ibid.

204 Ibid.

205 *NPP: Credential Broker Service*. Reference Number PW-$$XK-101-21556. Solicitation Number EN869-110512/A. Retrieved from www.merx.com

206 *Government of Canada Branded Credential Service*. Reference Number PW-$$XK-103-22095. Solicitation Number EN869-111909/B, www.merx.com.

Private Vendor Credential Brokering

The Government of Canada also sought a commercial "credential broker service" as part of its evolving approach to identity management and authentication. Within a federated identity system, a credential broker acts as a third party that authenticates requests from relying parties (e.g. government departments or service providers) by accessing approved identity credentials from authorizing parties (e.g. banking credential issuers). The Government of Canada awarded a $41 million contract for this service in 2011 to the sole bidder, SecureKey Technologies.[207] SecureKey describes itself as a "secure, cloud-based 'hub' that eliminates password fatigue and makes the sign-in process quick and painless for end users".[208] It facilitates a "single sign on" experience by leveraging existing banking credentials to authenticate users across a range of services. SecureKey's first product, Concierge, launched in smaller federal government departments in April 2012, with the pledge of more than 80 government services from 18 departments available by the end of that year.[209] By March 2013, however, Concierge disappeared from SecureKey's service offerings, apparently replaced by a next generation, mobile ready product called Briidge.

SecureKey promises a triple-blind user experience. Under this authentication paradigm,

> No one participant has a complete picture of the transaction. Each bank produces an anonymous MBUN [meaningless but unique identifier] for each customer. The banks will pass the MBUN to [SecureKey Concierge] during authentication. Our service will log any transactions completed in the session against the MBUN. To preserve anonymity between services SKC will further anonymize the MBUN for each relying party service and SKC will pass a unique number called the Persistent Anonymous Identifier to each RP".[210]

In other words, the bank does not see what government service is being accessed, the government does not see the bank or the user's banking information, and SecureKey does not see the user's identity.

As SecureKey acknowledges, however, this is strictly a "privacy veil" kept in place through access controls. As the credential broker, it has the technical capacity to link users to their MBUN and PAI and thus trace their activities through the system. This privacy veil does not and cannot defend against bad actors or internal abuse. Canadian Privacy Commissioner

---

207 Knowles Consultancy Services Inc. and Hill International Inc. 2011. Cyber Authentication Renewal Program Request for Proposal 2 (RFP2), www.tpsgc-pwgsc.gc.ca/se-fm/aou-aug-1611b-eng.html.

208 SecureKey Technologies. nd. *Our Solutions*, http://securekey.com/our-solutions/credential-brokerage-service-cbs.

209 SecureKey. 2012.

210 Code Technology, 2012.

Jennifer Stoddart raised concerns regarding "the levels of authentication offered in the service and possible issues of accountability gaps if privacy breaches were to occur".[211] In her 2011/2012 annual report, she also noted that while her office worked closely with the federal government agencies involved with bringing SecureKey Concierge online—Shared Services, Treasury Board Secretariat and Public Works and Government Services Canada—the privacy impact assessment (PIA) submitted for the credential broker service was "lacking in required documentation".[212] However, it is the privacy veil, or the "triple blind lite" approach to privacy, which only exacerbates the problems associated with a federated approach to identity, to which we now turn.

The Trouble with Federated Authentication

The central problem with the Government of Canada's federated authentication system is that it is fundamentally unfit for purpose outside of enterprise scenarios. In short, the system is technically unable to preserve Canadians' privacy or the security of the system architecture more generally. In what follows we briefly outline these failings by focusing on impersonation capabilities inherent to the federated model, the potential for using this model for surveillance, and how the model could facilitate governmental function creep.

When federated authentication models are used in enterprise scenarios there is a central server responsible for much of the identity credential handling. Given the nature of enterprise environments, this server is typically controlled by the user's employer and is responsible for logging the user into the employer's resources. The potential to "masquerade" as the user—and thus gain access to resources in the user's name—could be useful to understand what resources the employee is accessing and when. Alternately, this might be done so that one employee who is just "filling in" for another could continue to access the resources needed to temporarily assume a role in the business. Though these kinds of masquerading capabilities make sense in an enterprise scenario they are inappropriate in an identity model used for state governance. In these situations, access to personalized citizen resources (e.g. tax information, medical records, child support information) could compromise the security, privacy, or confidentiality of a person's engagement with government. Consequently, it is imperative that such impersonation cannot happen in government systems.

In effect, the challenge with federated authentication models is that they do not necessarily preclude centralized surveillance, nor do they necessarily prohibit impersonation powers. At best such models distribute these powers among multiple parties. Thus, in order to effectively

211 Stoddart, Jennifer. 2012. *Annual Report 2011-2112 on the Privacy Act.* Ottawa, ON: Office of the Privacy Commissioner of Canada, www.priv.gc.ca/information/ar/201112/201112_pa_e.asp.

212 Ibid.

masquerade an internal attacker would need to control the centralized identity broker and, potentially, parties that provide assurance that whomever is accessing the government services is authorized to do so. As an example, an attacker might need to compromise an element of SecureKey's network (which acts as a central party to the federal government's federated system) and the banks that provide identity assurance (e.g. to prove that the person accessing government services is who they say they are). This latter party might need to collaborate if its assurance processes apply characteristics of the person in question that are derived from their banking engagements, such as what web browser they use, what geographic area(s) they tend to access bank services from, what operating system(s) they use, and so forth. Thus if someone tries to masquerade and lacks these characteristics—which could prevent the bank from providing identity assurance—the bank might need to collaborate with SecureKey to bypass these assurance checks.

While parties may genuinely be committed to respecting and adhering to Canadian privacy laws and the laws prohibiting linking data between actors in the authentication process, a malicious actor could theoretically bridge data sources by compromising the network, an employee, or any other system or process that grants the actor trusted insider status. The implication of this potentiality is that despite the pro-privacy intentions of pan-Canadian federated identity management and authentication, the system undergirding this approach could facilitate surveillance and impersonation powers. In light of these potentials, and decades of basic lessons in computer security, it is imperative that distributed large-scale environments actively avoid the possibility of such collaboration. This is because while the federated system is not logically centralized, it functionally has the potential to behave as a centralized system and, as a result, is capable of mass citizen surveillance.

Another serious problem with federated authentication relates to service access. Specifically, Canadians will not be able to authenticate to government services – and thus receive the requested service – if any of the central/ intermediating parties are offline (because of a denial-of-service attack, a power interruption, or a server crash, for example) or simply refuse to vouch for you (or does so in a faulty manner). The consequence of such disruptions would be to instantaneously deny users access to services they may want to access. Yet another, separate, issue is that once a Canada-wide federated authentication system is in place it could subsequently be used to conduct data sharing across services. Indeed, this is where by far the most "value" will potentially be unlocked for government service providers, citizens, and businesses alike. Such expansions of service—function creep—of the federated system will be accompanied by all of the previously noted privacy, security (vis-à-vis insiders and viruses that can assume insider powers), and availability problems.[213]

213 Email communication with Dr. Stefan Brands, January 19, 2013.

From Identity Authentication to Identity Assurance

Although there has been no public mention of a national ID card for Canada, the federal government has maintained a clear and an ongoing objective of creating an integrated multi-jurisdictional identity system. As the foregoing discussion demonstrates, this objective is grounded by several high level policy documents, especially the *Pan-Canadian Strategy on Identity Management and Authentication*, and propelled by the Cyber-Authentication Renewal initiative.

A federated identity management framework continues to evolve under the direction of the Pan-Canadian Identity Management Steering Committee (IMSC), a group established by the Federal-Provincial-Territorial Deputy Ministers' Table on Service Delivery.[214] In 2010, as part of this work, the IMSC crafted an identity assurance model that was described as "the first step in the long road" toward a national identity system that will facilitate "maximum interoper-ability" between the federal government and the provinces.[215]

The *Pan-Canadian Assurance Model* is meant to let different jurisdictions trust "one another's assurances of identity and credentials as part of a federated arrangement".[216] Identity assurance is the level of confidence that a person is who they claim to be, and relates to the process of establishing a person's real identity. Credential assurance is the level of confidence that an identity credential is under the control of the person to whom it belongs, and has not been tampered with or modified; it relates to the process of binding an identity credential to a unique individual. Consistent with other government documents on identity management, this one anticipates the need to change existing laws in order to accommodate an integrated, federated approach.[217] The IMSC released a draft report in 2011 that outlines how to trust cross-jurisdictional identities in both the public and private sectors.[218] Federated identity is identified as key to achieving this ultimate objective.

The *Pan-Canadian Assurance Model* draft report only retains four of the eight guiding principles set out in the 2007 *Pan-Canadian Strategy for Identity Management and Authentication*. Once inspired by commonly accepted identity principals and fair information practices, the principles that now guide the development of Canada's identity system include:

---

214 Treasury Board Secretariat of Canada, 2011.

215 Identity, Assurance and Trust Working Group, Identity Management Steering Committee. 2010. *Pan-Canadian Assurance Model*, p. 4.

216 Ibid.

217 Ibid.

218 Pan-Canadian Identity Management Steering Committee. 2011. *Trusting Identities: The IMSC Pan-Canadian approach to enabling better services for Canadians*, p. 2, www.iccs-isac.org/en/km/transformative/docs/IMSC%20Paper_Trusting%20Identities%20Consultation%20Draft_EN.pdf.

1. Interoperable, cost-effective and innovative
2. Easy to use, client-focused and voluntary
3. Safe, secure and privacy-enhancing
4. Accountable and transparent.

There is little exposition or discussion of these principles. The newly refined national identity system takes only a cursory approach to the critical aspects of security and privacy. This is worrisome because it suggests these components of an identity system are less of a priority than other aspects, when in fact they should be foundational. Regarding Principle 4, however, the report does note that "trusted identities should be subject to clear governance, with governments accountable and transparent with respect to activities involving identity".[219] Thus far, however, the policy development process for a national identity system has been conducted behind closed doors with little, if any, input from Canadians and no clear mechanism for holding the government to account.

There are a number of follow-up documents that support the policy direction taken in the *Pan-Canadian Assurance Model* draft report. For example, the Treasury Board Secretariat's *Guideline on Defining Authentication Requirements* supports the implementation of the assurance model. The *Guideline* affirms separating identity from credentials as a key element of the Cyber-Authentication Renewal initiative.[220] The severing of identity from credential is meant to let government departments rely upon credentials issued by other departments or organizations, including banks, even though the identity of the person presenting the credential may be unknown. The guideline expresses the mandatory nature of cyber-authentication services for government service providers. This means federal government online service offerings must use either the private credential broker service (SecureKey) and or GC Key (the government credential service).

The *Guideline on Defining Authentication Requirements* supports the Treasury Board Secretariat's *Directive on Identity.* The directive pursues identity management practices that are "aligned with an integrated government-wide approach" and that "allow for interoperability, when appropriate, which enables the exchange of individuals' identity information".[221] It is the "first time within the Government of Canada that there will be a

219 Pan-Canadian Identity Management Steering Committee, 2011, p. 3.

220 Treasury Board of Canada Secretariat. nd. *Guideline on Defining Authentication Requirements.* Ottawa, ON: Government of Canada, www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26262&section=text.

221 Treasury Board of Canada Secretariat. 2009. *Directive on Identity Management.* Ottawa, ON: Government of Canada, www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16577&section=text#cha3.

policy instrument to ensure coherent identity management practices".[222] The recently published *Standard on Identity Credential and Assurance*, the latest rendition of the pan-Canadian assurance model, also dovetails with the *Directive on Identity Management* and supports the goal of government-wide identity federation.[223]

There are efforts underway at the federal level to establish a working framework for a national identity system, as the foregoing overview of high level policy documents indicates. These key policies do not preclude, and indeed appear to support establishing the conditions for an associated identity card. The implementation of a technically interoperable provincial ID card—the BC Services Card—suggests that the national identity system is being planned to support the inclusion of ID cards, and that such provincial cards will serve as a de facto national ID card.

The "Card Cartel"

Based on the years of policy initiatives reviewed in this report, it appears the Government of Canada is currently committed to a federated approach to digital identity management across federal and eventually provincial departments. The Identity Management Steering Committee (IMSC) is careful to state that a "trust-based and decentralized approach...does not include a national ID card scheme, a national identifier or a centralized identity database".[222] But as David Lyon, one of Canada's preeminent scholars on privacy, identity and surveillance, observes, "today's 'new' ID cards are ID *systems* based on the use of networked, searchable databases".[225] The continually evolving pan-Canadian framework for integrated identity management, authentication and assurance plainly outlines a national identity system designed to interoperate with all levels of government, and capable of including an ID card. This system is intended to accommodate identity cards that may be provincially issued but that function across all government bodies– in other words, a de facto national identity card. As previously noted, the absence of a centralized identity database does not alleviate associated concerns, such as citizen profiling, state surveillance or the potential for insider abuse and external attacks. In the context of British Columbia, it appears as if the BC Services Card will be able to interoperate with the federal system. Thus it is the first (proto-) pan-Canadian identity card.

---

222 Ibid.

223 Treasury Board Secretariat of Canada. 2013. *Standard on Identity and Credential Assurance*. Ottawa, ON: Government of Canada, www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26776&section=text.

224 Ibid, p. 7.

225 Lyon, 2009, p. 7.

If the federal government publicly hedges its desire for an ID card based system, the key vendor associated with the project is not so reticent. SecureKey Technologies envisions a "pan-Canadian public-private digital identity and authentication regime" that includes the provinces and looks beyond the banking industry to provide credential authentication to the telecommunication sector.[226] SecureKey has been forthright about its aspiration to enrol all the provinces, with the stated goal of "wrapping up" the rest of Canada. Perhaps most telling is the company's desire to name the BC Services Card the SecureKey Card. Regarding the data field in the card required for the personalization profile, a senior SecureKey official wrote:

1. Calling it the SecureKey Card will allow us, to the extent all the provinces (and other jurisdictions), sign up for this service, SK will be able to treat all the traffic as aggregated and get better pricing and routing if we go this route. As we are acting as the issuer for the card under the covers this seems a sensible approach.

2. Calling it the BC Service Card [sic] is an option, but makes it harder to aggregate traffic (because now we have to parse for every possible jurisdiction to know if the card app is one we know or not).[227]

As previously noted, the province directly awarded SecureKey the $20 million contract for the BC Services Card. SecureKey has been closely involved in the planning process, working with members of the provincial government and other vendor partners to establish the infrastructure needed for the card to "work" for service delivery. In the course of designing and developing the Services Card and its technical infrastructure there has been no meaningful public consultation or external evaluation or testing of the government's plan. Instead there have been close relationships among a group of elites intent on deploying the card. It is this set of characteristics—close government/vendor relations and the absence of public input—that constitutes a "card cartel".[228] Card cartels are "oligopolies of official identification" composed of governments, corporations and technology. As the product of a corporate-driven, technocratic approach to identification, card cartels alter what it means to be a citizen by conferring authority to determine and regulate identity to corporate mandates and technology protocols. Thus "it is not merely that governments are outsourcing some

226 SecureKey Technologies Inc. 2012. *Consultation Submission from SecureKey Technologies Inc. in response to Strengthening Canada's Anti-Money Laundering and Anti-Terrorist Regime*, www.fin.gc.ca/consultresp/pdf-pcmltfa-lrpcfat/023-SecureKey-eng.pdf.

227 FOI Request CTZ-2012-00117, p. 47.

228 Lyon, 2009.

services, delegating some tasks to external agencies, but that those agencies—corporations and technologies—help to define and constitute the systems themselves".[229]

British Columbia appears to be the first provincial "member" of the cartel to link in to the pan-Canadian identity framework, embracing the nationwide vision for an integrated, multi-jurisdictional identity system. This is no mere conjecture: the province has stated that its new identity card must "work with, interoperate with and [be] compatible with the federal identity system".[230] While government officials have denied any connection, it is clear that the BC Services Card is aligned with the evolving national ID program.

Federal and Provincial Privacy Commissioners

Provincial identity systems meant to integrate into a national ID system present particular challenges for federal and provincial privacy commissioners. Happily, Canadian federal and provincial privacy commissioners have a history of working collaboratively. As with the multi-jurisdictional issues raised by Enhanced Driver's Licenses, provincial ID systems are projects that fall under provincial jurisdiction, while simultaneously possessing aspects that also fall under federal jurisdiction. In the case of provincial ID systems, the federal aspects include any integrated uses for the purposes of federal government programs, as well as private sector uses of the technology that are governed by PIPEDA. Thus, it is clear that as with EDLs, provincial jurisdiction can be respected while the Office of the Privacy Commissioner of Canada attends to the file from the perspective of the federal role, working collaboratively with provincial commissioners as needed.

Commissioners' previous cooperation with respect to EDLs provides a blueprint for collaboratively addressing provincial ID cards. Like the EDLs, there will be mutual interest in the underlying technological architecture as well as the collection, retention, sharing, transmission, and use of Canadian citizens' personal information. If anything, collaborative work on the integrated identity system is more urgent than the work on the EDLs, on the basis that the new identity cards will be mandatory documents and because these cards will have important ramifications for both the private and public sector. The involvement of the private sector, particularly the banking and payment card industries, is now well beyond the planning and consultation stages. This is vividly illustrated by the roll-out of a new payment system for public transportation in the Lower Mainland of British Columbia. The new system, called the

229 Lyon, 2009, p. 80.

230 Minister of Labour, Citizens' Services and Open Government and Insurance Corporation of British Columbia. 2012. *Notice of Intent #SATP-290*.

Compass Card, is a fare payment card that stores value for fare payment. This system for a new transit 'smart card', which can be 'loaded' with value for fare payment through purchase by cash, major credit card or debit card, will be available for loading online,[231] with the current plan to leverage the BC Services Card for the online service interaction. As set out by the BC Ministry of Transportation and Infrastructure, "TRAN has prepared a plan for leveraging Shared Service BC identity management services and synching with plans for programs
within the ministry's accountability, including the Translink Compass Card."[232] The operationalization of the identity management framework for use by both the public and private sector is currently underway and, as such, it is imperative that Canada's privacy commissioners prioritize this file at the outset, rather than terminus, of the ID card's deployment.

As the OPC has noted in the past, provincial commissioners are autonomous. However, when provincial initiatives can potentially affect other jurisdictions, there is much to be gained from all of Canada's commissioners working together. Given that the provincial identity systems are designed to be components of a national federated system, it is not only obvious that the privacy commissioners of Canada need to work together, but that media coverage of issued reports, consensus statements, joint resolutions and the like are one of the few ways that Canadian citizens are apt to become informed about these developments. As noted, federal and provincial government initiatives in this field have been at best obscure and at worst deliberately opaque from the public. In addition to bringing their expertise and influence to the matter, Canada's privacy commissioners should exercise their education mandate to raise the issue of the interwoven provincial and federal identity systems to Canadian public.

231 Transklink Compass Card FAQS www.translink.ca/en/Fares-and-Passes/Compass-Card/FAQS.aspx.

232 British Columbia Ministry of Transportation and Infrastructure, 2013. Transformation and Technology Plan 2012/13 – 2014/15, p. 49 http://docs.openinfo.gov.bc.ca/D3599512A_Response_Package_TRA-2011-00290.PDF.

10. Alternatives

This report has identified potential security and privacy vulnerabilities associated with the datalinking architecture that underpins the BC Services Card, and with the physical card itself. Perhaps more significantly, however, it has identified how the Services Card and the federal infrastructure would support a pan-Canadian identity system that has been developed largely without public input or analysis. In what follows, we suggest alternatives to the existing plans and publicly stated proposals. We operate under the assumption that the current infrastructure is not carved in stone, and that public officials are interested in avoiding the worst of possible consequences related to the BC Services Card. To this end, we outline a process—and technical architecture—that could be used to confer legitimacy on any identity card project in the province while also serving to limit risks associated with bad actors or subsequent "de-anonymizing" processes that could reduce confidence in the card. To be clear: our proposals do not outline specific *security* solutions beyond modifying the relationship(s) between actors to an identity process. The modified relationships are intended to impose a genuine, privacy-by-design blueprint on an architecture that, at the moment, largely guarantees privacy-by-policy.

Considering the User

SecureKey's present system offers a kind of "triple-blind-lite" identity architecture: its "privacy veil" utilizes policy controls and presumes there are no bad actors or changes in technical behaviour to protect privacy. A stronger approach to protecting the privacy of citizens would adopt a genuine triple-blind system whereby it would be technically infeasible—regardless of legislative or policy change—to conduct mass surveillance using the identity infrastructure. For this reason, we suggest that the government should adopt a user-centric model.

The *Pan-Canadian Strategy for Identity Management and Authentication* describes the user-centric model as turning "traditional identity management and authentication models on their head, by putting users, rather than identity and service providers, in the centre of the transaction".[233] The authors of the pan-Canadian strategy call it a "likely trajectory for future identity-dependent web services" because in the long term, "internet users will begin to expect governments to be part of such services".[234] In effect, by putting users in control of their own data the government and other third-parties are largely taken "out" of the flows of

233 IJIMATF, 2007, p. 175.

234 Ibid.

data. This means that there is less likelihood for sustained collaboration between bad actors, and that (if implemented properly) it would be challenging for *any* third parties to create data portfolios or monitor citizens' interactions with government.

In what follows we outline how this system would work at a high level, and why it meets identification and authentication requirements. We then conclude this section by discussing its merits relative to provincial cards that serve as the basis for a federated national ID system.

What is a User-Centric Approach?

Sometimes referred to as "Identity 2.0," a user-centric approach to digital identity management lets users manage and share their identity information using an "identity agent". An identity agent stores credentials that identify a person to a service. Users obtain identity credentials from authorizing parties (APs) and associate these with their identity agent. So, as an example, before a user could access PharmaCare, she would obtain the necessary credential and store it with the agent that was on her home computer. When service providers (relying parties/RPs) request proof of identity or identity attributes, users can then present the appropriate identity credential. Disclosure of one's information might require a password or some kind of physical token (like a smartcard). Regardless of the method, another factor of authentication could be established so that if a user's computer was stolen, or smartphone lost, it would not be possible for someone else to access her health, school, or tax information by logging into her computer or phone. What distinguishes the user-centric model from the current BC model is that, as mentioned, the user remains at the centre of the data transaction and in control of her personal information. "The data always flows through the client's identity agent and, as such, the client is able to release information only as she sees fit".[235]

While it might seem fanciful to adapt BC's identity infrastructure to this new model the government can still adjust its course in spite of the sunk costs associated with the BC Services Card: according to the *Pan-Canadian Strategy for IdM&A* it is easy to extend the user-centric approach to a federated model. So, while BC is presently moving towards a semi-federated system (insofar as it depends on government 'federates' instead of the private federated parties as in the federal scheme) it can still "fit" within a more privacy protective model.

A User-Centric Approach Meets Identity Requirements

A user-centric model can satisfy many of the goals of most identity systems while minimally jeopardizing the privacy and security of citizens' sensitive personal information. In what

235 IJIMATF, 2007, p. 175.

follows we outline the parties that would be involved in such an approach and how data and control of information would flow.

The parties involved in a user-centric model include:

- The BC resident and his identity agent;
- The Service Provider the resident is accessing;
- An Identity Service Provider (IdSP) that is trusted by all parties, and which issues claims and identity tokens to validate user requests;
- A privacy broker, which takes the IdSP's identity token and converts the tokens into one of the broker's own, thus limiting collusion between the Service provider and the Identity provider.

Significantly, there are three discrete relationships in the identity transaction: between the resident and the service provider; between the resident and the identity service provider, and between the resident and the privacy broker. As long as the "regular" provincial service provider, such as the Ministry of Health, trusts the token(s) issued by the privacy broker it can dispense services without the broker or IdSP being able to link specific individuals with requests for service or the subsequent provision of service.

The data flow in a user-centric model might be as follows:

1. The cardholder wants to access a service online using her BC Services Card. She is redirected from the service provider's (relying party/RP) website to an Identity Service Provider (IdSP), with some notice of the kinds of access requirements that must be met before the service can be disclosed.
2. After arriving at the IdSP's website, she is prompted to present her card (waving it in front of a reader inserted into her computer) and enter her PIN associated with the card.
3. The IdSP then validates her identity.
4. After validating her identity, the IdSP generates an identity token with the claims or user attributes associated with the individual—for example, that the cardholder is authorized to receive health services. The token is sent to a privacy broker.
5. The privacy broker validates the identity token from the IdSP and exchanges it for one of its own. The broker's token has all the same claims/attributes as the IdSP's token.
6. The identity token is retained in the citizen's identity agent and, subsequently, released to the provincial service (RP) as appropriate.

The result of this identity token shell game is that the government service, the identity service, and the privacy broker are all blind to the full attributes of the person making a service request (e.g. that she is over 18; that she receives social benefits, that she is eligible for health services). This matters because in the absence of this "game" the government party and the IdSP (e.g. the Office of the Chief Information Officer and corporate partner hired by the province as an identity broker) could collude to trace the entirety of a citizen's interactions with government. As it stands, this shell game approach has not been adopted for the BC Services Card's identity management system and, as such, citizens cannot be assured that the system will never be used for mass surveillance.

The user-centric approach could encompass a series of identity service providers and a host of privacy brokers to create a scalable federated system. Thus there are no absolute requirements for a *single* or *mandatory* IdSP or broker. This means that both IdSPs and privacy brokers could "compete" on grounds of best service, security, or other features. Individuals could "shop around" for the best service or simply rotate through these parties to minimize any one group knowing too much about their engagements with government. Or they could choose one IdSP and one privacy broker and stick with them: the individual would be able to make the decision. The BC Services Card program offers citizens no such choice.

The overall result of the above-proposed model is assurance for provincial services that the ID document in question is likely authentic, and that the person who owns the document is the one making the service request (as guaranteed by using the PIN). Moreover, the user can better protect his anonymity insofar as he reveals only the information that is required to receive the service requested. Neither the IdSP nor the privacy broker necessarily know what *specific* service the user wants to access, what attributes or identity claims he provides to get it, nor whether he ever uses the issued identity tokens to receive the service. Even in the event of collusion between privacy brokers and the online government service being accessed (e.g. MoH), there is no way to connect the cardholder's true identity to the service used: the broker is merely providing authentication via the identity token based on attributes (from the IdSP) that might vary each time a service is accessed. Consequently, an identity system can be crafted wherein the privacy broker cannot develop an intimate understanding of who has come to it to exchange tokens over time. Importantly, this model is scalable because the IdSP does not need to establish a relationship with or know anything about the service provider.

The Comparative Merits of the User-Centric Model

The identity-based issues tied to how the BC Services Card is currently deployed relate to re-identification of claims requests. If citizens believe that previously discrete engagements with the government can readily be linked and tracked from a central location then worries related to mass surveillance may arise, along with attendant "guesses" for how the system impacts people's daily lives. Given the potential for the current infrastructure to track interactions

with government across the spectrum of services, residents might wonder if routinely accessing one service or another might have an effect on other Ministries' service provision. For example, if an individual routinely logs into government-affiliated websites to check how much money she would receive for a damaged vehicle, and then happens to have a car accident, will that activity be "counted" in a subsequent insurance or policing investigation? If a single-parent battling for child custody experiences depression, could logging into government mental health services at the early hours of the morning–when "normal" people sleep–be applied as demonstration of parental (un)fitness?

To be clear, *we do not* accuse *or* suspect the BC Government or any of its agents as contemplating such use cases. However, given the novelty of integrated identity systems, their technical complexity, and the perception (or reality) that systems are "imposed" by government, system users may internalize how they negatively understand such database-driven identity systems "actually" work. Moreover, there are valid concerns about function creep: the current identity system, sometime in the future, could be used in ways that citizens in a well-functioning democracy might oppose. The results of such internalization may be an effort by some residents to proactively protect their identity integrity by not accessing (potentially necessary or valuable) government services out of fear of prospective consequences.

It is in terms of trust-building and trust-management that the user-centric model we propose works to the advantage of all parties. If we ensure that the identity service provider always issues identity tokens containing *all* identity claims/attributes authenticated by the card, leaving it up to the user to decide which attributes to reveal to the service provider, then neither the broker nor the IdSP can ever know what service, specifically, the user is requesting. Nor can they know if a claim was actually fulfilled or completed. As a result the IdSP and broker are prevented from drawing conclusions about services accessed or significant inferences about the user. Multiple privacy brokers would let British Columbians distribute knowledge of their identity attributes over a range of issuers. Deploying such brokers lets the authorizing party—in the BC Services Card instance this is the Provincial Authentication Application via the Provincial Identity Information Services Provider (operated by the Office of the Chief Information Officer)—avoid appearing as a potential surveillance actor. Thus the BC Government would have a hand in securely verifying claims of identity without (subsequently) knowing how or if the identity was presented to other government service providers.

Meeting the 'High-Water' Standard of Identity Privacy

A user-centric national identity system is identified as core to the vision described in the *Pan-Canadian Strategy on IDM&A.* According to this guiding document, the user-centric approach to identity management is "at the very heart of the right to privacy". It is "inherently more privacy enhancing than other IdM&A models due to the ability of users to control the transfer of their identity credentials from one agency to another".[236] It suggests that other governments participating in the national identity system consider employing user-centric technologies.

The user-centric model we propose conforms with the pan-Canadian strategy's suggestion that Canadians have "informational self-determination". The strategy recognizes the importance of user-centric technology as way to let users control their identity credentials.[237] It is sensitive to the fact that "many systems are still built today that do not comply with best practice of user-centric development".[238] The system outlined above *is* intended to provide a framework within which best practices can flourish.

The pan-Canadian strategy acknowledges the inherent challenge in creating large, complex identity management systems designed to facilitate the maximal flow of information on the one hand but required to protect user's identity integrity and privacy on the other.

> Achieving both seamless service delivery—which is generally understood to involve more information sharing—and privacy protection—which is generally understood to involve less information sharing—requires a delicate balance and creative solutions. For example, it is likely that identity information can be shared in many cases across departments and jurisdictions for the purpose of providing a seamless, multi-channel service delivery experience, but it must be done in a controlled way and with the knowledge and consent of the client, where appropriate.[239]

The BC Government is slated to spend hundreds of millions of dollars over several years to establish the province's identity infrastructure. It should hold in abeyance current plans to fully deploy the infrastructure. If the province decides to proceed with its integrated identity management program, it should reorganize this program to incorporate a user-centric approach that is maximally privacy protective and meets the high-water standards outlined in

236 IJIMATF, 2007, p. 33.

237 Ibid, p. 89.

238 Ibid, p. 175.

239 Ibid, p. 29.

the pan-Canadian report. With the NFC chip on the BC Services Card not due to be activated for five years, there is ample time to consult with external experts and citizens on the need, efficacy and desirability of the Services Card program. If the public *does support* a high-tech identity card and associated "linked up" database infrastructure, then the government should use its significant market power to encourage the "creative solutions" envisioned in the pan-Canadian strategy.

The government is in the unique position of both wanting these cards *and* being able to shift market behaviour by creating significant market demand for privacy protective identity technologies. British Columbia has the potential to offer a democratically legitimated identity card that genuinely integrates privacy-by-design principles at the core of its service offering, instead of a government-centric experience that adopts a limited privacy-by-policy, "triple blind lite" system architecture. Only by getting privacy "right" at first can the province and its vendor partners hope to subsequently overcome the remaining security issues linked to identity cards and serve as the model for the envisioned integrated multi-jurisdictional identity system: all the security in the world will not protect citizens' privacy if privacy is not properly "baked in" from the very start of this identity project.

11. Recommendations

It is crucial for any large, complex and comprehensive identity system to have clear policy objectives supported by an evidence-based rationale. This foundation must be built in a transparent, open and consultative manner to gain public trust, and to thus ensure the democratic legitimacy of the program. To facilitate trust, good policy, and strong privacy and security controls we offer a series of recommendations. These recommendations are based on a cursory evaluation of international identity card systems, an in-depth look at identity management in Canada and British Columbia, and a careful consideration of identity and privacy rights, as well as alternative technologies and systems.

Our recommendations can be categorized according to normative conditions meant to ensure the democratic legitimacy of the card; policy recommendations meant to guide the government on developing citizen-centric and rights-governed policies; and technical recommendations that suggest how the card system could maximally protect the privacy and security of personal information.

The core takeaway from these recommendations provincially is that the BC Government should delay mass adoption or deployment of the BC Services Card program and its associated data linking infrastructure. The government ought to engage in widespread public consultations concerning the card and consult with external experts to evaluate the normative, policy, and technical appropriateness of the Services Card as designed today. Our findings support and reinforce the recommendations that the Office of the Information and Privacy Commissioner for BC has already issued, findings that warn against rapidly advancing the identity card initiative.

The core takeaway from these recommendations federally is that the privacy commissioners of Canada need to work collaborative to address the multi-jurisdictional issues raised by provincial identity systems that inter-operate with federal programs and the federally regulated private sector. The privacy commissioners of Canada have a critical role to play in terms of both providing expertise on standards of privacy and security, in addition to being the most likely means of initiating a public discourse and educating Canadian citizens about the identity proposals underway and options that would mitigate privacy and security risks.

Normative Recommendations

The BC Services Card constitutes a novel way of using residents' identity information because it relies on identity data linking systems that span government ministries and agencies. The aim of this integrated infrastructure is to make broadly available the personal information of British Columbians without establishing a centralized database in order to provide citizen services. In this, the system is essentially a microcosm of the integrated system

that is proposed federally. The province's new data linking ID "solution" relies on biometric analysis and strong document authentication processes at points of service, cryptographic analysis of identity cards by commercial partners, long-term reliance on vendors for the technical infrastructure to function, and legislative barriers (which, as was discussed earlier, were readily removed). To date the federal and BC governments have only minimally engaged the public to ascertain whether there is broad comprehension and acceptance of the identity systems in development. .

The full range of ideas and feedback regarding a potential identity system and a new health/access card for BC must be taken up and incorporated in subsequent government policies. The BC Services Card project has been so opaque to the public that the Information and Privacy Commissioner has recommended a "fulsome public consultation" before continuing to the second phase. According to Commissioner Denham, the government must explain its long-term vision for the card as well as attendant benefits and risks. Further, "solutions that the government proposes to address these risks must also be subject to scrutiny, by both the public at large and by those with technical knowledge in the field". We support the Commissioner's position: there is a significant need for public consultations in order to democratically legitimate the adoption of a new provincial identity regime.

It is difficult to over-emphasize the importance of the consultation process in developing identity policies that are secure, cost effective, robust, trusted and fit for purpose. Major identity and information management programs have the potential to reinvigorate longstanding social and political concerns. The identification of what constitutes a legitimate name, a legitimate series of data points to collect, and the appropriateness of visual or written depictions of citizens have created issues for governments attempting to impose new identity card practices. Unlike other Western nations, Canada lacks the history and laws pertaining to comprehensive, persistent and mandatory ID cards. It is important, therefore, that any imposition of ID cards be mindful of British Columbia's—and Canada's—longstanding legal, social and political traditions.

Recommendation

The BC Government should hold extensive consultations with a wide range of public stakeholders that address (at least) the following topics:

- Whether BC residents want to carry a new identity card, and channel all government services through this card, or whether they would rather carry discrete cards for discrete government purposes;
- Whether BC residents want to use the proposed BC Services Card, as presently designed, or if they prefer a user-centric approach that enables more individual control over personal information; and

- Whether BC residents want an interoperable provincial and federal identity system and the Government 2.0 data linkage programs currently underway and envisioned for the future.

Recommendation

The BC government should publicize the results of consultations on these topics and table a formal report that synthesizes British Columbians' positions concerning the BC Services Card. After tabling the report, the government should proceed to give clear policy direction to relevant government ministries. Such direction should follow from, and not run counter to, the results of consultations.

Only by holding the consultations can the BC Services Card be regarded as truly legitimate. We stress that identity policies are highly charged and, as such, can be more controversial than other policy initiatives due to how identity policies can impact the way citizens understand themselves in relation to government institutions and to one another.

Recommendation

The federal government should produce a document or a series of documents for the general public explaining in plain language its proposed integrated multi-jurisdictional identity system, including the on-going costs and business case for the proposal.

Recommendation

In light of the difficulty of convening a meaningful national consultation on this proposal, the Office of the Privacy Commissioner of Canada should lead a joint project with the provincial privacy commissioners to produce a response to the proposed Canadian identity system that includes perspectives from commissioners, civil society and citizens, and that incorporates:

- best practice recommendations, including communications and consultation recommendations;
- areas for further research;
- consensus statements on applicable standards and best models;
- lessons learned from other jurisdictions, and
- the results of any survey initiatives to poll the opinions of Canadians.

This collaborative 'reply' should include relevant qualitative and quantitative research and incorporate the voices of ordinary Canadians, either through written submissions or by using focus groups/meetings.

Policy Recommendations

Transparency is an essential element of effective policy development and good governance more generally. Our research was hindered by government's recalcitrance to publicly document or discuss the design and development process of the BC Services Card. Not only was there a dearth of publicly available information until mere weeks before the card's launch, government officials often denied or ignored interview requests from researchers, and responded to freedom of information requests with no responsive records, or lengthy delays. To this end we support the BC Privacy Commissioner's call for an end to "oral government" and a statutory duty to document the business and practice of government.

Recommendation

The BC Government should commit to making public the technical documents that detail how the BC Services Card and its related infrastructure interoperate. These documents should be suitably detailed to permit independent security researchers to evaluate the present security and privacy measures to guarantee that BC residents' personal information cannot be exposed to unauthorized third-parties.

In addition to inadequate public consultation in the lead-up to the deployment of the BC Services Card, the policy objectives and benchmarks for the program remain unclear. While the government has offered two key rationales for the program—reducing fraud and improving efficiencies (in the form of cost savings, streamlined service delivery and better patient outcomes) —neither of these has been supported by evidence. Thus the government has not shown clarity of purpose or demonstrable need for a mandatory, multi-purpose ID card.

Recommendation

The BC Government should publicize its business case for all phases of the BC Services Card, complete with an evidence-based rationale for each of its drivers and objectives.

Following from clarity of purposes, the government needs to publicly discuss its policies that address the privacy and security of residents' information that is linked to the BC Services Card, and e-government initiatives more broadly. These discussions should not constitute marketing slogans but genuinely demonstrate the government's capability to implement the technical infrastructure underlying the Services Card and evaluate the government's capability to establish and run the infrastructure. Any policy should include both the practical institutional abilities of the government to carry out this work as well as the security and risk assessments related to the data sharing networks the government is proposing.

Recommendation

The BC Government should immediately conduct a strategic threat and risk assessment on Phases I and II of the BC Services Card and publicize the results. It should consult with

experts external to government, including academics and computer security specialists, to review the results of the system test conducted in January 2013, and make public a summary of the consultation.

Recommendation

The BC Government should commit to publicly collaborating with experts to develop government policies that suitably address privacy, security, and business process needs associated with the BC Services Card.

As well as consulting with non-governmental actors concerning the privacy and security of identity documents, it is imperative that a close working relationship be developed between government Ministries interested in adopting the Services Card for government service provision and the Office of the Information and Privacy Commissioner for BC. Moreover, it is critical that stronger relationships be built between the Office of the Chief Information Office, which is responsible for the technical infrastructure linked to the Services Card, and the Privacy Commissioner.

Recommendation

The BC Government should commit to pursuing any further development of the BC Services Card and any other components of its integrated identity and information management program in close collaboration with the Office of the Information and Privacy Commissioner for BC.

The BC Services Card is a partial result of function creep, insofar as its enrolment policies incorporate ICBCs facial recognition technology and biometric database. These technical and associated data retention processes were advanced to comply with American border entry requirements, not the delivery of BC government services. Function creep is also a design feature, with the government promising to make more services accessible via the card. As government services are added, it will be increasingly likely that new and different uses will be found for both the card and information associated with cardholders.

Recommendation

The BC Government should clearly define potential future uses and services that may be associated with the BC Services Card over the next four years. Further, the government should identify the conditions that must be met prior to linking new services to the card's infrastructure. Any changes to those definitions and conditions should be publicly debated by legislators and new legislation passed before expanding the uses of the card.

Based on documentary evidence, it remains unclear if the BC Government has given due consideration to alternative ways of delivering online services to British Columbians. This lack of clarity denies citizens choice or agency in the way their personal information is handled, including processes that may be less privacy invasive. While it seems as if the Office of the Chief Information Officer may have, at one point, considered a more citizen-

centric identity infrastructure based on privacy brokerage systems, the BC Services Card program seems to have retreated from such strong privacy protections associated with such an infrastructure.

Recommendation

The BC Government should make public the alternatives considered in the development phase of the BC Services Card initiative, including alternate models, vendors and technologies. In advance of implementation, it should subject Phase II to renewed scrutiny to determine whether it meets British Columbians' needs in an identity system, and whether there are other more privacy protective means of achieving the government's objectives.

Technical Recommendations

This report identifies a series of prospective technical and security weaknesses associated with the BC Services Card. Moreover, in our critique of federated identity networks we found that they are often protective of privacy vis-à-vis policies as opposed to protective of privacy vis-à-vis technical characteristics. This report highlights the known vulnerabilities associated with smartcard-based systems as well as prospective technical security deficits of home computer and mobile phone chip readers. The following recommendations would ameliorate these weaknesses and maximize the privacy of citizens.

Recommendation

In light of federal and provincial initiatives to encourage accessing government services on personal computers and mobile devices, the federal government should develop holistic security standards for computer and mobile readers used to access government services. Given the U.S. Federal Trade Commission's complaint with respect to the security of Android smartphones[240] and other security problems reported in the technology press,[241] the federal government must provide leadership in developing the required minimum legal standards of securing personal computing equipment that is used to access government services. These security specifications should be set out in a harmonized federal standard that applies across all components of the integrated federal identity system.

Until such harmonized federal security standards are established and implemented, the BC Government should not integrate the NFC reading capability for consumer- devices (e.g. smartphones, home computer readers) and should restrict authorized "reads" to government-controlled points-of-service.

240 Ibid, p. 61.

241 Ibid, p. 61.

Recommendation

The BC Government should conduct detailed technical analyses using professional computer security firms to ascertain whether the government card readers and associated computer systems are vulnerable to smartcard-based attacks.

The BC Government technical analyses should be submitted to the federal government and all Canadian privacy commissioners in order to advance best practices and security coordination across increasingly integrated systems.

This report outlines a potential alternative for an identity infrastructure that embeds privacy in the technical design and enables users to control the disclosure and flow of their personal information that is held by government.

Recommendation

All Canadian jurisdictions should adopt a user-centric privacy-protective model that uses technical means to prevent information from being used for unintended purposes.

Recommendation

The provincial and federal governments, as part of any commitment to federated Canadian identity systems, should have their technical systems and associated business practices audited by an independent party every three years, publicly table that audit and implement the auditors' suggestions in a timely manner.

This report details the many IT systems in British Columbia that have received highly critical audits and in particular, have been found to have serious security flaws. Given the compounded jeopardy to security of a federated system, there is a need not only for audits of all parts of the system, but for implementation of auditor's recommendations. The sweeping role envisioned for the national federated identity system, encompassing both the public and private sector, calls for rigorous attention to security issues.

Recommendation

The BC Government should ensure that the current use of biometric imaging by ICBC, and the expansion of biometric templates to the BC Services Card, are proportional with regard to their privacy impact and securitization benefits.

Recommendation

The BC Government should conduct an audit of the current methods for evaluating accurate and inaccurate collections of data, and publicly make available their methodology for public review and critique.

Finally, media reports suggest that the BC Services Card may be used for online voting at some point in the future. Research to date suggests online voting is extremely difficult to secure in a way that protects the integrity of the voting process.

Recommendation

If the BC Government is considering the BC Services Card for online voting purposes, the card must undergo audits by the Office of the Information and Privacy Commissioner for BC, the Auditor General of BC, and all other relevant government and non-government stakeholders.

In summary, we have provided a series of recommendations that are meant to better secure citizens privacy and personal information. We support the Privacy Commissioner's call for the government to pause before implementing Phase II of the BC Services Card in order to widely and meaningfully consult with British Columbians. We are very concerned at the apparent late involvement of the Office of the Information and Privacy Commissioner. According to Commissioner Denham, she was still awaiting "information from the relevant ministries and government agencies" needed to complete her evaluation as late as January 2013. It is important to note that Denham was unable to conduct a full assessment of existing systems at ICBC or the Ministry of Health "because of the abbreviated time for review". To its credit, the government has accepted the Privacy Commissioner's recommendations fully, and pledges a "fulsome public consultation process" that "will inform both our design and communications related to the role identity management and BC Services Card play in providing British Columbians secure, privacy respectful access to government services and information". [242]

While British Columbia has started down the road of a government-centric identity system with the potential for state surveillance and subsequent risks to residents' privacy and informational security, the BC Services Card is not a fait accompli. Given the government's commitment to consult with the public before deploying the next phase of the project, the prevailing identity policy direction remains open to change. The policy process can still embrace transparency and citizen participation focused on a user-centric technical design that meets privacy-by-design criteria at the level of technology itself. That technological design can be further supplemented by strong policy-driven pro-privacy initiatives. Embracing this stronger pro-privacy position would be a clear improvement on the government's current privacy-by-policy approach.

Conclusion

There are many legal, political, social, economic and technical challenges related to designing large, complex identity systems. The outcomes of identity systems are often consequential,

242 Henderson, Kim. 2013. *Letter to Elizabeth Denham Re: BC Servicies Card Phase 1 Review.* Victoria, BC: Ministry of Citizen Services and Open Government, www.gov.bc.ca/citz/down/letter_E_Denham_Re_BC_Services_Card_Phase_1_Review.pdf.

insofar as they reify how citizens are defined to government and how they can engage with government institutions, as well as dictate what responsibilities and services the state will provide. This research has explored the policies, politics, and technologies informing the BC Services Card, a card that could serve as the template for subsequent national identity documents. Our research has raised a range of privacy, security and civil liberties concerns regarding the provincial government's approach to identity infrastructure. Our work has also documented how previous federal identity systems – upon which the BC system is based – could infringe on individuals' privacy. In what follows we briefly summarize key points from the report and conclude by again reiterating the importance of getting identity politics right.

This research has laid out rationales for how and why the BC Services Card could function as a national ID card by stealth. The Services Card is intended to (prospectively) integrate with federal and other provincial identity infrastructures. According to an advisory to the Premier of British Columbia: "a Pan-Canadian approach to identity management has been set as a priority by the Cabinet Secretaries and the payment card industry and BC is leading efforts in the design and implementation of the framework". We know that the BC Services Card fits within the Government of Canada's plans for a federated identity system, and that British Columbia has been a key player in developing the foundational documents meant to guide such a system. As identity policy becomes increasingly harmonized across Canada according to the framework laid out by the pan-Canadian strategy for identity management and authentication, and as more jurisdictions link in to the federal identity network, a national identity system may coalesce. Such a system is not only the objective of the Government of Canada, stated in numerous policy documents, but of SecureKey Technologies, the vendor that is principally responsible for the technical infrastructure underlying both the Government of Canada's online service delivery and the BC Services Card. Despite the federal government's affirmation that a national identity system would not consist of an ID card, the BC Services Card appears as the prototype for a pan-Canadian identity card through the provincial backdoor.

This report began with an overview of the importance of identity policy, and the challenges that arise with ubiquitous computing and the digitization of information. Governments seeking to maximize efficiencies and download service delivery to citizens often seek comprehensive and integrated databases of personal information. But identity systems, particularly those that incorporate ID cards, raise serious risks to privacy, civil liberties and democracy in general. Getting identity policy "right" is essential to preserving an equitable relationship between the state and the governed. The report continued by documenting the history of identity policy in British Columbia, which is closely linked to online government service delivery. It traced the gradual evolution toward integrated identity management based on data linking. "Government 2.0" or "joined up" government took root in the healthcare sector, with the e-Health mandate seeking to join patient information in longitudinal

databases that eventually interconnect across the country. Despite the BC Government's persistent drive toward integrated identity management, its major information technology projects have experienced serious problems in basic functionality, as well as in protecting British Columbians' highly sensitive personal information. As such, any adoption of new identity and information management systems in BC must be examined with care.

Next, the report detailed the drivers and inhibitors that influenced the development of the BC Services Card as part of the transformation of identity and information management in British Columbia toward an integrated model. It is notable that of all the rationales for the dramatic shift in approach to handling personal information, the government offers no evidence to support its claims. Particularly worrying is how the government weakened provincial privacy legislation to more easily (and legally) access data retained by provincial Ministries. Also troubling is the lack of transparency—bordering on secrecy—surrounding the design, development and implementation of the BC Services Card, despite the fact that it is a major departure from past identity management practice. Lack of transparency concerning government initiatives leads to poor policy development, non-holistic policy outcomes and a distrustful population. The report described the BC Services Card in as much detail as possible, given the dearth of publicly available documentation. It highlighted the role of SecureKey Technologies, the main vendor partner in the card program, and a close collaborator in its development. We noted the privacy vulnerabilities in the design of the system, as well as the role the company sees itself playing in a pan-Canadian identity system. Function creep is a particularly insidious concern, because the card is partially the result of function creep itself. Moreover, the infrastructure of the Services Card is designed to accommodate future, unknown uses quite apart from health care delivery or drivers' licencing.

The report contextualized the development of a provincial identity card in British Columbia within the drive for a national identity system. This is evidenced in a growing body of policy documents focused on creating an integrated online system of service delivery that incorporates provincial and even municipal governments. While the founding document for a pan-Canadian identity system embraces universally accepted fair information and identity principles, and supports a user-centric system, subsequent policy documents do not include these important components. We noted the problems with a federated approach to identity management, which the Government of Canada advocates, and discussed a privacy protective, user-centric alternative.

Public consultation is both the glaring oversight in the development of the BC Services Card, and the central recommendation of this report. To date, BC residents have not been consulted about the integrated identity management system currently being deployed by the provincial government. Nor have they had the opportunity—at either the federal or provincial level—to debate the merits and desirability of a pan-Canadian identity card system. Policy consultations have been limited to a closed network of elites and any involvement with civil advocacy groups has required signing confidentiality and non-disclosure agreements. This kind of

"transparency" is neither appropriate nor acceptable when debating policy that can significantly alter the relationship between citizens and the state. The consequence of this opaque means of governance is distrust and uncertainty from the public towards governing institutions. Despite what we have uncovered and discussed in this report, unanswered questions remain: Will the federal identity system be accompanied by an identity card? Will this system be designed such that it conforms to privacy-by-policy as opposed to privacy-by-design principles? From a broader perspective, will an integrated national identity system enhance the state's ability to know about its citizens and, in the process, potentially infringe on the privacy of citizens' lives? Will such a system endanger the confidentiality and security of British Columbians' personal information and engagements with their governments?

If a novel ID system is required to access government services then British Columbians and Canadians deserve an identity infrastructure that enables good governance through proportionate data sharing. It is difficult to over-emphasize the importance of the consultation process in development of identity policies that are secure, cost effective, robust, trusted and fit for purpose. British Columbians need an identity system that provides identity assurance in a manner that doesn't jeopardize their privacy, identity integrity, social entitlements or civil liberties. There is both scope and technological capacity for designing such an identity management framework. Government has long asked for the trust of its citizens in the development of identity infrastructures: now it is government's turn to trust that a transparent, sincere and comprehensive public consultation process will result in the kind of identity policy framework that works for all citizens.