Appendix I – Specialist Forum Report

IdentityNorth Specialist Forum – Proceedings

A Component of the Digital Services Consultation
November 27, 2013

Prepared by MASS LBP for the Province of BC

INTRODUCTION

BC's new Services Card was launched in February 2013. It replaces the aging CareCard, can be combined with a driver's license, and is already in the hands of a nearly three-quarters of a million British Columbians. Developed by three government organizations — the Ministry of Technology, Innovation, and Citizen Services (MTICS), the Ministry of Health and the Insurance Corporation of BC (ICBC) — the card is already being used by BC residents to access health services, show that they are eligible to drive, and as photo ID in their everyday lives. Within the next five years, it will be in the wallets of nearly every BC resident.

The Services Card is more than just a new piece of plastic. It has more than twenty security features. One in particular stands out: embedded within the card is a microchip that makes the card nearly impossible to counterfeit. This chip can interact with inexpensive and secure card readers — at a government office or connected to a personal computer at home — and, in combination with a simple PIN code, helps to prove that someone is who they say they are. The government has yet to 'turn on' this capability, but the necessary IT infrastructure is almost finalized and the government plans to move forward soon.

This microchip will make online access to government services safer and more secure. In an era where more and more of people's lives are happening online, governments around the world have moved only slowly to offer even simple services over the internet. Well-designed online options can often be not only more convenient for citizens but more cost effective for government.

So why aren't more government services accessible online? A major impediment has been the challenge of identity: how can a service provider, especially one with legal obligations to maintain privacy, confirm remotely that a user is really who they say they are? The fear of unauthorized access has kept many government services firmly planted in the physical world.

The new Services Card was built to help solve this problem, if BC residents desire it to. Its embedded microchip and supporting IT infrastructure (the government's 'Identity Assurance Service') allows users to confirm their identity online – thereby eliminating the need to show up in person with government-issued photo ID in hand. Users could potentially use their new Services Card to access medical records online, sign a child's permission slip on their school's website, or renew a passport.

Now that the Services Card is in circulation as a replacement for the CareCard and driver's license, the government is focused on identifying other government uses for the Services Card. Should it be used as a fishing license? A library card? The government is also interested in exploring the possibilities for non-governmental applications. In the same way that citizens use their driver's license to prove who they are not only to government but to banks, bars, employers and many others, the Services Card *could* add a capacity so that other organizations are able to use this online identity authentication service. The possibility exists for BC residents to use their Services Card to open a

bank account online, sign up for a cellphone plan, or do any number of things that typically one would have to do in person.

Obviously, these choices raise a number of important privacy and security questions. For this reason and on the advice of the BC Privacy Commissioner, the BC government is undertaking a broad public consultation on the future uses of the Services Card. Should the card's uses be limited to its current mandate: replacing the CareCard and acting as a driver's license? Should it be used to enable online access to government services? If so, which services are best suited to the Services Card? Are there any changes or additional features that need to be added to the Service Card's IT infrastructure in order to ensure that the privacy of BC residents is protected, that personal information is stored securely and that this new system is used appropriately?

Context

The IdentityNorth Specialist Forum is one component of the Provinces' Digital Services Consultation. The balance of the consultation process includes a Citizen User Panel of 36 randomly selected citizens of BC who will learn and deliberate over two weekends on how the BC Services Card should serve the population of BC. There is also an on-line survey open to all.

This two-day Forum, attended by delegates from the technology sector, civil society, academia, the public service and members of the Citizen User Panel, focused on eliciting expert reaction to the BC Services Card. In the eyes of local and international experts, does the card pass muster? What advice for improvement could they provide? The BC Government is confident that is has built a safe and privacy-enhancing system for accessing services online. But in hosting this conference, they encouraged delegates to challenge their positions and provide fresh perspective on whether the system is in fact designed with sufficiently robust security and privacy controls.

The conference was designed to be an expansive and in-depth conversation amongst delegates. While day one of the conference was structured around presentation by government officials and by leading experts in privacy and online identity from around the world, the day involved plenty of ongoing discussions, as delegates interjected with questions and broke into groups during breaks and over meals to discuss emerging questions. Day Two involved approximately two dozen breakout sessions where delegates were able to explore issues of their own choosing, discuss the finer point of the Services Card and explore its underlying identity infrastructure in greater depth. The results of these discussions are summarized below.

FOUR EMERGENT CONFERENCE THEMES

1. The Services Card is theoretically a smart design that opens up exciting opportunities for online access to government and other services

Generally delegates acknowledged that the Service Card held great potential to improve government services and increase convenience by offering the option to access services online (even "in one's pajamas", as one participant remarked) rather than having to show up in person, "take a number" and wait in line. Though many questions were raised concerning personal privacy and the security of personal information, delegates generally did not see these challenges as insurmountable.

Four broad categories of government services were suggested as possible uses for the Services Card: scheduling, licensing and permissions, making payments and accessing records. The most common examples cited were health related -- the ability to make doctors' appointments or look at health records online. Other examples put forth included renewing license plates, paying property taxes, and signing school permission forms.

Most participants felt assured that the new card could offer more speed, ease and convenience for citizens who chose to use it– particularly for those who have to access health or social services frequently, or for those experiencing stressful life events that often require "complex and frustrating" interaction with multiple, uncoordinated levels of government bureaucracy. Though ideas were plentiful, no clear and specific consensus arose about what service opportunities were most important for the government to explore.

Although there was some discussion about the potential to use the card to access federal government services (the ability to renew passports online, for example, was an important aspect of the New Zealand government's digital identity program), several delegates expressed strong concern about linking federal government services with BC's identity infrastructure. BC government representatives responded by assuring participants that the only way B.C. would share information outside of the province is if "a majority of British Columbians asked for a service that required doing so".

Delegates also recognized that data gathered through the use of the Services Card, if anonymized and handled safely, could be an important source of information for evaluating and improving government services. There is great potential in data that can show how an anonymous individual interacts with multiple government services – but this information is not currently accessible to policy analysts. Whether or not this type of data collection and analysis should be allowed — given worries about privacy and government surveillance— remained an open question throughout the conference.

When conference participants examined non-governmental uses, many saw considerable possibilities accompanied by a lack of clear policy direction. For the private sector, the card could be a valuable

verified credential, issued by a provider that has assured the user's identity. Given that usernames and passwords less and less trustworthy as authenticators for online services, the Services Card represents an attractive means of validating online sign-in. Several participants suggested that if the BC Services Card succeeds, government should expect pressure from the business sector to be allowed to use it.

There was no broad agreement however, on how any potential use of Services Card by private sector should be regulated or monitored. How would standards be enforced? How would privacy be protected? Some delegates expressed the view that government should only allow access for non-governmental entities if it individually examined, approved and enforced strict private policies upon every organization. Others saw this as too onerous a requirement — something that would severely limit adoption by the private sector and stifle the development of innovative new applications for the BC Services Card and its Identity Assurance Service.

Government representatives informed delegates that, at this point, BC is focused on services within its own ministries and agencies – not in the private sector. In the absence of clear government policies on non-governmental uses for the card, several delegates from the private sector noted that most companies would be unlikely to invest in developing potential applications for the BC Services Card. They felt that "more certainty concerning the policy framework could spur some investment" in this area.

Several participants and presenters reminded the government that, as new digital identity developments in the private sector continue to move forward, it is important to keep in mind a future where several secure identity authentication options are available. Mobile phones, one presenter asserted, are the "next obvious platform" for digital identity and authentication services, with mobile carriers around the world looking at phones as an identification device and secure portal to access various services with just one secure password. Government should consider designing the BC Services Card and the accompanying access infrastructure so that they remain attractive and easy to use for BC residents even after these other identity verification systems become more widely adopted.

2. *Privacy is Paramount*

Does the BC Services Card increase the potential for government surveillance of BC residents? Does it create an overly attractive target for hackers intent on stealing and using the personal identity of unsuspecting British Columbians? These questions require close examination of the system that underpins the Services Card – the databases, data pathways, and authentication procedures that enable the card to be used for multiple different services. As one conference delegate noted, "the Services Card isn't the magic thing here, it's the whole infrastructure underneath that matters".

Conference participants were encouraged to use their technical expertise and examine this underlying infrastructure — is it as safe, secure, and privacy-enhancing as the government asserts?

Many participants focused on whether or not the identity management system would link up information about a given individual across different service contexts. Would the government be building detailed profiles on each BC resident? Would service providers have access to more information than they needed?

Government representatives assured delegates that the card infrastructure was designed to strictly enforce 'contextual separation': no data from one government service would be accessible to the centralized Identity Assurance Provider or to other government services. ICBC would not be able to see health information, police would not have access to information from schools. They pointed out that this type of data collection is technically possible under the current system but required special legal authority (a warrant, for example) to collect and link up an individual's data in various government databases. Though the Identity Management System may make it technically easier to link up an individual's data, the legal protections that prevent such actions would continue under the new system. They expect that BC's independent Information and Privacy Commissioner will be watching the development of the Identity Management System closely and would be quick to alert the public to any changes that unduly infringe on personal privacy

Government representatives also pointed out that the card is built to enhance privacy because it will require 'data minimization'. This means that the Identity Assurance Service would only be authorized to give each service provider the minimum amount of identity information required for that given service[1].

Participants discussed at length whether the designs were satisfying. Many were sufficiently convinced, for the moment. Others wondered whether sufficient oversight was present to ensure that government followed through with its plans. Would the OIPC have the resources to undertake fulsome investigations? What happens when government (and government priorities) change? Some

[1] The example of the drivers' license used to prove one's age at a bar was given. A license contains much more information than the bouncer needs to see. The Services Card could be used in such a way that it could be tapped on a card reader, and the bouncer would only see whether one is over or under 19 – the minimum information required in that instance.

felt these questions deserved further attention.

Some expressed concern that, as more services started using the Card, the benefit to government of amalgamating data from separate service contexts would rise, exerting increasing pressure for policy change. This worry about 'function creep' — the process through which a tool designed to solve one problem then ends up being used to solve others, often without careful enough consideration – was discussed on several occasions throughout the conference, without clear resolution. Some delegates were tentatively supportive of the use of analytics and service personalization in order to improve policy and service delivery, but wanted clear assurances that personal privacy would remain fully protected under such a system. Others saw it as too dangerous to consider.

On a related note, some delegates raised questions about the cost of this identity management system: will the government be able to justify spending money on the Services Card's infrastructure if the card doesn't end up being widely adopted by various government services? There were concerns that government had not made the case for why this type of advanced (and potentially expensive) system was necessary.

Others wondered if the choice to access services in person rather than online (whether for privacy reasons or otherwise) might diminish over time. Government representatives emphasized that citizens will still have the choice to access services in person, as they always have. Some delegates worried that if online services are widely adopted by BC residents, this would inevitably cause a reduction of in-person government services. People who want to access services in person (potentially for privacy reasons) could conceivably face increasingly large barriers to doing so, especially in rural areas.

Participants were also asked by government representatives about whether the Identity Assurance Service should be configured so that individual BC residents could pull up a centralized personal usage record. Though conference delegates could see the benefits of this feature — a way for BC residents to check up on whether there is unauthorized access to their information — there was strong agreement amongst those involved in this discussion that the risks outweighed the rewards. They felt it was inappropriate for government to be keeping a record of an individual's usage history, and that individual ministries were better equipped to keep time-limited logs of service access. In the event that a Services Card was lost or stolen, the rightful owner could still request service access logs from various services in order to understand if and how their card was used.

3. Security Practices throughout the public service likely require modest upgrades

There was general agreement amongst delegates that no security system has ever proven itself infallible. Security breaches will occur with any system, new and old. The relevant question wasn't whether the BC Services Card was perfectly secure; it was whether this system was more secure than the system it was replacing. As identity fraud becomes increasingly sophisticated, government systems need to keep up. As one presenter remarked: "If we focus too much about what might happen in the new world, we forget that the old world might already be on fire."

Several delegates expressed the sentiment that it is difficult to accurately assess the risk of the BC Services Card without knowing what the infrastructure would be used for. They suggested that risk will have to be assessment on an ongoing basis, as individual services are considered.

That said, some general concerns were expressed about the security practices of government ministries and agencies. Several delegates felt that measures needed to be taken to increase confidence that all the different potential service providers (school boards, health authorities, ferries, libraries, etc.) have sufficiently robust security in place. Many felt it would be the job of MTICS to not only ensure they met security standards, but to help them in this regard.

There was also discussion concerning the security implications of non-governmental use. How will government ensure these entities are trustworthy? Will there be policies, and if so, how will they be enforced? Or is there a way to engineer compliance, and will these methods be independently tested? Delegates heard that "privacy isn't refundable," so what recourse is there if security breaches violate privacy? These questions remained largely unresolved.

Government representatives did respond to concerns about security threats by noting that the government's information security branch requires a Security, Threat, and Risk Assessment (STRA), and that the findings of that assessment need to be acted upon. Third party audits of security features would also be performed. Releasing STRAs publicly is problematic, since that would equip those looking to hack into the system with information concerning risk mitigation measures that are in effect. With that in mind, government is considering whether to release these STRAs to select groups — groups who can provide an assessment of whether these STRAs are sufficiently rigorous.

4. ***Public Trust can best be built through respectful communication, system transparency and thoughtful user design.***

Since most participants felt that privacy and security concerns were surmountable if government commits itself do addressing them, many conference attendees focused on how government could build public trust in the BC Services Card and the underlying identity management system. Even given the many potential benefits, these participants suggested that considerable work lay ahead if members of the public were to feel comfortable with this new identity system.

Participants felt the public would fall into three broad groups, and that government efforts needed to address the needs of all three groups. Group one covers those who are highly suspicious and want detailed technical information available. Group two is made up of those who are moderately trusting but will be unsettled if there is a lack of clear and understandable information; group three are those more focused on the benefits of the BC Services Card, but who may or may not be aware of the risks involved in using it.

There was general agreement that the public needs to have their choices, and the associated risks, clearly explained in a non-technical, jargon-free language. The government should refrain from portraying infallible, risk-free identity management system. Minor problems are bound to occur, they believe, and trust will be quickly lost if the public isn't made aware of this eventuality. In order to support fulsome public deliberation, government should focus on creating accessible explanations for lay audiences. Participants also felt that, on top of clear and simple explanations, detailed information needed to be readily available for those who had particular concerns or suspicions. Transparency, they suggested, would go a long way in reassuring critics.

One group of delegates also discussed the pros and cons of designing "seamless" online experience for users, in which the workflow of a system is as effortless as possible for the user. As one delegate pointed out, many people are highly task driven. "They want to get something done and will agree in principle, to whatever they need to agree with in order to get it." In many online experiences, users are asked to agree to much more than is required, forcing them to either "cooperate or defect". Delegates suggested that the BC Services Card experience should introduce and demonstrate key steps (or 'seams') to ensure that users feel well-informed about what is occurring, about the steps in the process, about what information is being shared, by whom and to whom. They felt that this system should not place undue pressure on users to go through the whole process, and that if possible it would be best to offer more nuanced options than simply 'agree' or 'disagree'.

Finally, many delegates saw the IdentityNorth Specialist Forum as an important 'first step' towards building public trust. They believed government should offer event attendees an opportunity to examine the outcomes of the public consultation before they are "set in stone" — given the range of discussions and the many questions that remained unresolved, they believe further public deliberation is desirable, and look forward to the opportunity to participate.

FULL SUMMARY OF PROCEEDINGS

DAY 1

Identity 101

Hosted by Kaliya Hamlin, executive director, Personal Data Ecosystem (co-producer and facilitator of the Internet Identity Workshop)

Identity expert and conference facilitator Kaliyah begins the session with a primer on the digital identity ecosystem, and how individuals fit into it. The players in this ecosystem fall into government, private business or enterprise, and the "feudal estates" of Yahoo, Google, and Facebook. Typically, in order to access services these entities require authentication, or a log-in of some kind and through these log-ins, we build an online identity spectrum. Sometimes we use pseudonyms, or made-up user names (YouTube); sometimes we use our real names, as validated by friends or colleagues (Facebook); sometimes we are required to have our identity verified by an official source (such as online banking).

Each identity comes with a specific set of attributes, or personal information, that can have high market value.

It's technically possible to link these identities between the different contexts in which we use them but for many people, this isn't desirable. The right to move between these identities, without having them linked together is known "limited liability" or "contextual separation": concepts that that are a recurring theme throughout the conference. Kaliyah says that the technologies for maintaining Limited Liability needs to be built into a system as it's designed, with rules in place that mandate how a person's various identities interact. Ensuring these rules are implemented in practice boosts accountability and a good online experience.

The presentation concluded with one delegate question, about Kaliyah's thoughts on enterprise federations, which would allow entities to link up systems or databases, and allow one set of users to log in to another. She thought these make a lot of sense -- but they do raise questions about security assurance -- and added that the next generation question that needs to be addressed in the identity sphere is that of delegation: how could an individual delegate specific tasks or abilities to another, without handing over total control?

Welcome Session

Hosted by Aran Hamilton and Mike Monteith, founders of IdentityNorth; John Jacobson, deputy minister of Technology, Innovation and Citizens' Services of BC; Elizabeth Denham, information and privacy Commissioner.

Hosts Aran and Mike welcomed delegates with a brief introduction to their organization Identity North (founded to bring together the public, industry experts and government) and kudos for what the British Columbia has achieved in this field. They noted that the work of the BC government "miles ahead on the world stage" is what has drawn so many internationally-recognized experts to this conference.

John Jacobson outlined the two broad

tasks for conference delegates: First, to challenge the government's adamant position that they've built a very safe identity infrastructure "through the process of tearing it apart, both intellectually and at a technical level;" second, to determine what government can do with this infrastructure. "What kinds of uses should this card have, and where should government draw the line?"

Privacy Commissioner Elizabeth Denham emphasized the importance of this task given the "profound reach" of the government's new identity services program and noted that the potential of the program to connect a person's discrete activities across a lot of platforms presents "a big privacy risk here, if it's not built right." Denham told delegates that this ability to collect and analyze huge amounts of data is an issue that weighs on the minds of Canadians and citizens worldwide.

Why does identity matter? To whom does it matter?

With Don Thibeau; Kim Cameron; Krystyna Hommen; Andre Boysen

Panelists discussed how, in an era of declining budgets, this expanded infrastructure will allow government to meet increasing service demands. For Exceleris, a private-sector business providing health services, the card "provides an opportunity to enhance services." Delegates were told there is tremendous demand in private sector to access health services online, and a recognition in the health sector there needs to be upgrade in those tools. "The public is asking for these kinds of things." In addition, delegates heard, the card also offers an opportunity to "get beyond user names and passwords." One panelist noted the password reset problem was a reason why government tends to limit what it does online. With the Services Card, like a bank card, security is anchored in the card, "something they always carry around" rather than the password.

However, delegates also heard that "the card isn't the magic thing, it's the whole infrastructure of what gets the card used for." Technology allows the card to act as multiple cards, for multiple uses, but much of the conversation in this session focused on the importance of contextual separation; these multiple uses shouldn't be connected. Panelists agreed that the need to retain this aspect of privacy online, where one's discreet activities in separate spheres can be kept separate, is "at the heart of our culture." One example cited was that people don't want ICBC to know what's going on with their health records. The need for a system with the means to allow this isolation was emphasized, and government representatives responded with assurances that this identity infrastructure was designed with no one central database. In addition, delegates heard, it was built with the notion of proportionality, or the ability to allow people to give up only those elements of their identity required "to get what they came for today."

Panelist noted that the challenge is creating a mental model to communicate to people that this is the case. even though they are using one card, that's not the way it's being propagated throughout the digital system. The only way to guarantee that contextual separation, suggested one panelist, is to have a "provably blind" technology that does it mathematically. Ian Bailey responded to concerns about contextual separation by affirming that it legally cannot do this without explicit permission. Still, at the end of this session

delegates questioned whether we can trust the government not to link databases together anyway. One delegate also wondered if this question even matters to younger generations, and how much work was being done to consult them.

Understanding the community: Who is here? What do they know?

Facilitated by Graham Whitehead, IT and Services Professional, Member of ID Ecosystem Steering Group

This session teased out some critiques of the identity infrastructure, which fell under several themes: the government's prerogative to create the card in the first place; it's ability to maintain privacy and security as it currently envisions the card; and the potential for privacy and security threats as the card evolves and likely becomes used in the private sector.

One “antagonist” of the government asserted that it hasn't made a case for why it was necessary to spend money building this new identity infrastructure. “Is this a good use of money public?” Another described it as a “very nice Cadillac” of an identity system that now has to determine where it wants to go. There were concerns expressed by several delegates who identify with privacy about “function creep”; the notion that the system will graduated take on more and more uses, and with each, the security and privacy risks will rise exponentially. At a federal level, one delegate noted that since the advent of Health Canada's electronic health record systems, they've seen “a lot of pressure from the private and public sector to use the information for secondary purposes.” From the New Zealand government's perspective, noted Colin Wallis, businesses are taxpayers that have the right to able to consume that data responsibly.

In response to security threats generally, one delegate pointed out that there is no system that hasn't been broken and that the focus should be on adapting to imperfect systems. “If we worry too much about what might happen in the new world, we forget that the old world might already be on fire.” In response to security threats specific to the identity infrastructure, Ian Bailey noted that the information security branch is required to undertake a security risk threat assessment, although it's uncertain at this point whether it will remain internal to government, be released to the public, or be released to select groups. They are planning to have a third-party review the risk assessment, and are waiting for the results of this group consultation to determine how far they will go with it.

Talking about Values and Roles in Society

Facilitated by Richard Austen, IT expert and Counsel, Deeth William Wall LLP;

Vincent Gogolek, Executive Director, BC Freedom of Information and Privacy Association

Vincent Gogolek and Richard Austin discussed the various roles that make up an individual's identity and the values and attributes that are associated with those different roles. These can be consistent, but the context can change. The hierarchy of values can change somewhat. This led into a conversation about what this means to different people.

An IT specialist hired to help build the government’s Services Card system described a “whole community of people” who know him not as an IT guy but a

custom bike wheel builder. Privacy commissioner Elizabeth Denham described having to “keep mum” when political topics come up in her book club. Another delegate gave an example of how the people on his block each supported a neighbour who had lost a spouse, but chose not to talk amongst themselves about the death in an unspoken agreement to respect the privacy of their grieving neighbour.

Case study: How online service delivery is faring around the world

Raphael Diaz, North American Strategic Engagement Lead, GSMA

Diaz introduced GSMA as a trade association of mobile industry and mobile users worldwide. He told delegates that the industry's need for secure digital identity and authentication services because “everything is converging on mobile.” Delegates heard that mobile phones make sense as an identification device because it's portable and stays with the users most of the time, and its ubiquitous. The biggest asset for identity is the mobile phone number itself, with SIM-based security, local regulation and a billing relationship, regular customer contact, and consumer trust.

Using one's phone as a portal to access all kinds of services is appealing to their UK market: people don't have to remember passwords. KDDI in Japan and Dialog in Sri Lanka are two examples of mobile carriers that allow users to use the same login for hundreds of third-party websites.

Diaz described the market need in the UK is a trust entity to provide citizens and service providers with a secure digital identity, and discussed several commercial pilots in the works, including a UK Alpha project. The wider vision, for the alpha project and beyond, is a secure and trusted marketplace that allows consumer to control share and benefit from their digital transactions and personal information. He told delegates that mobile carriers can be the “trusted guardian of customers' digital identities.”

Several delegates objected to Diaz's association of anonymous “burner” phone with drug deals. A representative from a social service that works with survivors of violence pointed out that given the prevalence of sexual assault, there's a significant portion of the market who would want to access services without having their ID authenticated and stated that from her agencies' perspective, “we believe people have the right to anonymity.”

Case study: Comparing online service delivery approaches

Colin Wallis, Authentication Standards, Department of Internal Affairs NZ

Wallis opened this session with his take on how things are changing in the international identity sphere. Delegates heard that initiatives are no longer mostly government led, there is an increasing amount of specific legislation, and they are beginning to become optimized for mobile devices.

He described the New Zealand experience building two foundation services that are centralized but separate: a government login service, and a government identification authentication. The former is pseudonymous, merely confirming “you are the same personal as the last interaction,” while the latter is a “triple blind” identity assurance service that confirmers a users' identity from an

internal affairs verification service. “No one part of the system as all the information to profile you,” he noted, so that it information can't be aggregated in a way that gives “all the keys to the kingdom away.” Delegates heard that while there have been “plenty of transactions”, there are only 1.1.6 million total citizens logon accounts, less than 30 per cent of the population. In terms of RealMe accounts (the id authentication service) there are only 3,800. Wallis noted that there has been increasing private sector involvement, and that a major “PR win” for the government was the availability of online passport renewal.

Wallis identified two types of consultation; a genuine attempt to build something together, and the putting up of a litmus test to gauge reaction to what has already been decided. “Between these points is a sweet spot where the court of public opinion allows the government to do the work. I think BC will maybe get value out of trying to find that spot.”

Presentation of the BC Services Card

Bette-Jo Hughes, Associate Deputy Minister and Government CIO, Ministry of Technology, Innovation and Citizens' Services

Jay Schlosar, Assistant Deputy Minister, Strategic Initiatives Division, Government Communications and Public Engagement

Ian Bailey, Assistant Deputy Minister, Technology Solutions, Ministry of Technology, Innovation and Citizens' Services

Jay Schlosar opened this session reflecting on his own family's rather unique and constant demands for health care services. He personally sees a huge advantage to being able to access these services online. And, he pointed out, a large majority of British Colombians are already likely to use government websites as primary channels for services. The private sector has created more comfort around digital services, and BC's new identity infrastructure is about augmenting what government, expanding services, increasing “stickiness” so users come back. That means thinking about service as a journey with “quality each step of the way.”

Broadly speaking, “the BC services card is a chip-enabled card that can be used to securely access government services online and in person.” Its main purpose, delegates heard, is to replace the care card, and it was developed by three organizations (the Ministry of Technology and Innovation, the Health Ministry and ICBC) over the past 12 years. So far, just shy of 700,000 cards have been issued: 130,000 are non-photo, 250,000 combo cards, and 350,000 stand-alone cards. Government representatives reiterated the questions the government has as it proceeds to the next stages of implementation: What services should be accessed first? Should we draw on BC Services Card usage data to improve policy and services? How else could the BC Services Card be used by non-government organizations to improve the lives of residents?

Ian Bailey described some of the details around the architecture of the card. The biggest decision, he said, was settling on the EMV contact-less chip, after determining it was the most cost-effective, secure and commercially available. Bailey demonstrated how the card works by using it to access a school district websites. The demonstration prompted some questions from delegates. There was considerable

concern that the school district website showed card history. There were also concerns raised about how the school district (or whatever entity) would be able to protect information given in these transactions. This was identified as an area of improvement.

Success by design, focusing on the task: What is success? What is the required discussion?

Facilitated by Gerri Sinclair, Corporate Director, TSX Group, Vancouver Airport Authority; Principal, The Gerri Sinclair Group

Sinclair brought up a series of questions she felt were key to the process, but which remained unanswered: How, and if, the government would use the public consultation; what it could learn from the low adoption rate in New Zealand's identity program? And what it could learn from the rollout of the smart meters or HST? She also reiterated a point raised earlier in the day, of whether the program is a good use of public money, and asked if a chip reading fob would be a "hassle for us to deal with."

Sinclair noted that, from the perspective of a private enterprise, working with this identity assurance service puts a lot of trust in the government. "If you were my payment card processor, for example, would want to see PCI certification to know you've done due diligence. Where is that with government?" Again, she raised the issue of contextual separation, and expressed concerns that anonymous linkages could be undone "by force of law." One delegate echoed her point made about PCI certification and raised concerns about the boundaries of the infrastructure. "If the intent is to confine this capability to government services....then I for one am comfortable that we don't need as much evidence of trust that we need if we're going to go outside of the province. I think citizens need to know what the intent is."

Group Dinner and Fireside Chat

Panel discussion moderated by Aran Hamilton

Andre Boysen, EVP Marketing SecureKey Technologies Inc.;

Colin Wallis, New Zealand Department of Internal Affairs;

Kerry Munro, Group President Digital Delivery Network at Canada Post;

Don Thibault, Chairman of the Open Identity Exchange.

This evening panel discussion focused on "what's beyond the card," and what possibilities exist in the private sector. Discussion focused on letting users decide what they want, and building privacy infrastructure around those market drivers. Wallis noted that often government take the position of "we know best," but instead, when it comes to determining how far this identity infrastructure should reach, governments should "let the court of public opinion decide where the balance lies."

Panelist Don Thibault told delegates that "identity is the issue of our time." He noted that US companies will take e along time to recover from the Snowden disclosure, something that will fuel intense resistance to identity projects like this in the future. "When you violate trust, it takes a long time to recover." He told delegates that the next challenge for leaders in this sphere is the mobile device sector, clearly "the platform of choice."

Kerry Munro highlighted this, pointing out that Canada Post's mobile app was the most downloaded in Canada. He noted that Canada is the most digitally engaged country on the planet, with the average customers spending 45 hours a month online. From his perspective, identity authentication infrastructure holds big potential for e-commerce, "so if we build a product for a user exclusively in a large company or exclusively for a government, we are missing the mark." Delegates heard this passing of information between customer and business comes with risk. "Facebook and other great companies. . . make their business on your data." The big questions, he noted, are how to give information to someone but keep it protected.

DAY 2

Minister's Address

Remarks by Andrew Wilkinson, Minister of Technology, Innovation, and Citizen Services

Andrew Wilkinson, Minister of Technology, Innovation, and Citizen Services, addressed delegates before the beginning of the "unconference' breakout sessions. Wilkinson described health care fraud as one of the primary impetuses for the Service Card. There are more card cards out there than residents in BC, which is a big problem for health records as well. The Service Card is meant to give British Columbians a more solid form of identification, one that is less "clunky" than a birth certificate or passport.

He identified three "legs" of this issue. One is identity, the second is payments, and the third is the "big, big pool of data." On the issue of identity, he noted that government and citizens want a secure identity "so nobody else is abusing your name and stealing healthcare service." Government also wants to look to the wider world and ask what citizens would like.

On the issue of payment, Wilkinson noted that users could link their Service card to their bank card – could essentially be used to "replace most of the cards in your wallet." He emphasized that all expanded services will be optional, and although it's up to government to inform and give people legitimate options, "government can't be a nanny."

On the issue of big data, Wilkinson emphasized that the Services Card "cannot be inadvertently signing up our population to bad deals" like those consumers are subjected to when they click on most privacy agreements online. "It is not our role to facilitate junk mail and banner ads." He told delegates that government wants to put out a safe and valid menu of service options for people to consider. Delegates heard that government is essentially competing against private-sector initiatives like Google Health Wallet – ones that will likely be "data-mined like crazy' and will be the default if governments don't step up.

After Wilkinson's' presentation, a delegate asked if services that are voluntary at first would eventually become mandatory. In response, Wilkinson noted that it wouldn't be in government's' best interest to force services on the BC population, a place where people "expect their rights and autonomy to be respected." Wilkinson told another delegate that the government's goal is to have 3 million cards in circulation in the next four years. "By that time, I'm hoping people will be clamouring and enthusiastic to get their cards."

Identity North Conference
Day 2 Breakout Session Notes

Session 1.1: "It's me again." Commercial opportunities from a widespread, strong authentication service

- The group all immediately agreed that there was not enough motivation for the card to be an additional authentication service for commercial transactions because there is no need: we already have too many authentication services and compared to what people are using it is redundant.
- The group brought up that authentication of residency or age online (for buying alcohol, for example) for would be the only benefit, since this is not currently possible.
- In the physical world (i.e. for building or locker access) everyone agreed that there would be benefit because physical access is normally high friction.
- There was widespread agreement in this session.
- Debate is whether people need to be using the card a lot first before they are used to it enough that they will benefit from the authentication system. Otherwise it's just a new thing that they will need to learn. People don't understand it. Unless they have to use it to get in for like a government site or something. And if so, then is it easier than calling or going in.
- Unresolved question
    - Are we building infrastructure or a point solution?

Session 1.2: Human Rights in a Digital Age

Facilitator Lead: Dan Hall

- Participants were concerned about how well their rights to privacy could be protected in light of the creation of a narrative or persona through the increasing linkage of data to one identity – though the BC Services Card does not do this, it is increasingly occurring in the Digital Age.
- Participants were also concerned about the value of such comprehensive and linked databases becoming a target or driving a monetization or commercialization of the information, and the irreversible damage done in the event of losses of privacy.
- While concerned by the inherent risks of creating valuable (and potentially targetable or sellable) databases of information, participants also saw great potential value for improving efficiency and personalization of government services.
- Participants were interested in gaining greater control over the information associated with their identity, but unsure how much control would be appropriate or what the mechanisms for this might look like.
- Participants saw great value in the possibility to use linked information in aggregate (de-personalized) to inform more effective service delivery models (for

example, improving public transit planning, or identifying environmental factors impacting public health).
- An in depth review of relevant provincial and federal policies could help solidify participant understandings of the risks and potential benefits of sharing data between databases

Session 1.3: How to communicate to an anxious public?
Facilitator Lead: Patricia Wiebe

- In this session, people presented ideas about how to not just make the card secure but on how to make people trust that it's secure.
- This discussion focused on the challenge of explaining technical and policy changes to the public audience.
- There was concern about jargon and technical language that was inaccessible to a wide audience (ex: "unidirectional linkages," "polymorphism," "trust framework")
- The public needs to have their choices and the risks clearly explained to them.
- However, there will be a small number of people who will want to know detailed information about security features: "There are identity geeks out there. We need to have the complicated, detailed information for them."
- People need to know that no personal info is stored on the chip.
- There is a need for a whole package of targeted messages to reach a diverse audience.
- Focus on "Keep It Simple Stupid" and "What's in it for me?"
- "Citizens are willing to give up information for value. If we simplify the process, then people will trust it more – not necessarily for the better. The private sector does really well. They smooth over the links and make it very easy for people to sign in and give up a lot of information without people even realizing they're doing it because it's so simple. The government needs to be careful about this"
- The default should be the minimal amount of information shared.
- Communication and Trust Building ideas:
    - Stories
    - Convey that you don't have personal info at Front Counter offices (ICBC)
    - Whiteboard Animations
    - Diagrams
    - Short ads on television
    - Government must be transparent
    - Messaging should be responsive and change over time
    - Central database issue – How do we convince people that it actually doesn't exist? There's a cognitive dissonance. If you get all these services on this one card, how are they not all stores in a database? We need an analogy, some way of explaining that there is no central database. What we're proposing is there is no map between all the disparate identities stored on the card.
    - governments need to be transparent / government needs to provide info of what it's doing to gain trust

    - One proposed solution by one: having people consent to authentication and use of identity information EVERY TIME the user logs in - "If you have a consent form every time that people have to consent to giving information, then people will understand that government doesn't actually know anything about them."
- Unresolved Questions:
    - Should Government track transactions so they can provide citizens with a log?
    - "We need to collect some basic information for the product to run. Yesterday's 'smashing the glass idea to get to the fire alarm' analogy was good – we need to set it up so you smash the glass to get to the data."
    - Can we build the system to forget out data?
    - Surveillance vs. Security
    - How will Government monitor the private sector 3rd party contractors who are connected to Service Cards?

Session 1.4: Trustworthiness of different programs and issues of understanding identity authentication; Certification

Facilitators: Graham, Earl, Ben, Peter, Peter

- Members identified that there was a lack of knowledge and uncertainty over the authentication process.
- A government official identified that the Bank Act of Canada is the one source of legislation that specifies a set of criteria for authentication.
- International standards were suggested and a framework for accreditation and possible adoption of standards for the BC government to consider.
- It was suggested that the government refrain from suggesting this new process is infallible and avoid all invincibility descriptions.
- It was discussed that if organizations use recognized standards then it is possible they may be protected from legal liabilities.
- Some participants raised the concern that most people assume some of these issues are being taken care of, yet many of these issues remain to be addressed.
- Can we trust this system to be rock solid? Some participants stated that they are not aware of a better system, but acknowledged there are risks with every system.
- The British Columbian Government is the authority of the BC Services Card and could be the assurer of data and information.
- An outstanding question that remained was are there indicators or evidence that can demonstrate the system is trustworthy?

Session 1.5: No Universal Identifiers

Facilitator Lead: Patricia Wiebe (with input from Andre and Dmitry)

- This session served as a chance for the facilitators to explain, provide further clarification and to describe the strengths and privacy benefits that informed the decision for the BC Services' Card not to use Universal Identifiers.

- Throughout the explanation, there were differences identified concerning the use of the word ‘consent’ — BCPS personnel emphasized its specific legal and policy use and its variance from its less formal use in our conversation. Participants sought a deeper understanding of how citizens were indicating what actions they did or did not ‘consent’ to; staff described the concept of ‘informed notification’, and drew parallels with what is unspoken and implicit in in-person, front-desk transactions in order to clarify how information is to be used to render a service or proceed with an interaction.
- A participant expressed concern about ‘cross-system enforcement’ — the idea that action might be taken in one context (such as a restriction on driving) based on information or policy from another context (such as one’s health assessment). BCPS personnel emphasized that this activity already happens. While implementation of the card makes such activity comparatively easier, in practice, the same policy safeguards governing this activity now will continue to ensure such cross-pollination only occurs with legislated authorization.
- One question was raised about the responsibilities of the identity service and the service providers in cases where services are being abused. Facilitators responded that the services’ own procedures on responding such cases would be in effect, and it is anticipated that the Identity System will help service providers in verifying identities to prevent these kinds of abuse or activity from proceeding unnoticed.
- Some lingering uncertainty remained about whether policy safeguards would be sufficient to prevent cross-system enforcement from impacting citizens in unforeseen ways.
- A number of security concerns were raised in this session; Dmitry offered to go into a deeper explanation of the security and cryptographic features of the chip, chip readers, Identity Assurance System and Secure Key database procedures in a later session (which was held in Room F during Session 3). Some of the concerns stated and addressed in this and the technical session were:
    - whether chips in cards were vulnerable to ‘skimmers’ (as widely rumoured online)
    - whether chips in cards were vulnerable to physical attacks or ‘man in the middle’ attacks in the communication layers
    - whether chips could easily be cloned, through exposure at the hardware manufacturer level
    - what procedures and protocols were involved during chip personalization
    - the risk to individuals of compromised chip readers and terminals
- In technical explanations, staff made reference to GUID and UUID standards. A participant pointed out that while these terms signal something to those familiar with technical standards, the terms in these acronyms (‘Global’ and ‘Universal’) run counter to the session title’s claim that no universal identifiers are used in the implementation of the BC Service Card. Facilitators acknowledged the value of this.
- Some felt the Government faced significant obstacles in being able to convey this information in a way that could effectively anticipate and address the wide spectrum of the public’s concerns (technical, legal, practical, etc.) on this topic.

- Transparency in informing and educating about safeguards in the system (technical and otherwise) is important, although the same communication challenges exist.
- At various points in the discussion, certain features and directions were referenced which facilitators and staff stated "could" happen (primarily on technical topics, such as whether chip numbers are static or dynamic, or whether chip PINs will be used). Participants were interested to know more about how and when these decisions would be made.

Session 2.1: Sociological aspects of the issue
Facilitator Lead: Gordon Ross (gordonr@openroad.ca, 604-566-8301)

- Participants frequently returned to a theme of the state reducing a person's complex identity to an overly simple, codified identity. A government employee explained that the government isn't so much interested in developing long linked narrative identities, but more about finding a better way to solve the problem of delivering services.
- Is the province approaching this from a stance of "We have a hammer, now what are the nails?" … " To what problem is the identity system a solution?"
- Some participants felt that there is inevitability to the mass implementation and ensuing loss of optionality (no longer truly voluntary) to the one card solution.
- Even though government representatives explained no data is shared by departments, and there is the same level of possibility now as in future for departments to share data, some participants were still concerned that the card suggested, even if only symbolically, that the government is moving toward sharing data between departments.
- It was noted that the card is technically irrelevant to identity management and the potential for data sharing is always present, independent of the card. It is common practice to conflate the card and identity.

Session 2.2: Building on Identity 101
Facilitator Lead: Kaliya Hamelin

- This session built on the Identity 101 session from Day 1 on "The Valley of User-Centric Identification." The facilitator described the recent history of Enterprise Identity Systems, the difference between the rights, responsibilities and expectations in the relationship between, on the one hand, enterprises and employees, and on the other, governments and citizens.
- The facilitator then described the current state of affairs in The Valley, populated by unregulated companies engaged in data collection (Google, Facebook, and others), companies focused on data aggregation (Equifax, Intellius, and others) and advertising networks. There are also "peasants" — individuals being manipulated into providing their habits and data for someone else's largely financial gain who receive little protection or attention, who largely remain unaware of how data collected from their environment, interaction, actions, etc. is increasingly being used to shape their online and offline experience. The topic

also moved to the emerging tools, services and applications of "personal data clouds."

- The facilitator shared a number of diagrams and slides to help illustrate the breadth of potential data collected now and in the future from citizens, the number and size of the players in "the Valley" using this data for profit, and the risks associated with emerging kinds of data being collected (such as biometrics) for identification and profiling purposes.
- Participants discussed why The BC Services Card is significant: because it is designed to keep information from being linked together "behind the scenes" without permission of the individual at the centre of it. The unique nature of a government's broader and long-standing relationship with an individual makes it more likely that it will be more conservative in establishing such links and strive only to do so in ways that the individual controls or approves of, compared to other private interests operating in the identity space.
- The role and/or value of personal data clouds for the public interest is intriguing and promising, yet currently largely unknown.
- Some participants concluded that the overlaps and areas of divergence around the collection of data by various third parties, on the one hand, and the value and control of data one collects about one's self, are likely to both shed light and obfuscate on how government might proceed.

Session 2.3: Verified Attributes

Facilitator Lead: Andrew Hughes

- This discussion untangled the idea of verified attributes and explored the role government should be taking in providing credentials to citizens. The facilitator challenged participants to question why Government takes the lead role on verifying identity when it could be contracted to a private specialized company.
- This discussion explored how individuals through the BC Services Card can control information flow.
- "In the online context you need a protocol to pass those attributes over and you need trust."
- Identity is a set of attributes. Policy has a major role to play.
- The consultative process is valuable.
- At the core of this issue is trust. Trust can be built through a variety of processes such as maintaining a good track record, knowing people who use it and by receiving a referral.
- It was noted that the BC Identity space has grown out of user-centricity. The authentication part is important but not the central part. The chip technology is not at the core.
- Participants discussed the need for a way to transport credentials.
- Unresolved Questions:
    - If a private organization is authorized by BC Government to connect to the Services Card will the BC Government be accountable if the private organization infringes on my right to privacy?

- Will the terms of service be provided to Citizens in an understandable format?
- If you have 6 data points confirmed, why do you still need government ID?
- Is it the business of government to be the source of truth?
- How will BC technology link up with other Canadian jurisdictions?

Session 2.4: Card History, Where has my Card Been Used?
Facilitator Ian Bailey

- Discussion is around whether and how much the province should be tracking how and where the card is used. There was widespread agreement of the need for policies around this and citizen trust, but no concrete method for achieving this.
- It was agreed that a major reason to track how the card is used is for fraud prevention, which is a need that we have heard from the public. People want better control over their information, and we as the government feel like we have a responsibility to address this issue.
- The group spent a lot of time discussing the issue of citizen trust of government and in the security of the card and their privacy, especially when the explanation of how that security works is so technical and difficult to comprehend. The question arose of how we get people to trust that the government in keeping their information secure and not abusing their own power. There needs to be enough trust that they use it the first time
- How the data is kept needs to be reviewed. There are different options in terms of how long the data is kept, if the government itself needs to keep that data or can we have a third party deal with that, and if people can opt out of having their data be stored so that we are not taking away their agency.
- The group identified that with this ease of aggregation, there are more risks of crossing boundaries. Different groups are going to want access to the data as well, such as law enforcement.

Session 2.5: Creating an identity ecosystem – collaboration in identity services

- The facilitator proposed the question: how does a service in Ontario create something new on a platform developed in BC to be used somewhere in NS and as part of the process create benefit for each one of those actors?
- Generally, participants saw tremendous opportunity for new services to be developed, but acknowledged there was also considerable risk for service developers. Consequently, participants found a need to understand what types of identity we're trying to create services for
- What an ecosystem does is provide continuity for innovation within which there are boundaries of acceptable use. We can help bring people through the entire continuum (of creating a service) in an accelerated process that creates benefit for each of the actors.
- Some participants focused on how to create a better framework for collaboration (to create identity services that could be used with the BC services card), others focused on the difficulty of trusting every actor in the identity ecosystem.
- One participant distinguished between the who vs. what of identity – and argued that people were ok with revealing the who (basic identity to authenticate) vs. what (more the role that they play, or roles, or other personal information)
- Unresolved Questions:

    - How do we ensure the trustworthiness of all the players in the ecosystem? Is there something we can engineer to ensure compliance, is it something in the private sector or is there a role for governments in all this?
    - What is needed for tech transfer to be commercialized, what is the role of private sector and government in protecting identity? If we are to have a digital economy and technological transfer, what do we need to have? And who creates these services – private sector or government?
    - How does the ecosystem itself mitigate risk? Because from a business perspective it's all about risk. How does the system multiply efforts? How is the ecosystem managed and how is the ecosystem governed?
    - Sharing information – who is getting the value?? Are the companies getting the value from citizen's information? Who is getting the most value?
    - Policy vacuum creates a lot of uncertainty; if you create some certainty in the policy framework then that could spur some investment. So the question is what comes first, policy or services?
    - "Facebook and Google are getting this information anyway. Already people are trading their identity for very insignificant trade-offs. And policy still hasn't caught up with that. I deleted my Facebook but Facebook still owns that content that put there for perpetuity. Where is the precedent for that?"
- Barriers to identity ecosystems:
    - Investment. Some people are now trying to develop applications and saying the BC services card is a path to this application but investors don't want to get onboard because there is too much risk
    - risk mitigation
    - technology authentication barrier – "someone can always get past security measures that are in place"
    - policy barriers
    - digital identity info from province is not available to private companies
    - lack of trust and non-participation (solution = education)

Session 3.1: The lifecycle of data

Facilitator Bill A.

- Discussion took place around the question what happens when you die or want data taken down. Data doesn't die like it does in the criminal system.
- There is no refund on privacy when it's infringed upon – once the data has been taken, there's no erase button, it's gone for good.
- Points of the discussion:
    - "It's a case by case thing, how government services get delivered online. This isn't about a central information bank, this is about how governments deliver services. And should we figure it out on a case by case basis?"
    - "Over time, we can imagine all gov services ending up online, so how do we envision that operating? We need to start thinking about that now."

- Participants showed a lot of concern that the BC services card would start out as option but eventually, if the majority of BC residents had one, it would become a major inconvenience to not have one – in effect, people who didn't have one would have trouble accessing services. There was also a lot of worry expressed about the security of online data – if data can be assembled for an end user from various disparate online places, then how easy would it be to assemble that data for someone else, not the intended user?
- It was discussed that the BC services card is not a centralized bank of information.
- Participants made recommendations that the government should make sure that people who chose to opt out were not left behind; that the government should focus on improving the general delivery of services and not only moving services online.
- Discussion of the benefits and risks of the potential of data linkage:
    - It is difficult to draw the line between monitoring data for good and bad uses – how do we protect data from being misused? Should monitoring occur to protect against bad uses?

Session 3.2: Is this actually optional or is it mandatory?
Facilitator Lead: Colin Bennett

- Participants felt, that there is a deficit of public confidence in what is being done, and agreed that more transparency is needed. In line with this, there is a need for citizens to better understand what they are authorizing the government to do and be involved in making the next steps together with the government.
- Some participants expressed interest in the possibility of the card to helping to improve services and citizens' control over their own information.
- Others were concerned by strong suspicions that the one card system is not likely to maintain its voluntary nature, at least in a de facto way. For instance participants were concerned by the potential of the card (and it's facilitation of more online service provision) to cause a reduction of in-person government service availability. In essence, they were concerned that not having the card would put some citizens at a disadvantage thus making the card de facto mandatory for best service provision.
- Regardless of how information and identity data is actually managed, some participants raised the point that the card would likely become symbolic of citizenship/identity, similar to a mandatory ID card.

Session 3.3: Facilities Security and other Weak Links
Facilitator: Dan Hall

- This discussion was about the physical security of the places where data is stored or accessed. A government official explained how data centres are protected from all forms of disaster, damage, loss or theft. The BC Government uses a variety of security mechanisms to protect personal information of British Columbians.
- Participants were searching for the "weak links", where mistakes could happen or accidents could arise. The group discussed fires, earthquakes, power loss, thieves, disgruntled employees and other risks that might put BC government data at risk.
- Discussion moved to citizens who might be at risk for loss or theft of their cards such as homeless populations.
- Participants were concerned about thieves using chip readers to scan the cards through a wallet while in public.
- Unresolved Questions:
    - How will the Services Card assist vulnerable populations like the homeless to access their services and entitlements?
    - How would people access their services without a computer or smartphone?

Session 4.1: Conversation on the Power of Data - Exploring how there will be new possibilities and new data that results from new services online.

Main Points:

- The group was immediately concerned that government monitoring of identity is problematic and with all data centralized this can lead to government and law enforcement having too much information on us. Several members of the group expressed feeling uneasy about the potential level of surveillance and how it could lead to the criminalization of individuals.
- There was general agreement that we should be anonymizing all this information, as we currently do with the medical system, because this can protect our privacy and we can still collect useful data and still can do authentication. There was some discussion on what's the minimum amount of information that should be logged?
- The group discussed potential benefits of the identity service such as reducing friction in the school registration process, however there was still some unease from some group members by how much information is collected in this process and if families can choose to opt out of it.
- Most of the group came to agreement that something like this can be used to better align services because different agencies can share data more easily but this does not necessarily mean that there just has to be one database that is all accessible to achieve this.

Raw Notes:

Intro: There is a deep mistrust about this from the public. One way we can assuage people's concerns is to assure them that data is not being linked together. There are

interesting ways to leverage this, but we need to consider the mistrust of the public and how this will affect this.

- Once individuals know that there is some data then people will want to use it. Like the facial recognition software.
- Can we anticipate some of the reactions/consequences? And can we make policy around it?
- Person from analytics company: there are great things the government could do, but it makes me uneasy. Brings up Britney case as part of utopian state to be able to prevent this.
    - Britney case: Britney is a young girl, dad in custody. He gets out and he's an alcoholic in probation. Foster care puts her into his care. He goes to work one day, and loses his job. He goes home and drinks. She comes home, he gets mad and pushes her down the stairs. She breaks her arm. Now he's in custody.
    - Utopia would be: State understands he is in probation. Job lets probation officer know he will lose job. They call school and let them know. They put her in foster care for a couple of days. She's ok and he stays out of trouble
    - Question: is this part of his probation or generally monitoring of identity. Because if it's the latter then it's problematic.
- Identity system shouldn't know any of that.
- Another example. Someone uses their card to check in at the bar, then the liquor store, then the hospital, then to file an ICBC complaint. Should we be using that data? Should we be building in to the identity system? Answer is No.
- So what can you do: Anonymize all of the data.
- In New Zealand case they dealt with two court orders to get data and they went to the identity people. The court can get the info. But it's hard. It's easier to have law enforcement go to each service place, not to the identity system. It's always simpler to do other things than go to the identity system. That's the way it should be.
- Data exhaust: definition: a piece of data that is a by-product of a transaction
- School or whatever can have its own exhaust but it's problematic to have this big database that cuts across all the systems.
- Medical system: can have access to all anonymized data to use. Source data. Not the infrastructure data.
- What is the minimum set of information that needs to be logged is the question. Is there a minimum set of logging? Depersonalize them. Anonymize them. Is there a set of criteria that minimizes the data created?
- We do not want to generate more data from data. Like VISA generates a lot of data and can sort of tell when your card is stolen. But…
- We haven't heard of anyone duplicating a card. Fraud. There could be a clone card. We don't need to know what system they are accessing normally. We just need to know that the credentials are appearing in multiple locations.

- Example: I go to doctor A and say that I have diabetes and need prescription. And then go to doctor B and say the same thing and get another prescription. If I go to two different pharmacies will they know?
    - Yes. This already happens in the pharmacy system. It is connected. Pharmanet has this infrastructure to deal with this. They have all the info. But it is a completely different system than the identity system
- But this is totally different than the hospital knowing you bought booze before you got into a car crash. This is knowing too much.
- Medical system is different than identity system. In the medical system this is to protect the patient. Alarm is raised not when the doctor's are visited. But alarm is raised at pharmacy level. Health care system.
- Centralized identity system has worse information than the medical system. They should not be making decisions based on their information.
- Is this conversation specifically around fraud or is there a larger conversation?
- Larger: what should be bundled together and what shouldn't. Planning process. Personal opinion: as public services orgs, we don't have good info on which to make decisions.
- There are opportunities here to ask questions on what data interactions create connections that we hadn't seen before. Data helps our services. It can create a new kind of interaction
- Example given by facilitator: School registration: Imagine a different way to look at schools and then register. If it becomes way more automated then it gets more interesting once kids are in school. Resource management. Easier to sign up for field trips. Sign up for French immersion, etc.
- Data stored in a school system is richer BUT this does not need to use identity system.
- But it is easier with the identity system, it will lower the friction. But you don't any new data exhaust within the identity system. Because then we are looking at statistics about who is signing up where and have so much info.
- Law enforcement angle: all the different entities have information and police currently have to go to each individual one to get information. But if there is more data exhaust in the identity system then the police can just go there and say what's Joe up to?
- Now they have to figure out who to ask information about Joe from which is good. If they think there is a drinking problem they have to go to the liquor store and ask. They shouldn't be able to look at your personal info that you have gone to the liquor store.
- But some companies/entities already retain some of the data this way. Banks can tell if you do something suspicious to protect against fraud.
- Is the liquor store example valid? If you don't do anything wrong—you can't get into much trouble accessing services.
- But it's problematic to say that you won't get in trouble if you're doing everything right. The government shouldn't have that information.
- Question about school registration. Do you give permission?

    - Yes, you choose to do this registration system that validates.
- Data BC: Strategic use of data within government. Is this the end to be focusing on, to be bringing together the parties to look at data?
    - Data should be anonymized. Like in health care data. We create good data to analyze health/disease. But it's not problematic because it's anonymized. University of BC anonymizes data.
- Hypothetic Question: What if there was a system that uses access card to see if someone is qualified to do a job. To validate a professional credentials or training. Has the individual gone through training?
    - Again you can validate something but still have it be anonymous. You don't need to share someone's name for this.
    - Right now the system doesn't exist. There is the identity store but nothing is there.
- You can ask the identity source one question. For example: is this person of drinking age. Or do they have a degree and are they certified by the medial board? You can do chaining where you can. Chaining: if you have three questions that gain you access to someone. So different ways to do that. Ask three separate question or just one source/broker that validates you but the problem is that this person who is not any of these sources sees all your data.
    - Makes someone uncomfortable- go to the source
    - Problem is that some system somewhere becomes aware of the answers to these questions. So while it's less convenient to ask three questions instead of one, you eliminate the middle-man.
- The endurance point: so do we still want to see the exhaust data? We should build a system that doesn't have it. So it can't be misused.
    - Can we ask the citizens if they want to contribute the information?
        - Issue is when people don't understand what is going to happen?
    - But is shouldn't be the identity system. Should we build this option into the identity system?
    - What happens when government wants to become more proactive like Netflix—tailoring data to you.
        - Issue is of choice. I don't have a choice of government unless I move. I have choice of Telus. Or Netflix.
- Still question is will the data exhaust be productive? It could simplify life in many ways. I'm not sure we need the exhaust data to support that. But I'm worried about getting driven out to silos again.
- Something that could help. Can better align services because different agencies can share data more easily. Doesn't necessarily mean that there is just one database that is all accessible.
- When you talk about doing a privacy assessment: someone will come forward with a good idea, we have to look at the privacy compliancy and we don't just say no, we try to look at what we can do. Can we anonymize this?
    - But this is a harder sell for the public.
- Pattern in conversation. There has been a universal response that we shouldn't look at the identity service to do this. But we can do this idea. Don't

throw the idea out because we shouldn't do it through the identity service but look at other agencies can do it.

- Issue back to choice. We have a choice with providers of almost anything, but we don't have a choice of government. We can technically opt out of Google.
- You are driven at privacy at it's heart but companies are trying to get there other ways.

Session 4.2: Is Payment Technology Appropriate for Protecting Privacy?
Facilitator Lead: Andrew

- This discussion questioned the premise that government should trust and use technology that was developed originally for banks.
- Participants argued that payment technology was never designed to protect privacy, only to protect the bank/credit card company from risk. Therefore, the government should not go to payment technology for a program that requires privacy to be central.
- "Data persistence is a huge problem and the question is what do they do with it?"
- "Possession of a card when I go to access a private service is two things, it's a thing you gave me, the thing is present, and I'm present. The thing and the secret in combination allow you to access goods and services. It's about this chain of custody and data and trust. We need to tease these things apart. We need to know what the Government is going to tell someone else when you get involved in a transaction."
- The conversation then shifted to a detailed explanation by Ian from the BC Government about the analysis and selection process his Ministry used to pick this particular technology. He explained the factors they considered when shopping for card technology and the different options they tested. He told the story of how they finally came to choose this card technology over the others. The process took about 4 years and was extensive. Ian's key points:
    - The reader is so small that you can put it in the mail.
    - Cost per unit on the reader is about $5 per reader.
    - We did about 4 years of research at least.
    - We studied cards from many different countries.
    - The intense choice process was about 6 months.
    - Visa and SecureKey is not getting any info.
- Unresolved Questions:
    - Is payment technology appropriate for privacy protection?
    - Is a proprietary algorithm sufficient for protecting privacy, when it hasn't been independently tested?
    - Are you willing to accept the risks that you don't know about?
    - How do you ensure that the citizens know that we've done our diligence and that the 3rd party contractors are also doing their diligence?

- What are the reasonability tests associated with divulging your info online?
- What about when the technology becomes obsolete?
- We started with the premise that privacy isn't refundable, what kind of recourse do we have if our privacy rights are violated?

Session 4.3: Experiencing Identity: frictionless service with identity awareness
Facilitator Lead: Gordon Ross & Alex MacLennan

- In the practice/profession of user experience, it is often assumed that the best experiences are "seamless" or "frictionless," with "invisible design" being seen as inherently desirable. Some of this was heard in presentations on Day 1. The facilitators discussed the reasons that the assumption of this as a self-evident good is problematic (drawn from the work of Timo Arnall[2]), including:
  - it makes technology seem immaterial
  - it perpetuates the myth of "natural" or "intuitiveness"
  - it ignores interface culture
  - it ignores the history of technology and design
- Other examples cited include redesigned Residential Tenancy Branch dispute forms that are so streamlined that their users don't resonate with their status as formal, legal agreements.
- Two participants agreed with the goal of making experiences frictionless and seamless, while allowing for the fact that more information may be needed in some situations (such as when initial authorization is being granted) than in others (such as when a person is engaged in a recurring action, or can be reasonably defined as a power user). Experiences ought to adapt for "learnability".
- One participant emphasized, departing from Arnall's argument, that there is "no universal context" — that a person's comfort level with an organization, an interface, a set of knowledge or a task will always be influenced by a wide range of factors, some of which can be anticipated by designers but many of which cannot. This person emphasized the importance of empowering users as much as possible to self-identify and reflect on their comfort level, and to adjust the speed or friction accordingly.
- Participants concluded that designs may often be bias towards features or defaults that stack the deck to lead a user to pursue certain desired flows of action. With users used to "just clicking agree" to actions put before them, tools may encourage them to remain ignorant about their rights and responsibilities within transactions. The "friction" existing in current practices (such as handing a card over to a worker) serves purposes for users. Understanding how to continue to fulfill these purposes in the course of design interfaces will affect the various qualities informing trust.
- Other participants noted that in situations where they felt a high degree of control and empowerment and viewed interactions in a goal-oriented fashion, the experience of seams (such as in the School Enrollment scenario demonstrated on Day 1, when the

[2] "No to No UI", Timo Arnall. March 2013. http://www.elasticspace.com/2013/03/no-to-no-ui

identity task was being graphically negotiated with the School website) may be disconcerting, unwelcome or undesirable.

- Several participants agreed that existing service experiences are open to a broad range of interpretations that may colour their openness or willingness to learn the new procedures associated with the BC Services Card; for example, users and employees' differing views on what goes wrong and right in service experiences, ambiguity in connecting people with problems with people who can do something about it ("The Amazing Race"), and the impact of varying levels of visibility that users desired or are accustomed to having across service processes.
- Participants noted that the Demo on Day 1 started from the middle of an experience (assuming a relationship already existed with the school) instead of the beginning, which may have affected how well it was received.
- Governments are in a different position than private application developers, and some way of balancing "hand holding" or wizard-based approaches, with interfaces suited to power-users, is needed.
- "Seamful" experiences can be important, to allow individuals to feel empowered by always knowing where one was in the process, what was required at each step, and to have mechanisms and supports close at hand preventing negative surprise or incident.
- The existing framing requires people to agree to full disclosure of requested information ("attributes") to receive a service, or to refuse it entirely and not get what they want — a "cooperate or defect" approach. This situation could be greatly improved by introducing some mechanisms for nuance, or at very least explaining why giving the information is required.
- Outstanding Question:
    - Are there procedures or other mechanisms in place to ensure that designers of transactions involving identity are thoughtful in ensuring key empowering steps are not de-emphasized in favour of seamlessness"?

Session 4.4: What safeguards are in place to make sure that the government protects our private data?

Facilitator Lead: Karyl Olstad - member of Citizen User Panel

(Two note takers were present in this session)

Note taker 1:

- The group had discussions on what happens if there's a change of government? How are databases going to be connected in to the identity system? What is the on-boarding process?
- Citizens need to be educated around the choices that are involved with having databases accessed through the same BC Services Card portal.
- Currently these various systems are not designed to work together. I.e. the databases are not designed to share information.
- A government official stated that in order to connect the database to the BC Services Card portal, they first have to have the authority to do that. Organizations like ICBC and WCB have legislation that they must follow, and law enforcement have certain protocols that need to be followed if they were to

want access to any of the databases. Finally the Privacy Commissioner will need to be involved and evaluate any changes in connectivity between databases, prior to implementing any changes.

- Participants wondered: could ICBC use private medical information against me in a claim? A government official said Private medical information remains in your doctor's office. ICBC will not have access to your private medical records. Health records and ICBC remain completely independent data sets. ICBC could within the current structure (before the existence of the BC Services Card) formally request your medical records and this will not change.
- A discussion was had about access to federal services. A BC government representative said, “In four more years we will have the majority of British Columbians using this card and the only way that we would share info outside the province is if the majority of British Columbians started asking us to use a service that require our sharing data. Then we'd have to reassess and come back to answer that question. Not only do we believe we have safeguards in place to protect your identity and information but we believe that our safeguards in this card are better than the ones we have right now.”
- Government officials communicated they felt there was an opportunity to do these services better, relating to driver’s license authentication applications e.g. bar watch.
    - Gov rep told story about how a girlfriend got carded at a bar and then the bouncer at that bar contacted her later using the info on her drivers' license. “That bouncer does not need to know her name or address. That bouncer only needs to see her picture and a checkmark that should that she's over 19. No other info is needed and that's what the BC services card will provide, just the basic info needed to establish identity.”
    - Another example is education. Now, if you want to enroll for education, you come to the office and you give them your driver's license. They'll take that information and they'll record all that information about you in their system. And no one is there to say how much is needed so often they'll take a little more information than they need and no one is there to tell them not to. Being as they are under the regulatory framework, we would hope that they then keep that info to themselves but nonetheless, there is no one there standing over them to make sure they don't take more info than they need and do what they will with it. I would argue that the BC service card would provide that regulatory restrictions and framework to prevent people from taking more than the absolute minimum. And they'd actually collect less information than others are doing now.”
- Participants discussed the idea of communicating to the public that this identity system is safer than those currently used.

Note taker 2:

The group asked questions about and discussed the safeguards that the government has and will put in place so that citizens know their data is not ending up in unintended hands. This group was organized by Citizens' User Panel member Karyl. At the end, she

said she was reassured that the government is working to protect her data and make sure it's not ending up in unintended hands. She said her worries were alleviated but that she would continue to interact with and ask the government for continued information. In particular, she wanted to make sure that successive governments would not reverse police all of the sudden, and use her data in ways that we are not envisioning now. But overall, Karyl said that she thinks the government has a higher standard for data security than what we have now.

- How can you assure me that the info you're taking from me now won't be used for a different purpose later? Maybe by a different government or a few governments from now? How do I know they won't use my information for an originally unintended purpose?

- BC government representative: "In four more years we will have the majority of British Columbians using this card and the only way that we would share info outside the province is if the majority of British Columbians started asking us to use a service that require our sharing data. Then we'd have to reassess and come back to answer that question. ... Not only do we believe we have safeguards in place to protect your identity and information but we believe that our safeguards in this card are better than the ones we have right now."

- Gov rep told story about how a girlfriend got carded at a bar and then the bouncer at that bar contacted her later using the info on her drivers' license. "That bouncer does not need to know her name or address. That bouncer only needs to see her picture and a checkmark that should that she's over 19. No other info is needed and that's what the BC services card will provide, just the basic info needed to establish identity."

- "Another example is education. Now, if you want to enrol for education, you come to the office and you give them your driver's license. They'll take that information and they'll record all that information about you in their system. And no one is there to say how much is needed so often they'll take a little more information than they need and no one is there to tell them not to. Being as they are under the regulatory framework, we would hope that they then keep that info to themselves but nonetheless, there is no one there standing over them to make sure they don't take more info than they need and do what they will with it. I would argue that the BC service card would provide that regulatory restrictions and framework to prevent people from taking more than the absolute minimum. And they'd actually collect less information than others are doing now."

- Same with authenticating your address, the BC service card could authenticate your address without actually revealing your address.

Session 5.1: Service Card for B2B/B2G. Worksafe Perspective

Facilitator: Jens H

- The group identified a central question to be whether people should be using their personal identity data in your workplace and if they want to be linking the two? That is giving a lot of power to one card and potentially merging personal identity and corporate identity.
- There was not necessarily agreement or disagreement in the group, just potential concerns.
- The group talked about a potential feasibility issue of a workplace card as often workplace IDs can require much more out of the card than the service chip is designed for. It might involve redesigning the service card and this is not necessarily going to be done by the government.
- Several people were concerned about privacy and asked if the card could be used for authentication only? Also, they identified the need for an option to opt out of having all their information tied to one card.
- Another issue that came up was the fact that it's not just giving the card itself power, but is all our workplace and personal information going to be linked in one system/database. Many people did not think the public would like that.

Session 5.2: What do digital identity services enable for me?

Facilitator Lead: Alex MacLennan

- Participants in this session were primarily interested in understanding what is desired by, and in it for, the end user.
- Speed, ease and convenience of service; security of information; and simplifying the interaction with bureaucracy – especially during stressful major life events were all common interests expressed by potential end users. One quote seemed particularly apt in capture the sentiment of end users: "I want to be able to access services in my pajamas."
    - "When life is smooth, there isn't significant interaction with the government but the biggest life events, having a child, marriage, divorce, buying a house, caring for someone, having a death, then we start to interact with multiple levels of government and that's when it gets complex and frustrating."
- Participants in this session also imagined a number potential improvements to service delivery methods enabled by this card including:
    - scheduling appointments for service online instead of taking a number upon arriving at a service location;
    - being able to access medical records online (E.g. prescribed medication information, and immunization history of dependents)
    - Digital payment for license plate renewal stickers to avoid the lines.
    - Vital signs monitored online, real-time by someone at a nursing station (a participant explained this is done in Ontario).
- The group identified the following as the benefits of digital services:
    - quality
    - sense of security
    - ease – "access in my pajamas"

    - on my time
    - on behalf of others
    - simplify complex interactions
    - government as a platform – build community
    - time frames – better responsive, less anonymous but safeguards; self-service
    - one stop
    - 24 hour access
    - geographic access
    - non-explicit – safe road
    - liquor stores
    - Revenue Canada; Canada Post; property taxes
    - licensing
    - research
    - open data provided by the government; library
    - schools
- While participants did envision major improvements possible in service delivery, they also recognized that this one card was not going to be a panacea and should not be over-promised.
- Participants also felt that government should proceed carefully in considering changes to service delivery methods.
- "I think a lot of the problems discussed here today are inefficiencies. Digitizing something may not cover all the inefficiencies. Solving all these problems with a service card is over-promising."

Session 5.3: How did this work for you?

Facilitator Lead: David Hume

- The facilitator sought feedback from conference attendees on how Identity North served them, what concerns if any they had, and what they might propose doing differently for future events.
- One participant, a third-party vendor with experience working with APIs from government bodies, expressed broad approval for the way the event achieved its goals for deliberation on various topics. The participant was positive on the format. This was coupled, for the participant, with some concern, based on their experience with previous consultation processes. In this participant's view, the open space format was limited in its ability to reassure participants that they had an active hand in observing the government moving through "the ladder of inference" from observation to conclusion, then to recommendation. "It is important to get some consensus — that that is how we said what we thought we said."
- That same participant shared knowledge from their own facilitation expertise, recommending techniques around story or anecdote circles that allow for exchange of experience; followed by a group signification process; ending with multiple rounds of clustering ideas and themes collectively while soliciting agreement throughout the day. These methods, it was argued, support the goal of

emerging with rich archetypes and coherent, broadly-bought-into outcomes that can be tested and re-tested with participants in a different way than the unconference does.

- Another participant, a member of the citizen user panel, comment: "The science and technology are done by the people who are good at it. The User Panels can give a sense of its worth." This participant felt the day was centered a lot on risks and security vulnerabilities, while seizing less upon the opportunity to present a vision of opportunities and benefits associated with the BC Service Card. Another participant agreed, saying that for citizens, seeing non-expert peers navigate the consideration of tradeoffs can be positive and helpful.
- For the event convenors, the event has not typically been part of a project timeline as this Identity North event has been, with regards to the BC Government's consultation timeline. A significant amount of learning about what could be changed/improved is likely to result.
- The event convenors are receiving suggestions by e-mail (contact@identitynorth.ca) and compiling a reading list to distribute to participants to facilitate further learning.
- Timing and the public discourse will matter significantly in collecting user feedback — a participant shared their experience of launching a service, where general satisfaction for the service (affected by the broader conversation) collapsed for factors unrelated to users' ability to and comfort with the service.
- It is very important that the government work closely with event convenors and reporters on providing "traceability" — ensuring that the recommendations are well-connected with statements and discussions at the event. Releasing the raw, unedited notes was presented multiple times as a way to do this.
- What the law means, as well as what the law means to citizens, ought to be the key driving factors determining how services are built.
- The Identity 101 session may be too low-level for some of the attendees, and may be best left for citizen user panel members to experience separately.
- Are there any important outstanding questions that remain unresolved?
- Will there be opportunities for event attendees to examine the outcomes of and recommendations from this process before they are too "set in stone", in order to avoid awkward "forced" buy-in due to the momentum of the work?

Session 5.4: I'm from BC but I don't live here. Can you help me?

Facilitator: Kaliya Hamlin

- This discussion explored the potential for the BC Services Card to serve as a primary ID document for non-resident British Columbians who do not require services from the BC Government.
- It was suggested that the BC Services Card should have an option for "Birth Certificate Only" (no services) so that people who were born in BC but don't live here could use the card as a way to prove their identity (verified attributes).

- The government officials explained that at the moment they only issue BC Services Cards to residents who are entitled to services (MSP and ICBC) but that in the future there is a potential for a "Birth Certificate Only" option.
- It was suggested that BC needs a Document Verification Look Up service like they have in the USA.
- The facilitator stated, "The BC Government is authoritative for my attributes but I don't want services. I just want my attributes. I want to be able to use my birth certificate in my digital life."
- Unresolved Questions:
    - What if I move?
    - What if my ID is from somewhere else that is highly suspect?
    - What if I split my residence between different jurisdictions?
    - What about snowbirds, university students, refugees, people who travel to BC frequently etc?
    - Why is context separation important? Is it important to a younger generation?
    - If you leave and come back would you get a new BC ServicesCard?