IdentityNorth Specialist Forum Proceedings

A Component of the Digital Services Consultation

Prepared by MASS LBP on behalf of the BC Ministry of Technology, Innovation, and Citizen Services and IdentityNorth
December 2013

BRITISH COLUMBIA | Ministry of Technology, Innovation and Citizens' Services

IdentityNorth

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 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 also 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 really is 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 functions 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?

The IdentityNorth Specialist Forum is one component of the Provinces' Digital Services Consultation. The balance of the consultation process includes a BC Services Card User Panel of 36 randomly selected residents 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 online survey open to all.

The IdentityNorth Specialist Forum ran for two days and was attended by delegates from the technology sector, civil society, academia, the public service and members of the BC Services Card User Panel. The Forum 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 it has built a safe and privacy-enhancing system for accessing services online. But in hosting this conference, they encouraged participants 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 participants. While Day One of the conference was structured around presentations by government representatives and leading experts in privacy and online identity from around the world, Day One also involved plenty of ongoing discussions, as participants 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 participants were able to explore issues of their own choosing, discuss the finer points 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 conference participants 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, participants 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 participants expressed strong concern about linking federal government services with BC's identity infrastructure. BC government representatives responded by assuring participants that the only way BC would share information outside of the province is if "a majority of British Columbians asked for a service that required doing so."

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

There was no broad agreement however, on how any potential use of the Services Card by the private sector should be regulated or monitored. How would standards be enforced? How would privacy be protected? Some participants 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 one. 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 Services Card and its Identity Assurance Service.

Government representatives informed participants that, at this point, BC is focused on services within its own ministries and agencies – not in the private sector. Several participants from the private sector noted that, in the absence of clear government policies on non-governmental uses for the card, most companies would be unlikely to invest in developing potential applications for the 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 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 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 participant 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' so that 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 and aggregation is actually already technically possible under the *current,* pre-Services Card system, but requires 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 felt these questions deserved further attention.

Some expressed concern that, as more services start using the Services Card, the

[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.

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 participants 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 participants 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 in-person services 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 in-person services, as they always have. Some representatives worried that should online services be widely adopted by BC residents, this would inevitably cause a reduction of in-person government services. People who want to access in-person services (potentially for privacy reasons) could conceivably face increasingly large barriers to doing so, especially in rural areas.

Government representatives asked participants whether the Identity Assurance Service should be configured so that individual BC residents could pull up a centralized personal usage record. Though conference participants could see the benefits of this feature — for example, as a way for BC residents to check up on whether there has been 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 appropriate, 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 participants 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 participants expressed the sentiment that it is difficult to accurately assess the risk of the Services Card without knowing what the infrastructure would be used for. They suggested that risk would have to be assessed 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 participants 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? Participants 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 which 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 to addressing them, many conference attendees focused on how government could build public trust in the 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 need to address the needs of all three groups. Group one covers those who are highly suspicious and want all 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 includes those more focused on the benefits of the 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 this as an 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 robust 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 should to be readily available for those with particular concerns or suspicions. Transparency, they suggested, would go a long way in reassuring critics.

One group of participants 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 participant 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." Participants suggested that the 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 participants 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.

Summary of Plenary Proceedings

DAY ONE

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 began 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 organizations like Yahoo, Google, and Facebook. Typically, in order to access services these entities require authentication or a log-in of some kind. Through these log-ins, we build an online identity spectrum. Sometimes we use pseudonyms, or made-up user names (for example, YouTube); sometimes we use our real names, as validated by friends or colleagues (for example, 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 were recurring themes throughout the conference. Hamlin asserted that the technologies for maintaining limited liability need 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 enhances online experiences.

The presentation concluded with one participant question, about Hamlin'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

With 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, IdentityNorth (founded to bring together the public, industry experts and government) and expressed support for what 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.

Deputy Minister John Jacobson outlined the two broad tasks for conference participants. First, to challenge the government's 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 remarked 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, Chair, The Open Identity Exchange;

Kim Cameron, Architect of Identity, Microsoft;

Krystyna Hommen, President and CEO, Excelleris;

Andre Boysen, EVP Marketing, SecureKey Technologies

Panelists discussed how, in an era of declining budgets, this expanded infrastructure could allow government to meet increasing service demands. For Excelleris, a private-sector business providing health services, the card "provides an opportunity to enhance services," noted Hommen. Participants heard there is tremendous demand in the private sector to access health services online, and a recognition in the health sector that there needs to be upgrades to those tools. "The public is asking for these kinds of things." In addition, delegates heard that the card also offers an opportunity to "get beyond user names and passwords." One panelist noted the password reset problem was one 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, participants also heard that "the card isn't the magic thing, it's the whole infrastructure of what the card gets 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: 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 have access to 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, participants heard, it was built with the notion of proportionality; the ability to allow people to give up only those elements of their identity required "to get what they came for today."

Panelists noted that one challenge is creating a mental model to communicate to people that this is the case – that one card can act as many cards within the digital system. The only way to

guarantee contextual separation, suggested one panelist, is to have a "provably blind" technology that does so mathematically. Ian Bailey, BC's Chief Technology Officer, responded to concerns about contextual separation by affirming that government legally cannot connect databases without explicit permission. At the end of this session some delegates still questioned whether the public could trust the government not to link databases 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 in the system as it is currently envisioned; and the potential for privacy and security threats as the card evolves and possibly becomes used in the private sector.

One self-identified "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 participant described it as a "very nice Cadillac" of an identity system that now has to determine where it wants to go. Several participants expressed concern about "function creep" -- the notion that the system could gradually take on more uses and with each new use the security and privacy risks would rise exponentially. One participant noted that since the advent of Health Canada's electronic health record systems, that department has seen "a lot of pressure from the private and public sector to use its information for secondary purposes." Colin Wallis noted that, from the New Zealand government's perspective, businesses are taxpayers that have the right to be able to consume that data responsibly.

In response to security threats generally, one participant 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, the province's Chief Technology Officer, noted that the information security branch is required to undertake a Security, Threat, and Risk Assessment (STRA), although it's uncertain at this point whether that will remain internal to government, be released to the public, or be released to select groups. Government is planning to have a third-party review these risk assessments, and are waiting for the results of this group consultation to determine how best to handle STRAs.

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

Gogolek and 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, they noted, but the context and the hierarchy of values can change. This led

into an open conversation with conference participants about what identity means to different people.

A 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 participant 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

Presented by Raphael Diaz, North American Strategic Engagement Lead, GSMA

Diaz introduced GSMA as a trade association of mobile industry and mobile users worldwide. He told participants that the industry needs secure digital identity and authentication services because "everything is converging on mobile." Participants heard that mobile phones make sense as an identification device because they are portable, they stay with users most of the time, and they are 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.

Diaz explained that using one's phone as a portal to access all kinds of services is appealing to their UK market because it means 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 have the same login for hundreds of third-party websites.

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

During question period, some participants 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

Presented by 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. Participants heard that initiatives are no longer mostly government-led, that there is an increasing amount of specific legislation, and that they are beginning to become optimized for mobile devices.

He described New Zealand's experience building two foundation services that are centralized but separate: a government login service, and a government identification authentication service

called RealMe. The former is pseudonymous, merely confirming "you are the same person as the last interaction," while the latter is a "triple blind" identity assurance service that confirms a users' identity from an internal affairs verification service. "No one part of the system has all the information to profile you," he noted, so that information can't be aggregated in a way that gives "all the keys to the kingdom away." Participants heard that while there have been "plenty of transactions," there are only 1.16 million total citizen login accounts -- less than 30 per cent of the population. There are even fewer RealMe accounts -- 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 extremes of consultation: the first is a genuine attempt to build something together, and second is 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," he noted.

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, Chief Technology Officer, Province of BC

Schlosar opened this session by sharing his own family's 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. He described how BC's new identity infrastructure is about augmenting what government already does; it is about expanding services and increasing "stickiness" so users come back. That means thinking about service as a journey with "quality at each step of the way."

Schlosar described the Services Card as "a chip-enabled card that can be used to securely access government services online and in person." Its main purpose, participants heard, is to replace the CareCard, and it was developed by three organizations (the Ministry of Technology, Innovation and Citizens' Services, the Ministry of Health and the Insurance Corportaion of BC) over the past 12 years. So far, just shy of 700,000 cards have been issued: 130,000 are non-photo, 250,000 are combination cards, and 350,000 are stand-alone cards. The speakers reiterated the questions government is seeking answers for as it proceeds to the next stages of implementation. What services should be accessed first? Should government draw on the Services Card usage data to improve policy and services? How else could the Services Card be used by non-government organizations to improve the lives of residents?

Bailey described some of the details around the architecture of the card. The biggest decision, he explained, was settling on the EMV contact-less chip, after determining it was cost-effective, secure and commercially available. Bailey demonstrated how the card works by using it to access a school district website in a mockup demonstration. The demonstration prompted some questions from participants, who were mainly

concerned that the school district website showed card history. Bailey reiterated that this was a mockup and didn't mean the features were set in stone. There were also concerns raised about how the school district (or other entities) would be able to protect the information given in these transactions. This was identified as an area that would required work in the future.

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 raised a series of questions she felt were key to the process, but which remained unanswered for her at the end of Day One. How would the government use the public consultation? What could the government learn from the low adoption rate in New Zealand's identity program? What could government learn from the rollout of the smart metering program or the Harmonized Sales Tax? Sinclair reiterated a point raised earlier in the day: whether the program was 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, I would want to see PCI (Payment Card Industry) certification to know you've done due diligence. Where is that with government?" She also raised the issue of contextual separation, and expressed concerns that anonymous linkages could be undone "by force of law." One participant echoed her point 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, with:

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 Thibeau, Chairman of the Open Identity Exchange.

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

Thibeau told participants that "identity is the issue of our time." He noted that US companies will take a long time to recover from the Snowden disclosure, a factor 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 participants that he felt the next challenge for leaders in this sphere is the mobile device sector, and that clearly that is "the platform of choice."

Munro highlighted this as well, and pointed 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 consumer 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." Participants heard that passing information between customer and business comes with risks. "Facebook and other great companies... make their business on your data." The big question, Munro noted, is how to give information to someone but keep it protected.

DAY TWO

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 Services Card. The fact that there are many more usable CareCards in circulation than residents in BC is a big problem for health records as well. The Services Card is meant to give British Columbians a more trustworthy form of identification, one that is less "clunky" than a birth certificate or passport.

Wilkinson 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 Services Card to a bank card – that it 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 many privacy agreements online.

"It is not our role to facilitate junk mail and banner ads." He told participants that government wants to put out a safe and valid menu of service options for people to consider. Participants 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.

Following Wilkinson's' presentation, a participant 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 online services on the BC population, people who "expect their rights and autonomy to be respected." Wilkinson added 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."

Breakout Session Summary 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) would be the only benefit, since this is not currently possible.
- In the physical world (for example, for building or locker access) everyone agreed that there would be benefit because physical access is normally high friction.
- There was debate about whether people would need to use the card frequently before they are used to it enough to benefit from the authentication system. Otherwise it could just be a new thing that they will need to learn. Would they have to use it to get in to a government site, for example? And if so, would it be 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 Dan Hall framed the discussion around the relationship between one's self, one's community identity and one's identity within the state.
- 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 Services Card does not do this, this happens frequently 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 access might look like.
- Participants saw great value in the possibility of using 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.)
- The concluded that 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?

- In this session, participants presented ideas about how to, not just make the card secure, but how to make people *trust* that it's secure.
- Discussion focused on the challenge of explaining technical and policy changes to the public audience.
- Facilitator Patricia Wiebe emphasized that the public needs to have their choices and the risks clearly explained to them.
- Participants were concerned about jargon and technical language that was inaccessible to a wide audience (for example, "unidirectional linkages," "polymorphism," "trust framework.")
- However, participants also noted there will be a small number of people – "identity geeks" - who will want to know the complicated and detailed information about security features.
- Participants saw a need for a whole package of targeted messages to reach a diverse audience, all of which assure users that no personal information is stored on the chip itself.
- They felt the messaging should focus on "Keep It Simple Stupid" and "What's in it for me?"

- Participants noted that "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." They felt government should be careful about making it too easy for citizens to give up information and felt that users should have to consent to authentication and use of identity information every time they log in.
- Participants strongly felt the default should be the minimal amount of information shared.
- Participants brainstormed 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
  - An analogy is needed to explain that there is no central database.
- Unresolved questions:
  - Should government track transactions so they can provide citizens with a log?
  - Can we build the system to forget out data?
  - How will government monitor the private sector 3rd party contractors who are connected to the BC Services Card?

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

- Participants identified a lack of knowledge and uncertainty about the authentication process.
- A government representative pointed out 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.
- Participants discussed that if organizations use recognized standards then it is possible they may be protected from legal liabilities.
- Some participants expressed concern that most people would assume some of these issues are being taken care of, yet many of these issues remain to be addressed.
- Some participants stated that they are not aware of a better system, but acknowledged there are risks with every system. "Can we trust this system to be rock solid?"
- Participants recommended that the BC government, as the authority of the Services Card, could be the assurer of data and information.

Session 1.5: No universal identifiers

- Facilitator Patricia Wiebe and colleagues used this session to explain, provide further clarification and to describe the strengths and privacy benefits that informed the decision for the Services Card not to use Universal Identifiers.
- Facilitators identified differences concerning the use of the word 'consent' — it has specific legal and policy use and also connotations in informal conversation. Participants sought a deeper understanding of how citizens were indicating what actions they did or did not "consent" to; government 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). Government representatives 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. Government representatives offered deeper explanations 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:
    - Are chips in cards were vulnerable to 'skimmers' (as widely rumoured online)?
    - Are chips in cards were vulnerable to physical attacks or 'man in the middle' attacks in the communication layers?
    - Could chips could easily be cloned, through exposure at the hardware manufacturer level?
    - What procedures and protocols were involved during chip personalization?
    - What is 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 Services Card. Facilitators acknowledged the value of this.
- Some participants 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

- In this session, led by facilitator Gordon Ross, participants frequently returned to a theme of the state reducing a person's complex identity to an overly simple, codified identity. A government representative 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.
- One participant wondered if the province approaching this from a stance of "We have a hammer, now what are the nails?" and questioned, "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.
- Although 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

- This session built on the Identity 101 session from Day 1 on "The Valley of User-Centric Identification." Facilitator Kaliya Hamlin 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.
- Hamlin also 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. She described "peasants" — individuals being manipulated into providing their habits and data for someone else's largely financial gain -- who receive little protection or attention and remain largely unaware of how their data is being used to shape their online and offline experience.
- Hamlin 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 Services Card -- designed to keep information from being linked together "behind the scenes" without permission of the individual at the centre of it – is significant in this context. 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.

- Participants felts 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

- This discussion untangled the idea of verified attributes and explored the role government should be taking in providing credentials to citizens. Facilitator Andrew Hughes challenged participants to question why government takes the lead role on verifying identity when it could be contracted to a private specialized company.
- Participants explored how individuals through the Services Card can control information flow. They discussed the idea of identity as a set of attribute. "In the online context you need a protocol to pass those attributes over and you need trust."
- Participants agreed that the consultative process is valuable, that policy has a major role to play and that trust is at the core of this issue. They discussed how 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 government to connect to the BC Services Card will 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?

- Discussion focused on 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.
- Participants agreed that a major reason to track how the card is used is for fraud prevention.
- Facilitator Ian Bailey acknowledged that people want better control over their information, and government has 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. Participants agreed that there needs to be enough trust to get people to start using the card, although the question arose of how we get people to trust that the government in keeping their information secure and not abusing their own power.
- Participants felt the question of how the data is kept needs to be reviewed. Bailey pointed out that there are different options in terms of how long the data is kept. Government itself could keep that data, or a third party could deal with data, or people could opt out of having their data stored to maintain their agency.
- The group felt 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

- This session opened with the question: how does a service in Ontario create something new on a platform developed in BC to be used somewhere in Nova Scotia? And how could that process benefit each of the 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.
- Participants heard that an ecosystem provides continuity for innovation within which there are boundaries of acceptable use.
- Some participants focused on how to create a better framework for collaboration (to create identity services that could be used with the 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) but not necessarily the what (more the role that they play, or roles, or other personal information)
- Participants identified barriers to identity ecosystem:
    - 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 information from province is not available to private companies
    - A lack of trust and non-participation
- 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?

Session 3.1: The lifecycle of data

- This discussion focused on the question what happens when a person dies or wants data taken down. Participants noted that data doesn't die, and that there is no refund on privacy when it's infringed upon.
- Participants wondered how services would operate on a case-by-case, service-by-service basis.
- Participants showed a lot of concern that the 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.
- Although it was noted that the BC Services Card would not be a centralized bank of information, participants expressed concern 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?
- Participants made recommendations that the government should make sure that people who choose to opt out are not left behind and that government should focus on improving the general delivery of services and not only moving services online.
- Participants discussed the benefits and risks of the potential of data linkage and wondered how to protect data from being misused – should monitoring occur?

Session 3.2: Is this actually optional or is it mandatory?

- Participants felt that there is a deficit of public confidence in what is being done, and agreed that more transparency is needed. Facilitator Colin Bennett emphasized the 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 in 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. 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

- This discussion was facilitated by citizen user panelist Dan Hall, who expressed concern about the physical security of the places where data is stored or accessed. A government representative explained that data centres are protected from all forms of disaster, damage, loss or theft and that the government uses a variety of security mechanisms to protect personal information of British Columbians.
- Participants searched 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 expressed 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: The power of data: How to approach using data for service and policy improvement

- Participants in this group were concerned that government monitoring of identity is problematic and centralized data can lead to government and law enforcement having too much information. Several participants expressed feeling uneasy about the potential level of surveillance and how it could lead to the criminalization of individuals.
- There was general agreement that government should anonymize all this information, as we currently do with the medical system, because this allows for protection of 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 participants agreed that this could 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 to achieve this.

Session 4.2: Is payment technology appropriate for protecting privacy?

- This session 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, government should not go to payment technology for a program that requires privacy to be central.
- Participants felt there needed to be more clarity around chain of custody. "We need to know what the government is going to tell someone else when you get involved in a transaction."
- Ian Bailey offered details 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. Bailey'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 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

- Facilitators Gordon Ross and Alex MacLennan described how in the practice of user experience, it is often assumed that the best experiences are "seamless" with "invisible design" being seen as inherently desirable. They discussed the reasons that the assumption of this as a self-evident good is problematic: it makes technology seem immaterial; it perpetuates the myth of "intuitiveness;" and it ignores interface culture. Participants cited examples like the redesigned Residential Tenancy Branch dispute forms which 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 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. They 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 might often be biased 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 were 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 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, and the impact of varying levels of visibility that users desired or are accustomed to having across service processes.
- Participants noted that the demonstration 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.
- 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.

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

- This session was organized and facilitated by Citizens' User Panel member Karyl Olstad, and focused on questions about the safeguards that government has and will put in place so that citizens know their data is not ending up in unintended hands. Participants felt strongly that citizens need to be educated around the choices that are involved with having databases accessed through the same Services Card portal.
- A government representative emphasized that currently these databases are not designed to share information and stated that in order to connect the database to the Services Card portal, government would need to be authorized to do so. 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 would need to be involved and evaluate any changes in connectivity between databases, prior to implementing any changes.

- Participants wondered if ICBC could use private medical information against an individual in a claim. A government representative responded that ICBC will not have access to private medical records and that 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.
- Some participants were curious about access to federal services. A BC government representative noted that, "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."
- Government representatives communicated the card offered the opportunity to provide services with more privacy; that the Services Card would provide the regulatory restrictions and framework to prevent people from taking more information than the absolute minimum.
- Participants discussed utilizing the Services Card within employer's facilities, and that this could possibly enhance the employee/employer relationship. However, some disagreed with having to use confidential Services Card information to be displayed prominently in a workplace (i.e.) replacing employee IDs with this new service card.
- There was also discussion of the concept of having multiple identities showing up on the cards so that professional practice versus your private name can remain separate.
- By the end of the session facilitator Olstad said she was reassured that the government is working to protect her data and make sure it's not ending up in unintended hands, and 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 policy, and use her data in ways not envisioned now.
- Unresolved questions: Who is liable for the consequences of releasing data?

Session 5.1: Service Card for B2B/B2G, and the Worksafe perspective

- Participants identified a central question of whether people should be using their personal identity data in the workplace and if they want to be linking the two – essentially merging personal and corporate identity and potentially giving a lot of power to one card.
- There was not necessarily agreement or disagreement in the group, just potential concerns.
- Participants discussed potential feasibility issues 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 participants 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 would not just give the card itself power, but could result in all workplace and personal information being linked in one system/database. Participants agreed the public would likely not like this.

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

- Participants in this session were primarily interested in understanding what is desired by, and what's in it for, the end user.
- Participants discussed benefits of speed, ease and convenience of service; security of information; and simplifying the interaction with bureaucracy – especially during stressful major life events. One participant noted, "I want to be able to access services in my pajamas."
- Participants 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;
    - Ability to access medical records online (for example, 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.
- The group identified the following as the benefits of digital services:
    - Quality
    - Sense of security
    - Ease of access at one's convenience
    - Ease of access of services on behalf of others
    - Simplification of complex interactions
    - Enabling government as a platform to build community
    - One stop, 24-hour access, regardless of geography.
- Revenue Canada; Canada Post; property taxes 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 David Hume 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 and 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, commented: "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.
- The event conveners 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.
- It is very important that the government work closely with event conveners 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.
- Participants wondered whether there would be opportunities for event attendees to examine the outcoes 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?

- Kaliya Hamlin facilitated this discussion exploring 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.
- One participant suggested that the 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.
- Government representatives explained that at the moment they only issue 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.
- Another participant suggested that BC needs a Document Verification Look Up service like they have in the USA.
- Unresolved Questions:
    - 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?

Presenters

Richard Austen	Information Technology Expert and Counsel, Deeth Williams LLP
Ian Bailey	Chief Technology Officer, Province of BC
Andre Boysen	Executive Vice President of Marketing, SecureKey Technologies Inc.
Kim Cameron	Distinguished Engineer, Architect of Identity, Microsoft
Elizabeth Denham	Information and Privacy Commissioner, Province of BC
Raphael Diaz	North American Strategic Engagement Lead, GSMA
Vincent Gogolek	Executive Director, BC Freedom of Information and Privacy Association
Kaliya Hamelin	Executive Director, Personal Data Ecosystem
Aran Hamilton	Co-founder, IdentityNorth
Krystyna Hommen	President and CEO, Excelleris
Bette-Jo Hughes	Associate Deputy Minister and Government CIO, Minister of Technology Innovation and Citizens' Services, Province of BC
John Jacobson	Deputy Minister, Ministry of Technology, Innovation and Citizens' Services, Province of BC
Mike Monteith	Co-founder, IdentityNorth
Kerry Munro	Group President, Digital Delivery Network, Canada Post
Jay Schlosar	Assistant Deputy Minister, Strategic Initiatives Division, Government Communications and Public Engagement, Province of BC
Gerri Sinclair	Corporate Director, TSX Group, Vancouver Airport Authority; The Gerri Sinclair Group
Don Thibeau	Chair, The Open Identity Exchange
Colin Wallis	Authentication Stds, Department of Internal Affairs, New Zealand
Graham Whitehead	Information and Technology Services Professional, Member of ID Ecosystem Steering Group

IdentityNorth Specialist Forum Proceedings

A Component of the Digital Services Consultation

Prepared by MASS LBP on behalf of the Ministry of Technology, Innovation, and Citizen Services and IdentityNorth