Canada, We've an Identity Problem -

We can't easily act anonymously and control our identity

It's Time for a New Age Canadian Identity using Privacy by Design

Copyright: 123RF Stock Photo

Author: Guy Huntington, President, Huntington Ventures Ltd.

Date: September 2018

TABLE OF CONTENTS

Executive Summary

In Canada we use birth certificates to obtain other identity documents such as driver's licenses, health care cards and passports. Birth certificates are now easily forged. When we walk into bars or want to buy cigarettes or alcohol, we use driver's licenses that contain our name and address. The result…large scale identity fraud and an inability to easily act anonymously. Our identity verification information is copied over and over again into many different systems. It's time to change.

This paper carefully lays out a new system for doing identity verification. It shows how there isn't one thing to do. The existing system can't be easily tweaked.

Instead, it lays out a new age way of doing this, designed from the ground up using the following privacy principles:

- A person should be able to act anonymously
- A citizen is able to have multiple personas either physical and/or digital
- They should also be able to "live off the grid" if they so choose
- A citizen should be able to control their provincial/territory vital stats identity except where otherwise specified by laws
- **However, when they interact with government or financial services, there should only be one physical identity per citizen**

It then shows how to use new tools, such as Blockchain and Sovrin to assist BUT it also points out challenges by using these, including people who don't use the technology and electromagnetic pulse attacks.

The paper also addresses the use of biometrics and consent. It calls out for new laws and regulations protecting these. Consent for children as well as digital identities for them is also discussed.

The paper then addresses an emerging problem…human cloning. Regardless of if this will be legal or not, it recommends next steps to address it.

Next, the paper states privacy design for the new age in which we live. It makes note of different potential attack vectors requiring address to mitigate privacy risk.

The paper ends with a series of recommendations for governments on next steps.

Canada, it's time we collectively address our existing identity verification problems. We must look forward and not backward to design a system, protecting our identity privacy, for the next 100 years.

Introduction

Canada, we have an identity problem. Our existing identity verification processes are no longer working. We can't easily act anonymously and we don't control our identity. How can this be? What does it mean to me?

How Can This Be?

Whenever you apply for services like a driver's license, health care card or bank account, you have to provide documents that verify you, e.g. birth certificates, etc. The modern birth certificates we use were designed in the 1800's and were very hard to produce. Thus, the fact that you were carrying one likely meant that you were who you claimed to be.

Historically, federal and provincial/territorial governments wrote laws describing these as acceptable identity verification documents. This worked well for the next 100 years. Then along came technology. Today, birth certificates are easily to reproduce cheaply.

In security circles, birth certificate documents are called "breeder documents". Why? Because with one, a person can easily obtain other identity documents like driver's licenses, passports, social insurance cards, health care accounts and also open up bank accounts.

Let's use Jane Doe as an example…

An identity claiming to be Jane Doe shows up in a province/territory wanting a health care card. She provides her birth certificate, some documentation proving she lives in the province/territory and another supporting her identity, e.g. current employee ID card, etc. The province then creates a new health care account for Jane. Yet, is it Jane?

It could be Jane. She may or may not have notified the other province/territory she's leaving that she has moved. However, it might not be Jane...

It could be organized crime has obtained or created a Jane Doe birth certificate and is using it to establish false identities. What's in it for them? The ability to then use Jane's identity to obtain prescriptions etc. which can then be resold on the street. They can also use Jane's false identity to create bank accounts, take out loans, etc. Thus, there is money to be made by using false identities.

What Does it Mean to Me?

It affects you directly and indirectly.

Directly We are Affected

Many people are victims of personal information fraud. In Canada, recent personal information fraud numbers are hard to come by. In Australia, the government publishes this:

"Each year, the personal information of an estimated 1.7 million Australians is stolen or misused. This makes identity crime one of the most prevalent personal crime types in the country. Identity crime also provides a foundation for many other types of crime and has been rated by the Australian Crime Commission as a key enabler of organised crime."

Taking the Australian numbers and applying it to Canada means that approximately 2.5 million Canadians are annually affected. Some of this comes from weak identity verification.

Indirectly We Pay a Price

Indirectly, we all collectively pay a price. For example, Canadian health care fraud rates are estimated between 2-10%. Some of this is due to fraudulent billing. However, some of it is related to identity fraud.

The federal government will likely introduce before the next election a proposal to provide free pharmacy to Canadians, i.e. Pharmacare. The projected annual cost is approximately $20 billion. **Taking the 2-10% health care fraud rate results in some staggering numbers, e.g. between $400 million and $2 billion dollars annually to fraud!**

Weak Silos of Identity Verification Systems

Across Canada, each province/territory maintains their own vital stats services (e.g. registries for birth, gender change, name change, marriage and death) as well as their own health care systems, etc. This results in problems doing identity verification. Let's use Jane Doe again as an example…

Jane wants to apply for a job at Acme Ltd. She presents her birth certificate as an identity verification document. This document show's she was born in a different province/territory than the one she is currently living in and applying for a job. The employer enters the number into their systems but has no ability to check to see if the document Jane provides is valid. Thus, the employer is at risk if Jane is not whom she claims to be.

To mitigate this, in Australia, for several years, the federal government got together the states and they offer a "Document Verification Service" (DVS). With the citizen's consent, employers pay a small fee (ranging from $0.40 to $0.80) to see if the identity document is valid.

Let's say Jane is trying to masquerade as someone who had died. The document verification service would then let the employer know that Jane isn't whom she claims to be.

If we could have this in Canada, does this solve our identity verification problems? No. It doesn't tie the actual identity document to Jane. It simply states if the identity document is valid. So, if Mary is masquerading as Jane using Jane's valid birth certificate, then the identity verification system will still approve her.

Using a document verification service reduces what I call "identity fraud for dummies", i.e. using identities that are already dead to masquerade as others. However, it won't solve the entire identity problem.

In Canada, we need to design our identity privacy from the ground up addressing changes in technology and science that render old ways of doing identity verification less secure. So, what are other solutions?

Biometrics, Technology and Privacy

As a result of existing weak identity verification and authentication, many enterprises and governments around the world are deploying biometrics to tie the identity to the person appearing before in-person or electronically. Examples include the use of fingerprints or scans, retina or iris, face recognition, voice, palm prints, etc.

We also use are now willing giving our DNA, e.g. sending a sample to an ancestry service to see if you're related to anyone. However, most people don't understand both the technology and implications to their privacy when providing them.

Not all biometrics are the same in terms of accuracy. There is something called the "equal error rate" (ERR) which measures the false acceptance rate to the false rejection rate. These can widely vary, i.e. different biometrics have different levels of accuracy. Then there are the biometric readers…

Today, smart phones, laptops, etc. are coming out with biometric readers. These too can vary widely in being foiled. There are few independent testing agencies that set standards for biometric readers. Thus, an enterprise may be using a biometric with a high degree of accuracy BUT the reader used might be easily foiled.

Some biometrics which have been widely used for many years, e.g. facial recognition on driver's licenses are now no longer as reliable. Why? Face masks have improved at low price points. Organized crime likely uses these together with fake birth certificates to create false identities.

Most importantly, there are few laws and regulations protecting a citizen's privacy regarding the use of biometrics. For example, if you provide a biometric to a government agency or, a third party, how do you know how the biometric will be stored, the length it will be stored, if the enterprise can send it on to others with or without your consent, how you can request it can be removed from their databases, etc.? It is a case where the technology and deployment has outpaced our ability to protect our biometrics.

I wrote a paper in the Fall of 2017 "Biometrics and Government" where I lay out the underlying principles required to protect our biometrics used for identity verification and authentication. These principles need to drive new laws and regulations protecting our biometrics:

- One physical identity per citizen
- A citizen is able to have multiple personas either physical and/or digital
- A citizen should have ways of anonymously identifying themselves
- Biometrics will be obtained at birth or, in a citizen's early years, to uniquely verify the identity
- Biometrics used in identity verification must be able to differentiate between genetic twins and human clones
- Biometrics used for identity verification must be protected by law so that they will only be used to identify the person and will not be used for any other purpose
- Biometrics used for identity verification must be securely stored
- Governments must not build the "mother of all citizen identity" databases
- The government agency managing identity verification must be protected by law from any interference by other government agencies and/or third parties from obtaining the identity verification biometrics and using them for purposes other than identity verification
- The government agency managing identity verification should have the ability to confirm to a requesting party that an identity exists without having to provide the identity information
- Any biometric obtained from the identity during their lifetime for use by either governments and/or third parties must be governed by laws prescribing the following:
    - Recorded citizen consent must be done to obtain and use the biometric
    - The consent must clearly state how the biometric will be obtained, stored, used for identity authentication, archived, and eventually destroyed
    - Any biometrics used to verify the identity must be securely stored
    - There must be no transmission or sharing of the biometrics with other parties without the express consent of the identity
    - Biometrics must not be used for medical research, profiling, marketing, etc. without the express consent of the citizen
    - There must be a process in place so that citizens can request that their biometrics be removed from government and third-party databases

So, would having new biometric laws and regulations to protect our identity suffice to solve the challenges of weak identity verification? No. It also requires putting control of the identity back into our own hands…

Control Over Our Identity

In today's world, it's hard to act anonymously. For example, if Jane Doe walks into a bar or wants to buy cigarettes, she must show a piece of ID to validate her age which usually is her driver's license. This contains her name and address and prevents anonymity. We are using old technology used for one purpose, e.g. driver's licenses to drive cars, for another purpose, i.e. identifying someone to show they are of legal age.

I've written in other papers some underlying principles regarding an identity:

- A person should be able to act anonymously
- A citizen is able to have multiple personas either physical and/or digital
- They should also be able to "live off the grid" if they so choose
- A citizen should be able to control their provincial/territory vital stats identity except where otherwise specified by laws
- **However, when they interact with government or financial services, there should only be one physical identity per citizen**

What new tools exist that we can use to enable this?

Blockchain and Sovrin Identity

Blockchain uses encryption algorithms with the concept of a general ledger published, in public, on thousands of servers all over the world. You can sign something using your private key which others can then validate using your public key.

Sovrin is a new digital protocol that uses blockchain to then allow a citizen to control their identity. You control what identity information to share and who you share it with. Here's an example using Alice:

- The post office issues a verifiable claim to Alice attesting that her street address is 123 Main Street
- Alice shares this claim with her credit union as part of opening a new account
- Without having any connection to or interaction with the post office, the credit union instantly and cryptographically verifies that Alice's claim is signed by the post office and has not been revoked
- Alice now owns this proof-of-address claim and can use it anywhere she wants, as much as she wants, and now the credit union can trust that Alice's address is 123 Main Street

Let's assume that a provincial/territory vital stats service offers citizens the ability to act anonymously by validating their age. So, Alice is walking into a bar with a vital stat claim in her digital wallet. How does the bar know that it's her and not someone who's obtained her digital wallet containing the anonymous claim?

The answer is for the vital stats agency to obtain Alice's photo when she reaches age of majority and digitally sign this as part of her digital claim. **The bar sees the digitally signed picture in the claim, verifies it against the signature provided by the provincial/territory stats service, matches it to Alice and lets her in. Thus, Alice can enter the bar anonymously with her in control of her identity information.**

Now let's say Alice wants to open a bank account. The risk is higher than her post office issued address. The bank will want to mitigate the risk that the person claiming to be Alice hasn't obtained her digital wallet and her private signing key. How?

The answer is for the provincial/territory vital stats service to have collected other biometrics like her iris and fingerprints. Upon reaching age of majority, the vital stats service would issue a digital certificate to Alice allowing her to digitally sign documents. When Alice shows up to open a bank account, with her consent, she would provide a iris and a fingerprint scan. This would be securely sent to the vital stats service to confirm it is Alice. She would then digitally sign the bank document and be granted a bank account.

While all of this puts control of the identity back into the citizen's hands, it come with a hidden price…

EMP Events Resulting in the Collapse of a Digital Identity System

As the world digitizes identity, we become increasingly reliant upon digital vital stats systems with vital stats databases. If anything happens to the underlying databases, then "poof" goes the heart of legal identity trust in Canada. What can cause this? Electromagnetic pulse events (EMP) from the sun or, from a terrorist attack. Is this possible?

Yes. The "Carrington Event" of 1859 or "Railroad Storm" of 1921 would digitally wipe out most servers on the planet. When recovery begins post EMP event, one of the first things is to verify you are you. If the digital citizen biometric identity database is destroyed, this will be almost impossible to do.

The answer is to mandate, by law, that data centres holding vital stats information be placed in EMP resistant data centres or, into existing data centres that have EMP resistant sections. Note this isn't common today.

The same applies to blockchain holding identity information. Any server holding blockchain data can be affected by EMP events and should be stored in EMP resistant data centres.

So, does using Blockchain and Sovrin with EMP resistant data centres solves the identity verification problem? No. Not everyone will either be able to deal digitally with identity verification or, decide they don't want to use technology for this.

Identity Verification for All Regardless of Technology Used

Some people don't own cell or smart phones and/or don't want to use them. The vital stats services must be available to all citizens regardless of technology. Here's how this can be done…

A provincial/territory vital stats identity card can be issued containing the digitally signed claims using blockchain/Sovrin for the identity. It's possible that two cards can be issued:

- One for an anonymous identity with the claim that Alice used to enter the bar
- The other contains her full birth certificate information and also contain her digital certificate issued by the vital stats service allowing her to digitally sign documents

Alice can use either one, as she chooses, when she interacts with different levels of government and/or third parties like banks, etc. Note, the identity card data could be possibly stored on existing identity cards such as driver's licenses or health care cards. As an example, let's use Alice interacting with a government agency or third party.

Alice would walk up to the service counter, give her consent for her identity card to be used and then present her identity card. It would be swiped into a reader. She would then provide a 4-digit number to validate her digital signature. On the screen would appear her digital photo, signed by the vital stats agency. The government or third party now has reasonable confidence it's Alice they are dealing with.

So, does having physical cards as well as digital wallets using Blockchain/Sovrin solve the identity verification problem? No. There are privacy challenges needing to be addressed.

Citizen Consent

I have a former customer whom I worked with who is a diabetic. He told me he's using a device inserted into him measuring his blood sugar levels. It broadcasts to an app on his phone, which then alarms him when the levels drop. He wants to be able to provide his consent such that the data would be sent from the company providing the device to his provincial/territory health insurance agency as well as to his wife and doctor. This device is just the first in a wave of literally hundreds of devices we will use ranging from our bodies, appliances, clothes, etc. How will he keep track of all of his consents?

The same challenge exists with our identity verification. Recall that Alice gave her consent to the bank to obtain her biometrics and send it to the provincial/territory vital stats service to verify her or, where she provides her consent to use her physical card for identification. How can she keep track of who she gave her consent to when she interacts in the near future with hundreds of internet of things devices, people and institutions?

There is a new protocol "Kantara User Managed Access" and "Kantara User Managed Access Federation" which allows one to centralize their consent management to one place, across the different systems you use to interact with. This service can be operated by government, non-profits, commercial enterprises on your behalf or, that you could conceivably operate yourself.

While all of this is good, this is another case where the technology is ahead of our laws and regulations protecting our privacy. For example, how do you transfer from one consent management service to another? What's the time period the consent data will be stored? What kind of identity verification and/or authentication is required to access different levels of risk? For example, providing consent to other people or enterprises for data from your fridge about something going off is a different level of risk than providing your biometric data and or identity verification to others.

I wrote a paper in the Fall of 2017 "Citizen consent and the Internet of Things" where I laid out the underlying principles that should be used to create new consent laws and regulations:

- End user consent must be required to use the device except in those cases where consent is mandated by laws and regulations.
- The chain of custody for consent must exist at all levels, i.e. from vendor through to final user or users based on risk and laws/regulations.
- The device, the system that controls it, and/or the identity management system the device is part of, must be able to use "User Managed Access" and also "OpenID Connect" protocols.
- Any individual, government, or enterprise offering a centralized user consent service must be mandated by laws and regulations.
- Any consent management service must adhere to regulatory security best practices including identity and credential assurance, data storage and transmission as well as archival processes.
- Based on risk, the identity assurance and the credential assurance must be applied to obtain and/or transfer consent between the user and various enterprises and/or other Internet of Things devices.
- Secure, delegated access of consent should be part of the device's consent management system.
- The user of a centralized consent management service should have the ability to transfer this service to other enterprises offering this service in a secure manner.
- When a user leaves a centralized consent management service, the service must securely store the data for a predetermined amount of time according to the timeframes set forth by laws and regulations.

Then there is legal consent regarding managing a citizen's identity…

When a child is born, the parents or legal guardian will act on the child's behalf. They will be given a Sovrin/Blockchain digitally signed claim for the child's identity and, if they want, a physical identity card for the child. They can then act on the child's behalf to use their identity to create health care accounts for the child, enroll them into schools, etc.

The new age vital stats service should also contain the legal guardian of the child from the authoritative source, the justice system. For example, if a parent shows up at a social services counter with a child they claim is their own or, they're their legal guardian, then they provide their consent for both the child's identity and their own to be verified. The social worker would then see who the legal guardian of the child is. If it matches the person standing in front of them, then they can proceed. If not, then different business processes would occur to deal with the child and the adult.

A similar, yet slightly different, situation exists for people who are mentally not able to look after their affairs. Existing legal processes for managing things like Power of Attorney would be amended to include a change in the vital stats database to having a person's identity with this authority being added to the mentally challenged person's identity. For example, when the person with Power of Attorney is taking over bank account management or selling a person's home, they would be able to use both their own identity as well as the mentally challenged person's identity to verify themselves and legally make the transactions occur.

So, does having new consent laws plus Sovrin/Blockchain solve all the identity verification problems? No. There is science to contend with…

The Age of Human Cloning

In 1996 a sheep named Dolly was cloned. Early this year, Chinese scientists announced they had successfully cloned monkeys. Today, for a price, one can clone their pets. So, what was once thought of as science fiction, i.e. human cloning, is now upon our doorstep.

Regardless of if human cloning becomes legal or not, the vital stats services need to be able to differentiate human clone 1 from human clone 2 or 3 or 4 at birth and onwards from all the other citizens in Canada. How can this be done? Likely using biometrics such as fingerprints and iris and possibly DNA. Yet, there are many privacy and technical challenges associated with this.

In 2006 I wrote a paper, "The Challenges with Identity Verification" in which I proposed using biometrics, including DNA, to be used in vital stats services. **I took criticism from this from people who were worried about the government maintaining a database of DNA for all its citizens AND… they were right. Our privacy must be protected**. That's why in 2017 I wrote the paper “Biometrics and Governments” where I laid down the underlying principles to protect our biometrics to create new laws and regulations.

Let’s hypothetically assume that citizens won’t want to have the DNA stored in the vital stats database for fear of mis-use by governments. How will the new age vital stats system address human cloning at birth? There are some technical challenges that need to be addressed.

Babies biometrics change AND they can be hard to obtain, e.g. iris scans. One avenue that should be explored is the work of Dr. Anil Jain and his team at Michigan State University. They have been pioneering new techniques to obtain babies fingerprints. A longitudinal study needs to be put into place to track the fingerprints obtained from the babies as they grow older.

Let’s hypothetically assume this works. Scientific studies need to be done to confirm that the fingerprints will then be able to differentiate clone 1 from clone 2.

Another possibility is to then obtain the iris scan of the identity when they attend their first year of pre-school or of school. The child is now old enough to provide the iris scan. Studies need to be done to assure that the iris biometric is able to differentiate clone 1 from clone 2.

Based on this research, then we, as Canadians, will know if we can use fingerprints and iris to differentiate human clones or, if DNA will be required.

So, does the use of Blockchain/Sovrin, a new age vital stats service with laws protecting our biometrics and consent and the ability to differentiate clones solve the identity verification problem. No. There is death to contend with…

Death – Legally Closing off the Identity

The new age vital stats service can offer some additional tools to medical practitioners who are completing the medical certification of death. The biometrics used in the vital stats database can be applied to ascertain that the deceased person is whom others claim them to be. This is not a medical panacea because, in some instances, the deceased biometrics will not be accessible. However, the acts pertaining to medical certification of death need to be amended such that wherever possible, the biometrics are used to confirm the identity verification.

Then there’s the notification of death…

The new age provincial/territory vital stats service should be integrated into a new Canadian Identity Document Verification Service, similar to what Australia has done. Thus, both third parties, like banks and insurance companies, as well as different levels of government, can search the database, across Canada, to see if the person is living or dead.

Careful privacy thought needs to be given to automatic notification from vital stats services of death to different government agencies as well as to third parties, whom the citizen gave their consent to obtain this information before they died. For example, say Jane Doe took out bank loans for a mortgage. She would provide her consent, as part of the loan application, for the vital stats services across Canada to automatically notify the bank when she died.

So, does having updated legal death notification, plus the use of Blockchain/Sovrin with a new age identity verification service solve the identity verification problem? No. There is a fundamental privacy principle about separating identity verification from identity contact information that needs to be addressed.

Identity Verification MUST be Separate from Identity Contact & Authentication Services

A person's privacy must be maintained at their discretion. Recall the principles mentioned earlier about identity privacy:

- A person should be able to act anonymously
- A citizen is able to have multiple personas either physical and/or digital
- They should also be able to "live off the grid" if they so choose
- A citizen should be able to control their provincial/territory vital stats identity except where otherwise specified by laws
- However, when they interact with government or financial services, there should only be one physical identity per citizen

If a person wants to "live off the grid" then they should have the ability to do this. They can live their own life without letting others know where they live and/or their contact information. **Thus, the new age provincial/territory vital stats service must be separate from other government contact and authentication services. It MUST only be used to verify an identity**. Let's use Jane as an example.

Jane wants to live off the grid. The vital stats service's function is only to verify that Jane is Jane. Jane, when she reaches age of majority, has a digital wallet with claims from the vital stats agency verifying she is Jane and possibly, at her discretion, an identification card also containing the same digital claims.

Jane hypothetically could live her whole life on her own, without any contact with any government service. When she dies, if her body is found, she will likely be identified as Jane, assuming her identity card/digital wallet is found and/or biometrics are available to use and/or is identified by someone.

Now, instead, let's say Jane instead wants to obtain health care or a driver's license. By law, she will have to provide her identity as well as address and contact information. This information should be centrally maintained in a provincial/territory identity and authentication service, separate from the vital stats service. Here's the process Jane would go through to create her entry into this service.

She would first of all provide her consent to the identity and authentication service to use her identity verification claim to verify she is Jane. After successful verification, Jane would then enter her contact information. With her consent, the other provincial/territorial identity and authentication services are checked to see if she already exists in one of them.

Depending on how the provincial/territory authentication service operates, she might create a username and password for herself, a 4-digit pin and/or provide some biometrics used for authentication. Recall that any biometric used for authentication must follow laws and regulations from the new biometrics' laws created.

Jane may agree to having to provide her address et al to the provincial/territory identity and authentication service BUT she might not want other agencies, third parties or people to know of this. So, she would indicate this during her registration process. This means that only those agencies, required by law, are notified of her contact information.

Now, let's assume that Jane wants to let other government agencies and/or third parties know of her contact information. She would provide her consent to the provincial/territory identity and authentication service to notify other parties she then specifies. Jane goes to one place to change her contact information and then all the other parties, predetermined by Jane, are then notified. **There is a clear separation between the provincial/territory vital stats service and any other service used for identity and authentication management**.

So, does this now solve and identity verification problem? No. The digital age requires us to rethink the identity verification and authentication for infants, children and youth.

Identity Verification and Authentication for Infants, Children and Youth

Historically, most identity verification and authentications systems, with the exception of birth certificates, begin when a person reaches age of majority and/or applies for things like a driver's license. Historically, this began to change when families began to frequently travel outside Canada with parents obtaining passports for their children. Today, in the digital age, it's presenting new challenges. Let's use Jane Doe's son John as an example…

Let's hypothetically assume she's poor and requires social assistance for caring for her new son. As previously explained, in a new age vital stats service, she would use John's vital stats claim and also present her identity claim, as his parent, to verify John is John and she is his mother.

She enrolls him in government funded daycare. Again, she would use John and her vital stats claims to verify themselves.

On John's first day of school, she would again use the vital stats claims to verify themselves. The school identity the education system gives John is now tied to his vital stats identity.

At school, John has a digital identity. He will likely use different devices with different applications and services. How does he authenticate to the various devices, apps and services?

It's hypothetically possible that John could use the provincial/territorial optional identity and authentication service. He could use his voice to authenticate. This reduces complexity for school districts to use different authentication services to authenticate John. Each year, John would have to update his voice. As he accesses more sensitive services, he might have to add a 4-digit pin to his authentication.

Now let's assume that John is beginning to work part-time jobs while going to school and/or in the summer. Some of these jobs require him to obtain workers compensation number and/or sign contracts. He may or may not obtain a driver's license as well, requiring him to sign for his driver's license as well as open bank accounts. As more and more of these functions occur online, then it presents new challenges to verify John, obtain a digital signature as well as to authenticate him.

Today, children and youth act online very frequently. They may join online groups and apps as well as pay for services they then consume. In their interactions with physical and virtual third-party merchants. they will frequently be giving some of their biometrics to be used to authenticate them as well as revealing more personal identity information about themselves.

This trend of children and youth interacting digitally will only continue to increase. Therefore, very careful thought to this needs to be given by privacy groups, citizens, law makers, third parties and government agencies. We, collectively, need to reflect on how to digitally protect infants, children and youth as well as change our old ways of thinking that infants, children and youth don't need digital identities and common authentication systems. In the recommendation section of this paper, I lay out next steps to begin to rethink this.

So, assuming we address the infants, children and youth identity verification and authentication issues, does this address the identity verification problems? No. There is the privacy design for the new age vital stats service that needs to be addressed.

Privacy Design for New Age Provincial/territory Identity Verification Service

When designing systems for privacy and security, one must consider all the "attack vectors". These are places in the technology, business processes and people, where malicious people/organized crime can take advantage of weaknesses and penetrate the system.

Privacy Design Principle's

- A person should be able to act anonymously
- They should also be able to "live off the grid" if they so choose
- However, when they interact with government or financial services, there should only be one physical identity per citizen
- A citizen should be able to control their provincial/territory vital stats identity except where otherwise specified by laws
  - The use of digitally signed claims by the vital stats agency using Blockchain/Sovrin and/or physical cards provides the ability for the citizen to control their identity
  - Exceptions by law will include a person being arrested and their biometrics obtained to verify the identity in custody
- Infants', children's' and youths' identity verification and authentication MUST be protected by updated laws for them both digitally and in-person
- The ability to search the vital stats database will be mandated by laws protecting the identity of the citizen
- When an identity is searched for identity verification, the identity MUST provide their consent UNLESS otherwise specified by law
  - The identity consent record should be made available to the identity via Kantara User Managed Access (UMA)
- **THERE MUST BE NO ABILITY TO SEARCH THE PROVINCE/TERRITORY VITAL STATS DATABASE TO PROFILE CITIZENS**
  - The vital stats service is designed to ONLY provide identity verification
- Any biometric used for identity verification must be only entered into the provincial/territory vital stats database and NEVER BE ABLE TO COME OUT
  - i.e. it's a one way in system with the search response only confirming the identity yet never being able to provide the identity's biometrics
- Any biometric sample physically taken, e.g. if hypothetically DNA is obtained, must be destroyed after the sample is digitized
  - There must be no ability for a government, security agency or organized crime to obtain the sample and then use it maliciously for purposes other than what it was intended for
- Any biometric sample taken out in the field MUST BE SECURE
  - Births and deaths can occur at any place. Therefore, when the identity's biometrics are obtained, it must be securely done to mitigate risk of substitution with another identity's biometrics
- Any transmission of data into the provincial/territory vital stats database must always be highly secure, i.e. use secure encryptions and digital signatures as well as the latest Transport Layer Security protocols (at time of writing TLS v1.3)

    - This prevents common man in the middle attacks and/or endpoint attacks on networks endpoints
- Administrator access MUST BE SECURE.
    - Any provincial/territory personnel coming into contact with the vital stats service must be background checked
    - There must be double checks made on any access to the underlying data by an administrator
        - This prevents a malicious administrator from either accessing the data inappropriately and/or editing the data
- Provincial/Territory vital stats systems must exist in their own secure section of a data centre, on its own network, in EMP proof data centres and be highly available (e.g. 99.999%).
    - Provinces/Territories should cross-share their vital stats databases to ensure secure high availability AND NOT PLACE THESE IN COMMERCIAL CLOUDS
    - Email access by administrators must exist on separate networks to prevent risk of malware making its way from an email into the vital stats system
    - Use of dongles, etc. on computers with access to the vital stats service must be severely restricted to prevent risk of obtaining vital stats data
- Any person coming into contact with the identity to obtain a biometric must be background checked, trained and certified to legislative standards
    - This applies to:
        - Health care practitioners obtaining biometric samples to begin the birth record and/or pre-school/school samples
        - Personnel obtaining biometrics from landed immigrants
        - Government and third-party personnel, e.g. banks, who are obtaining a biometric to be used to verify an identity
- **Privacy groups across Canada MUST be consulted in the privacy laws, regulations and design of the Province/Territory vital stats service as well as BROAD consultation with the Canadian public prior to approval of laws, regulations and system implementation**

So, does this now address the identity verification problem? Not quite. The last component is rethinking identity assurance in Canada.

Rethinking Canadian Identity Assurance

Identity assurance is a measure of identity verification processes used to verify an identity versus risk. Governments, all over the world, usually break this down into 4 levels, with level 1 being the weakest. Here's a link to the existing Canadian identity assurance.

If you read through it, you'll see that that only at level 3, are foundational documents required and that biometrics are optionally required for level 3 and 4. Further, you'll note that "Children, minors and vulnerable individuals may not have sufficient evidence of identity to meet the requirements specified in the Standard on Identity and Credential Assurance."

This is what I call an “old school way” of viewing identity. The underlining identity documents no longer work due to the reasons outlined at the beginning of this paper. So, as risk rises, additional documents are required that are then more rigorously proofed and then the use of biometrics. My underlying premise is that it’s time to turn identity assurance upon its head.

Using a privacy by design model, with a new age vital stats service, hypothetically, in the future, a baby’s fingerprints would be obtained tying them to their underlying birth certificate. Then, this would be issued in a digital claim, signed by the vital stats service, as outlined in this paper. Thus, the baby has the highest degree of identity assurance right from their birth.

I wrote a paper “New Age Identity Assurance: Turning it Upon its Head” in which I describe how it might work. Citizens have the ability to act anonymously, control their identity and, as the risk rises, provide biometric information and/or something they know (e.g. a 4-digit pin) to verify their identity.

Has any country done this? Estonia did, in a fashion, in 1999. They created their “Identity Documents Act”, that required citizens, at the age of 15, to provide biometrics. This is then added to their population registry. What’s the result?

Today, they offer their citizens over 1,000 different online services, including e-pharmacy, e-school, e-voting, etc. Since banks and other third parties trust the identity, today, almost all legal contracts are digitally signed by the citizens.

Why can’t we simply duplicate what Estonia has done? There are privacy laws required for the use of biometrics and consent that Estonia doesn’t have. The citizen can’t easily act anonymously. Things like blockchain and Sovrin, didn’t exist then. Their model isn’t able yet to differentiate human clones at birth. It’s a good example of what can be done BUT, in Canada, we need to first of all start with a privacy by design model for all citizens, from birth to death.

So, if we have all the different components outlined in this paper, do we then successfully address the identity verification problem? Yes.

Canada – We Need A Privacy Designed Identity Verification System for the Next 100 Years

The point of this paper is that our existing identity verification systems are built using technology and processes from the late 1800's and 1900's that are no longer working well. We, as Canadians, pay a steep price for this, e.g. identity theft, an inability to act anonymously and huge fraud financial costs.

With science rapidly advancing, we are now facing the age of human cloning. Our old school ways of doing identity verification aren't able to address this. It's time to change.

HOWEVER, THIS IS NOT TO SAY THE IDENTITY SKY IS FALLING AND IMMEDIATELY ADOPT BIOMETRICS AND A NEW AGE VITAL STATS SYSTEM. The paper lays out the complexity of what's required. **Instead of rushing into this, a pragmatic approach needs to be taken to address this, based on the privacy principles illustrated in this paper.**

Recommendations:

Here are suggested recommendations for the federal, provincial and territorial governments:

1. Rapidly put in place a service similar to the Australian document verification service. This will begin to mitigate at least some of the identity verification risks occurring today in Canada.

2. Assemble a broad working group composed of privacy groups, identity practitioners, third parties, legal experts and begin to drill down into the following areas:
   a. Biometric legislation and regulations
   b. Consent legislation and regulations
   c. New age vital stats services laws and regulations
   d. Infant, children and youth identity verification and authentication
      i. Create use cases for the many different scenarios requiring them to provide identity verification and/or authentication and/or identity data
      ii. Determine how to protect them from malicious entities wanting to obtain their identity information to mis-use it
      iii. Update laws and regulations allowing them to securely provide their identity information
      iv. Work with third parties, like merchants, to establish new guidelines on how to interact with these target groups digitally and in-person.

   Note that the laws and regulations across Canada must be uniform to reduce "identity friction" for citizens, different levels of government and third parties to deal with.

3. Then do a broad citizen consultation across Canada to not only inform citizens but also to get their buy-in to the proposed new laws, regulations and vital stats systems. They need to be able to see that their identity privacy is front and centre or, this effort will politically fail.

4. In parallel to the above, do the following:
    a. Rapidly implement a longitudinal study with Dr. Jain’s group and Canadian researchers on the use of baby’s fingerprints
        i. This will prove out the usefulness of these over time and will affect the design of the vital stats database
    b. Implement a study to determine how to differentiate human clones
        i. This needs to determine what biometrics will be required to differentiate clone 1 from clone’s 2, 3, 4 etc.
        ii. Based on this, it then drives out the laws, regulations and operations of the new age vital stats service
    c. Determine what data centres across Canada are currently EMP proof including government data centres
        i. Then determine what the costs are to upgrade current government data centres or, build new ones
    d. Establish an independent biometric testing centre. It needs to:
        i. Test and publish equal error rates for biometrics
        ii. Continually test and publicly report on different biometric readers to determine how resistant they are to masquerading

    Note: Rather than have a “Canadian” biometric research centre, given that our trading partners also have similar problems, it might be worth considering partnering up internationally to do the work and then share the results more cost effectively

5. Design the new age vital stats service and then invite others publicly to try to attack it before implementation.
    a. This is what the open-source world has been doing for the last decade.
    b. It ensures that the whole process from the biometric sample being obtained, transmitted and then searched on is secure by the public/researchers able to know the security and then try to attack it
    c. By keeping it in the public domain, it ensures that any weakness now, or in the future, is quickly detected.

6. Design the new age vital stats service such that it can be quickly upgraded across Canada
    a. We've building a identity verification service for the next 100 years. Who knows what changes will occur in technology and science?
    b. Thus, the system needs rapid governance processes where all provincial/territory services can agree on a change and then securely, rapidly implement it with excellent testing to ensure no new security hole is created.
    c. Changes made should be publicly announced.

Summary

This paper lays out the underlying privacy principles of a Canadian new age identity verification system:

- A person should be able to act anonymously
- A citizen is able to have multiple personas either physical and/or digital
- They should also be able to "live off the grid" if they so choose
- A citizen should be able to control their provincial/territory vital stats identity except where otherwise specified by laws
- However, when they interact with government or financial services, there should only be one physical identity per citizen

As the paper illustrates, there's no easy quick fix to create this. For example:

- Biometrics section of this paper shows that new laws and regulations are required protecting our biometrics.
- We require control over our identity allowing us to act anonymously if we want to
- The consent section of this paper illustrates that new laws and regulations are required protecting our consent
- Sovrin and Blockchain section of this paper shows new digital tools offering us control over our identity BUT don't assist citizens who don't have access to the technology. The "Identity Verification for All" section proposes solutions for this.
- EMP section of this paper illustrates that our rush to digitize identity puts our legal systems at risk in the event of a major EMP event. Thus, EMP data centres are required.
- The identity verification service needs to be separate from contact and authentication services
- Infants, children and youth section of this paper describes the new challenges in identity verification and authentication as the digital age unfolds
- The processes used to confirm an identity at death and notification need to be updated
- Human cloning section of this paper illustrates that it's now upon our doorstep. The recommendations section of this paper specifies doing research on the use of fingerprints and iris scans to determine if this will suffice for differentiating human clones.
- Obtaining biometrics at birth can be difficult since they can change with age. A longitudinal study is proposed measuring babies' fingerprints to determine its efficacy
- The privacy design principles for a new age provincial/territory vital stats service section creates a framework for discussions on what the new age vital stats service should be
- The "Rethinking Identity Assurance" discusses rethinking old school assurance models
- The paper concludes with a series of recommendations for governments to do in conjunction with privacy groups and a broad public discussion. Some can be done quickly, while others require much consultation and research.

Canada, it's time we collectively address our existing identity verification problems. We must look forward and not backward to design a system, protecting our identity privacy, for the next 100 years.

About the Author

Guy Huntington is a veteran identity architect, program and project manager who's lead as well as rescued many large identity projects with many of them involving identity federation. His past clients include Boeing, Capital One, Kaiser Permanente, WestJet, Government of Alberta's Digital Citizen Identity and Authentication Program and Alberta Blue Cross. As one of his past clients said "He is a great find, because he is able to do high quality strategic work, but is also well-versed in project management and technical details, so he can traverse easily from wide to deep. With Guy, you get skills that would typically be encompassed in a small team of people."