New Age Vital Statistics/Civil Registration Services: What They Do and Don't Do

Author: Guy Huntington, President, Huntington Ventures Ltd.
Date: Updated November 2018

Note to Reader:

I have been writing about rethinking civil registration systems since 2006

- "The Challenges with Identity Verification"

Over the last several months, I have written 11 papers about:

- New laws required to do this
  - "Why We Need to Rethink Our Vital Stats Laws",
  - "Why Your Digital Consent Matters – Including Sex"
  - "Why We Need New Biometric Laws Protecting Our Privacy"
- What the new age civil registration/vital stats service does and doesn't do
  - "New Age Vital Statistics/Civil Registration Services: What They Do and Don't Do"
- Leveraging Blockchain and Sovrin
  - "A Modern Identity Solution: New Age Vital Stats/Civil Registries, Self-Sovereign Identity, Blockchain, Kantara User Managed Access & EMP Resistant Data Centres"
- Protecting the civil registration/vital stats infrastructure
  - "When Our Legal Identity System Goes "Poof!"
- Separating vital stats services/databases from other identity authentication services
  - "Architecture Summary"
  - "Creating Estonia Version 2.0 – Adjusting for Changes From 1999 to 2018"
- Rethinking identity assurance using new age vital stats
  - "New Age Identity Assurance – Turning it on its Head"
- Rethinking Civil Registrations in Remote Locations
  - "Where Shit Happens - Rethinking Civil Registrations in Remote Locations"
- New Age Civil Registration/Vital Stats Design, Implementation & Maintenance Vision
  - "Guy's New Age Civil Registration/Vital Stats Design, Implementation & Maintenance Vision"

This paper deals with what a new age vital stats/civil registration service does and doesn't do. I have amended it from earlier versions removing most DNA references.

Table of Contents

New Privacy Laws Required

New laws protecting privacy are required before implementing a new age vital stats/civil registration service. It's suggested to read the papers for discussion of privacy and new laws required to create the new age service:

- "Why We Need to Rethink Our Vital Stats Laws",
- "Why Your Digital Consent Matters – Including Sex"
- "Why We Need New Biometric Laws Protecting Our Privacy"

What Is a New Age Vital Stats/Civil Registration Service?

It's a digital service, i.e. birth, name change, marriage and death registry using biometrics tied to the registered identity from birth, name change, marriage and death. Parents' biometrics are linked to the identity registration. It exists separately from state/provincial citizen identity and authentication services as well as from any other government service at the federal, state/provincial or municipal level.

Why Do We Need It?

It addresses the following problems:

- Identity fraud by others using paper-based identity documents to masquerade as you
    - Birth certificates are frequently called "breeder documents" since with them, one can obtain other documents such as driver's licenses, passports, health care cards, bank accounts, etc.
    - With the advent of inexpensive printers, they are now easily frauded
    - Other identity documents like driver's licenses with a photo are also now no longer as trustworthy since realistic face masks can be used
- Differentiating genetic twins and human clones
    - In January of 2018, scientists announced they had successfully cloned monkeys
        - i.e. the age of human cloning is now on our doorstep
    - Regardless of if this will become legal or not, a modern vital stats service must be able to differentiate between human clones as well as genetic twins. This likely requires the use of biometrics such as fingerprints and iris scans in addition to DNA.
- Offer citizens the ability to prove their identity anonymously
    - Current paper-based forms show who the identity is preventing the citizen from acting anonymously in certain situations like proving age when going into a bar, etc.

My premise is the old documents and processes we use to verify an identity are no longer working due to technology and scientific advances. These documents:

- Are prone to fraud from organized crime
- Result in hundreds of millions of dollars losses annually to both governments and financial institutions
- Adversely affect millions of citizens who fall victim to identity fraud
- Aren't prepared for the near future, i.e. human cloning.

Principles for a New Age Vital Stats/Civil Registration Service:

- Citizens must have the ability to:
  - Have multiple personas
  - Act anonymously if they want to
  - "Live off the grid" if they so choose
- **However, when they interact with government services and/or financial ones, there should only be one physical identity per citizen**
- **Citizen's biometrics used for identity verification and/or authentication must be protected by new laws/regulations**
- With the arrival of the internet of things requiring consent and new protocols enabling citizens to centrally manage their consent across enterprises, it requires new laws protecting their consent including those where citizens provide their biometrics
- New age vital statistics/civil registration services need to be created where birth, name, gender change, marriage and death changes are tied to the identity biometrically
- This requires new infrastructure requirements protecting the digital biometrics database from electro-magnetic pulses relied upon legally by business and governments
- Recent protocols should be leveraged allowing for businesses and government agencies to use identity federation and/or Sovrin identity/blockchain to provide citizen biometrics, with their consent, to the state identity verification services and receive answers back

What Does the New Age Vital Stats/Civil Registration Service Do?

- Register births, name changes, marriages and deaths by:
  - Tying them to the physical identity using biometrics
  - Link the baby's parents' biometrics to their birth record
  - Registering creation of the identity and any change to it
    - E.g. gender change, name change, marriage and death
- Provide one way in system for biometric information about the identity
  - i.e. no biometric information leaves the system and goes out
- Parents/legal guardians are given a signed digital attestation for their child either digitally or, via an infant vital stats/civil registration card
  - They then use their consent to register their child in government services such as education and health care or with third parties e.g. to open a bank account for their child
- Anonymous identity verification when the identity requires it, with the citizen's consent
  - e.g. you're going into a bar and the bar wants to attest you are over the legal age requirement
  - Option 1:
    - You'd swipe your finger at the door, or present an iris scan. The scan would then be securely sent to the registry and it would come back with a yes or no
    - i.e. your identity is never released

- Option 2:
  - You provide a digital attestation from the vital stats service, via Soverin/Blockchain that anonymously attests to who you are
  - i.e. your identity is never released
  - For more information refer to:
    - "New Age Identity Assurance – Turning it Upon its Head"
    - "A Modern Identity Solution - New Age Vital Stats, Self-Sovereign Identity, Blockchain, Kantara User Managed Access & EMP Resistant Data Centres"

- Option 3:
  - You present a physical card from vital stats/civil registration service that only has your photo on it
    - This photo is digitally signed by vital stats/civil registration service when you come of legal age
    - The bar electronically verified the signature by vital stats/civil registration and then lets you in

- Provides identity verification services to other different levels of government agencies, with the citizen's consent
  - e.g. you want to get a health care card, driver's license or passport
  - You provide your consent to the government agency to take a biometric and it's securely submitted to the identity verification service
  - The service then comes back with your date of birth, name, marriage status or, if the identity with those biometrics has died
  - It won't come back with where you live because that's not the purpose of this identity verification service
    - It's simply verifying your identity
    - Your address and contact information should be stored in another government database systems like provincial identity and authentication services
- Under certain specified government acts and regulations, it can be searched to verify your identity without your consent
  - e.g. you've died and the coroner wants to ensure it's you and not someone else
  - You've been arrested and the police want to verify you're who you claim to be
- It can be searched, with citizen consent, across the country and different regional vital stats services
  - e.g. you're applying for a job and the employer wants to ensure that you are you
  - You've moved from one province to another and you are going to apply for a driver's license or care card
- Birth registrations will use, at a minimum, a biometric sample from the baby
  - Biological samples will be digitized and then the sample destroyed
  - Biometric data such as fingerprints and an iris scan may be obtained either at birth or, at an approved age by the act
  - These will then be added to the birth registration record
  - DNA has the ability to profile people

        - Therefore, after consideration, the author recommends against the use of DNA since governments can change and the risk is too high for mis-use of DNA
- Birth registrations, will use at a minimum, biometric samples from the parents which are then linked to the birth record
    - Recommend using fingerprints and iris scans
- The biometric data obtained will ONLY be used for identity verification
    - i.e. it won't be used to authenticate the identity
        - That's the job of other government and/or third-party services separate from the vital statistics service

Where Does it Live?

The vital statistics/civil registration service must exist on a separate network, in secure data centres, with high availability, that is protected from physical and electronic attacks as well as resistant to electro-magnetic pulses. The biometric data exists only electronically (biological samples are destroyed). If the biometric data is destroyed by an electro-magnetic pulse (like the "Railroad Storm" or the "Carrington Event") then "poof!" goes the heart of the identity trust in the region/country, i.e. the "cloud "is not the solution for this.

The security used for this, physical and electronic, must be VERY HIGH to convince citizens it won't be breached. No back doors to security services must exist. The legal trust of identity resides within this database.

Refer to "When Our Legal Identity Trust System Goes "Poof!"

What Doesn't It Do?

It won't:

- Allow for any type of research on the biometrics contained within the vital statistics database
- Allow for any individual or mass query of the database by any government ministry or agency at the municipal, provincial or federal level unless specified under an act
- Store personal information about the citizen e.g. addresses, phone numbers, email addresses, health or tax records, etc.
- Authenticate the citizen online
    - That's the job of provincial and federal identity and authentication services
    - HOWEVER, note that before a citizen can join these services, their identity will be verified through the provincial verification service

Can You Give Me an Example?

Let's use healthcare as an example.

There should be only one physical identity per person for every citizen. The state/provincial identity verification system is the source of truth for this. Landed immigrants will be processed by the federal government and then entered into whichever state/provincial jurisdiction the person moves to.

Once you're in the system, i.e. born or a landed immigrant, then with your consent (or your parents/legal guardian consent if you're underage), your identity can be verified to other government agencies and/or third parties for which you can then receive other tokens, e.g. health care cards, student numbers/cards, driver's licenses, passports et al.

So, if you're going to get pharmaceuticals and health care paid for by the government, you need to verify your identity to get a health care card in the local jurisdiction you're living in. There will only be one health care account per citizen since it's tied to the identity verification system.

For example, Jane Doe can't have two health care cards in a region where she's living since her identity is verified with the state/provincial identity verification service for only one card. If Jane shows up claiming she's not Jane or, that she's just moved here (when she hasn't) or, that she's lost her card and requires a new one, with her consent, she'll provide a biometric, her identity will be verified and she'll only have one account.

This way the federal government and the state/provinces now know exactly how many people should be receiving health care. Further, when Jane dies, the coroner service will obtain a biometric from Jane's body and then verify it's Jane in the state/provincial registry or, if it's not found there, by searching the other state/provincial vital stats identity verification service. It will then create a death certificate for Jane. According to state/provincial laws and regulations, the identity verification service can then publish Jane's death and push this out to other government agencies. This way people can't fraud a dead person for health care accounts, etc.

If you move to another jurisdiction you can choose to do the following:

- Live off the grid and not let anyone know who you are
    - This is your right
- However, if you're wanting health care treatment, etc. then you will have to notify the state/provincial government you exist and then, with your consent, have your identity verified, before the other government services can then be engaged
    - There are of course exceptions to this
        - e.g. you're in a car crash or house fire, etc. and you need medical treatment now
            - You will be provided care first to keep you alive
            - Then your identity will be verified

Has Any Country Done This?

Estonia has. In 1999, they created the "Identity Documents Act". It specifies, at the age of 15, citizens provide biometrics including fingerprints, iris scan and facial recognition. This is then added to their central population registry.

How is What I'm Proposing Different Than What Estonia Has Done?

- Refer to the paper "Creating Estonia Version 2.0 - Adjusting for Changes From 1999 to 2018"

Requirements for Longer-term Research on Using Baby Fingerprints

Dr. Anil Jain and his team at Michigan State University published "Fingerprint Recognition of Young Children" in September 2016 (http://biometrics.cse.msu.edu/Publications/Fingerprint/Jainetal_ChildFingerprintRecognition_TechRep_MSU-CSE-16-5.pdf). It shows promising results of obtaining and using baby fingerprints to successfully differentiate identities. I believe that a longer-term study needs to be done to confirm this.

Biometrics Are Not all "Golden"

What I am proposing will substantially reduce identity fraud by linking the identity biometrically to the person. However, it doesn't mean that identity fraud will be eliminated. Why?

Each type of biometric has different equal error rates, i.e. where false acceptance = false rejection. Biometrics like DNA, fingerprints and retina scans have low rates which is why they are used for identity verification.

However, these are prone to attack by the readers used to obtain the biometrics. For example, in this paper "Universal 3D Wearable Fingerprint Targets: Advancing Fingerprint Reader Evaluations" it documents how fingerprint readers can be spoofed. This paper in 2017 documents different techniques to foil biometric readers.

Thus, it is quite likely that over the coming years, government and financial institutions will play a cat and mouse game with organized crime, upgrading readers as new attacks are made. In the "Biometrics and Government" paper it calls out for independent institutions to continually test biometric readers and publish independent equal error rates.

Refer to "Why We Need New Biometric Laws Protecting Our Privacy".

Use Identity Federation and/or Self-sovereign Identity/blockchain with the State/Provincial Identity Verification Services

Traditional Identity Federation

Let's say that a citizen wants to open up a bank account. They would enter a local bank and first of all give their consent to the bank to obtain a biometric. The bank would "federate" with the state/provincial government identity verification service, securely sending the biometric to it. The service would then receive back confirmation of the potential new customer's identity and their legal name.

The bank would also obtain from the citizen their agreement to query a separate state/provincial government identity and authentication service. The bank would federate with this service and receive back citizen address information plus any additional information the citizen has consented to.

The bank would now know who the citizen is, where they live and then be able to open up a bank account with them. The same type of federation services can be used when the citizen wants to receive health care, social services, education, etc.

Self-Sovereign Identity/Blockchain

A citizen could apply online with a bank to open up a new bank account. With the citizen's consent, they would supply the bank with attestations from the vital stats that they are who they claim to be (e.g. using something like Sovrin). This could be instantly verified via blockchain.

With their consent they will also provide the bank with attestations about where they live, etc. This might come from a government agency, such as identity and authentication services, or elsewhere. The bank would then verify this attestation via blockchain.

Offer Citizens the Option of Centrally Managing Their Identity Information

The state/provincial digital vital stats service isn't the place where citizens contact information exists. As noted earlier, it should exist in state/provincial identity and authentication services. The government identity and authentication service should offer the citizen the option of centrally managing their identity information, such as phone numbers, address, etc. If the citizen decided to do this, they provide their consent to the service. They also specify parties they want to notify of the changes.

When a citizen makes a change, they authenticate to the central government identity and authentication service and then make changes to their identity. As soon as they have done this, the central identity and authentication service then securely sends out notification to all parities required by law as well as optionally specified by the citizen.

Note that this service is optional. If a citizen wants to live off the grid or, not inform parties of their identity changes, then this should be allowed, excepted where required by law.

Summary

We are in a new age where old paper based vital stats services no longer work to verify an identity. As the papers "Why We Need to Rethink Our Vital Stats Laws", "Why Your Digital Consent Matters – Including Sex" and "Why We Need New Biometric Laws Protecting Our Privacy" points out, there needs to be new laws and regulations protecting a citizen's biometrics and tightly controlling how the new age vital stats service works.

Citizen privacy groups must be consulted in the design of the new vital statistics acts, regulations and facilities before the services are created. By doing this, the government can show it will implement a service that protects citizen privacy.

What Estonia showed the world in 1999 was the importance of having one physical identity per citizen. They then leveraged this to change their economy, today offering more than 1,000 online services to their citizens. Most legal documents in Estonia are signed by digital signatures since the banks and courts trust the underlying government verified identity.

As the paper "Creating Estonia Version 2.0 - Adjusting for Changes From 1999 to 2018" **points out the scientific, technical and fraud landscape is different than in 1999**.

I believe the strategies suggested in this document:

- Addresses challenges from identity fraud and human cloning
- Offers citizens biometric privacy and new consent laws
- Sets the stage for governments and industry to leverage new technology protocols that didn't exist in 1999:
    - Open ID Connect
        - A modern identity federation protocol used by over 1 billion people/day
    - TLS 1.3
        - The most recent protocol used to protect data transmission on the internet
    - OAUTH Framework
        - A framework for authorization
    - Kantara UMA/UMA Fed
        - A new protocol offering citizens the ability to centrally manage their consent across many different enterprises
    - SCIM
        - A protocol allowing for different enterprises to securely share identity information
    - Self-Sovereign Identity
        - Protocols allowing one to store their own identity data on their own devices, and provide it efficiently to those who need to validate it, without relying on a central repository of identity data
        - Sovrin
        - Uport
        - Veres One
    - Blockchain
        - A growing list of records, called blocks, which are linked using cryptography and are readable by the public

It will substantially reduce identity theft and provide greater security to citizens over their identity and how their biometrics are used. It will also enable the economy to flourish by enabling a high degree of trust by third parties and governments in who the identity is.

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."