Why We Need to Rethink Vital Stats Laws

Copyright: 123RF

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

TABLE OF CONTENTS

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

This paper deals with Vital Stats/Civil Registration laws.

All papers are available at my website http://hvl.net/papers.htm.

Why We Need to Rethink Vital Stats Laws

What was once thought of as science fiction, human cloning, is now nearly upon us. We've gone from Dolly the Sheep in 1996 (first mammal cloned), to early this year monkeys being cloned to being able, for a price, to clone our pets. Regardless of if this becomes legal or not, our identity verification systems must be able to differentiate human clone 1 from human clone 2 from the rest of the population at birth. Our current vital stats system, i.e. registries for birth, name/gender change, marriage and death are not prepared for this. Then there's the issue of being in control of our identity…

We are forced to give and re-enter the same information about ourselves to different levels of governments and third parties like banks, telco's, schools, retailers, etc. over and over and over again. We have effectively lost control of our core identity. Then there's the issue of being able to act anonymously…

When we walk into a bar or, want to buy cigarettes or alcohol, we are forced to present a document, usually a driver's license, that has our name, address, data of birth and a picture on it. Instead of being able to act anonymously, we are using identification designed for one purpose, i.e. driving a car, for another, identity verification. Then there's identity verification issues…

In the late 1800's, birth registry systems were created registering the birth of a person. Their parents were given a birth certificate. In these times, they were very hard to forge. Thus, if a person had a birth certificate in their possession, it was likely them. This spread all over the world.

If one reads laws pertaining to obtaining a bank account, health care account, driver's license, passport, et al, one finds that a birth certificate is common in all of them. So much so that in security circles birth certificates are called "breeder documents" since with them, one can obtain almost all other forms of identification.

This no longer works. Today, birth certificates are easily forged. They don't tie the person holding them to the identity themselves.

Taken all together, i.e. cloning, loss of identity control, inability to act anonymously and ease of fraud of birth certificates, one can see that it's time to rethink vital stats. We need a new age vital stats system that will serve us for the next 100 years. So, what's involved?

The Business of Identity Management

New Laws and Regulations

There are three types of new laws required protecting our privacy:

- Biometric laws
- Consent laws
- Vital stats laws

The first two, i.e. biometrics and consent laws, are required as foundational laws that the new vital stats laws can be then built upon.

New Age Vital Stats Law and Regulations

Here's what the new age vital stats law and regulations include:

- Biometrically tying the identity from birth to the identity registered
  - DNA is possible BUT many people don't like the idea of a central DNA database on everyone
  - Fingerprints are possible
    - In many papers, I have called for more longitudinal research to be done on the work of Dr. Anil Jain of Michigan State University on fingerprinting babies
    - Hypothetically, assuming this bears out, then the laws must be written such that a baby's fingerprints are obtained at birth
  - Iris is possible
    - I have proposed that when a child enters their first year of school, an iris scan is obtained and entered against their birth record
  - Thus, from the get-go, i.e. birth, a citizen has a high degree of identity assurance, i.e. biometrics tied to their identity
- Use of biometrics to differentiate clone 1 from clone 2 from the rest of the population
  - In other papers, I have suggested that research be done to see if fingerprints and irises are sufficient to different clones from the rest of the population
    - If so, then there is no need to obtain DNA from the citizen
- Separating identity verification from identity information and authentication services
  - In other papers I outline a identity privacy principle
    - "A citizen should be able to live off the grid if they so choose"
  - This means that governments shouldn't have one central "mother of all databases" for all citizens
    - Identity verification MUST be separate from other government databases where citizens input where they live, their contact information and provide authentication biometrics
- The identity verification database:
  - Must be only a "one way in" system
    - i.e. no biometrics ever leave the database and go out
  - Must not be able to be trolled or used to profile people
    - i.e. it's only used to verify an individual

The Business of Identity Management

- o Must be on its own separate network
- o Must be able to withstand EMP events (Electromagnetic Pulse)
    - ▪ In the 1800's there was the "Carrington Event" and in the early 1900's there was the 'Railroad Event" that would wipe out most computer servers on the planet. If this happens with the core identity verification data, then "Poof" goes the heart of our legal trust system
    - ▪ So, in other papers, I say that EMP resistant data centres must be mandated by law to store the core vital stats information
- • Must give the citizen control of their identity information, except where mandated by laws
    - o I have proposed that vital stats systems use blockchain and Sovrin
        - ▪ This would give the citizen control over their vital stats information with them deciding when and how to use it
    - o However, some citizens might not have access to digital technologies to use it and/or decide to not use it
        - ▪ Therefore, I have recommended that physical cards be used which the citizen controls
            - • These cards would have signed digital attestations about the citizen which they can then use by sliding their card through a card reader and providing a 4-digit pin
- • Give the citizen the right to act anonymously
    - o When a citizen comes of age, they would go to a vital stats office, present some biometrics to confirm who they are and then have their picture taken
        - ▪ This would be digitally signed by the vital stats service
    - o They would then be given a signed digital attestation and/or a physical card enabling them to act anonymously
        - ▪ For example, when Jane Doe walks into a bar she would provide her anonymous vital stats digital attestation from her digital wallet
            - • The bar would then check the signature against the vital stats system to confirm it is legitimate
            - • Jane's picture would then pop up
            - • Assuming they match, Jane would be let in without having to give away any other information about herself
- • Issue a government issued digital certificate to the citizen when they reach age of majority
    - o This is something Estonia has done for many years
    - o It allows citizens to digitally sign documents
        - ▪ This rapidly picks up the pace at which an economy moves since bank et al trust the digital signature
- • When the risk rises, e.g. a citizen applying to open up a new bank account, the citizen will provide some biometrics to the bank which are then verified against the vital stats database
    - o I wrote a paper "Turning Identity Assurance on its Head" that describes this in greater detail

- Enable parents or legal guardians to act digitally on behalf of their child using vital stats issued digital attestations for the child
- Enable legal guardians of adults to act on their behalf using digital attestations signed by the vital stats service
- Tie the death record to the identity biometrically if biometrics are available at time of death
  - Assuming that fingerprints and irises are available at time of death, these should be used to help verify the identity of the person who has died
- Have strong internal controls on accessing vital stats data
  - The risk of an insider attack is great
  - To mitigate this risk requires numerous internal controls to protect the data
- Protect the endpoints on the vital stats network
  - The endpoints must be protected to thwart attacks such as denial of service and masquerading
- Use TLS 1.3 or later versions to protect the data in transit with the vital stats service
  - This will mitigate risks of man in the middle attacks
- Finally, I have also written that security for the vital stats system should be published such that it can be tested out, similar to the concept of open source software
  - The security MUST NOT be secret, since, over time, this leads to potential security breaches as new technology appears
  - Processes need to be in place to rapidly change encryption methods and business processes when potential risk factors rise

Summary

It's time to change our "old school" vital stats system. As this paper shows, it's no longer able to protect us in the digital age we live with cloning on our doorstep. As I have written about before, "**Instead of rushing into this, a pragmatic approach needs to be taken to address this, based on the privacy principles**."

We need to 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.

The Business of Identity Management

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."