"Where Shit Happens" – Rethinking Civil Registrations in Remote Locations

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

TABLE OF CONTENTS

Note to Reader I:

This is the second last paper in the series. In it I examine the challenges implementing a new age civil registration service in remote locations.

While agencies like the UN, UNICEF and WHO are working hard to get even basic birth registration done in many areas of the world, I am now complicating it by proposing biometrics be obtained from the baby and parents. This complication extends beyond the secure data capture (often in very challenging situations) and into criminal and political spheres.
Why?

I envision tying the identity biometrically to the registration will actually decrease potential identity fraud and thus increase the amount paid by malicious people to obtain a fraudulent civil registration. It will also create new problems for marginalized people trying to cross borders.

I've realized from my work leading large Fortune 500 and government teams doing identity projects that one of the most important things is to get as close to the end user as possible. To put it bluntly "shit happens." It's understanding the deployment challenges where the "shit happens" that one learns to build exceptions into their design and to operationalize it such that it works out in the field as well as in a large urban centre.

I welcome your comments and criticisms of this paper.

Note to Reader II:

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"

The New Way

As noted above, in Note to Reader I, I am proposing that biometrics be obtained from babies, at birth, as well as those of their parents to verify them and the baby. The type of biometrics is up for debate.

In my 2006 paper, I proposed obtaining DNA. I received a lot of criticism which, after reflection, I agreed with. The danger of using DNA is the ability for governments to profile people.

In later papers, I propose doing further longitudinal studies on the work of Dr. Anil Jain and his team to confirm that baby's fingerprints can be used at birth and through their life. I also propose that on the child's first year at school, their iris scan be obtained and entered against their birth registry.

Finally, I also propose that research be done to confirm that a fingerprint and iris scan are sufficient to differentiate human clone 1 from human clone 2 and the rest of the population.

Let's hypothetically assume that all of the above bears out resulting in DNA not being used.

I always tell my teams to follow the processes from the beginning to the end. We examine design requirements, associated costs and training for each stage, end user experience as well as potential attack vectors and mitigation measures. In the following sections, I view it from all of these different perspectives.

Registering a Newborn

Dr. Jain's team has done work on fingerprinting babies who are 6 hours old. This must work in the following settings:

- Remote villages
- First aid posts
- Urban

Design Requirements

The remote villages are the hardest to design for. They likely don't have electrical supply, limited or no cell phone coverage and can be unsterile. If the design can work for these locations, it will be able to work in any urban environment.

Biometric Fingerprint Readers:

- The reader must have enough resolution to differentiate newborn fingers
- It must be durable enough to be accidentally dropped into things like feces, be easily cleaned up and still work
- It needs to be electronically matched to the device that's attached to the biometric to prevent a "switch and play" scenario where a malicious person obtains a different reader they can control, switches it with the assigned biometric reader and then successfully uses it

- The reader must be able to have its own digital certificate securely stored within the reader to be used in securely connecting the reader to the data recording/telecommunications device. This mitigates risk of a malicious person attempting to modify the transmission between the reader and the computing device for their own use
- Its electrical consumption must be obtained via the data entry/telecommunications device it's attached to
- The reader must be sealed physically to mitigate the risk of a malicious person trying to take it apart and modify it
- Must be assigned its own unique identifier which is then registered in the central civil registry system as being used for a particular reading
    - This identifier must be secret and remain unmodified from any administrator or person
- Must be able to withstand significant temperature differences, e.g. hot and cold, to remain operable in inhospitable climates and be water and sand proof
- Must be cost effective to purchase to increase the likelihood of use in remote areas where budgets are very tight
- Must be resistant to an attack where a malicious person uses:
    - A fake finger to attempt to register as a newborn
    - Adult fingers to try to register as a newborn
    - Poor enrollment processes are used resulting in only partial fingerprints

Biometric Iris Reader (for scanning the parents to confirm their identity):

- Must have the same features described above for fingerprint readers
- Ability to detect a malicious person using:
    - A photo of an iris to masquerade as a person
    - Use of an eyeball to masquerade as a person

Reader Data Entry/Telecommunications Device:

- Muse be physically secure preventing a malicious person opening the device, altering it and then using it for their own purposes
- Must be able to authenticate the person who's in charge of taking the biometrics.
    - Possibilities include the use of:
        - Voice
        - Fingerprints
        - Iris
        - Facial recognition
        - Secret
        - Other?
    - An option is the authentication can be securely done on the device without requiring telecom access
        - However, this must be secure allowing for no one else to access the secure data storage for the authentication biometrics and/or the secret
- Data entry can be done via the following possibilities:

    - Keyboard type pad
    - Voice
        - Note that the use of voice must often be trained to the operator's voice
        - This may or may not work in remote locations where no training is available to register the voice pattern
- Data entry must be securely:
    - Time and data stamped with no ability to modify these by either the operator and/or a malicious person
    - Stamped with the operator who has successfully authenticated with no ability to modify these by either the operator and/or a malicious person
- Telecommunications:
    - Must be able to operate in the following conditions:
        - Use of a satellite phone connection in areas where there is no good cell coverage
        - Use of cell phone coverage in areas where it is available
        - Optionally, store the data on the device until it's brought into range with cell coverage and/or attached to a government network
            - However, this then negates the option of immediately verifying a biometric when it's taken remotely
                - Use cases need to be created allowing for all the possible permutations where an identity already exists, etc.
    - All connections MUST BE SECURE
        - Use of TLS 1.3 or later approved algorithms
        - Use of digital signatures for the data recording device and the vital stats service the device will be communicating with
        - Operator should also digitally sign the communications
- The data entry/telecommunications device should be able to operate on its own power supply via a battery, solar charging, etc.
    - The length of this between recharges should be long to ensure the device works over long periods of time remotely
- It must be low cost to allow for wide usage in tight budget environments
- It must be lightweight and durable, meeting the same requirements that the biometric readers use

Combined Biometric Readers, Data Entry and Telecommunications Device:

It's hypothetically possible to create a combined unit meeting the requirements illustrated above for biometric readers and data entry/telecommunications devices. One unit is then used.

I like the concept of this if it can be tied to low time use of built in satellite phone connections. The operator securely authenticates to the device, uses it to record different biometrics, inputs the data using voice and/or keypad, verifies the identities (parents and newborn) and then is done.

The unit must be small enough to fit into a medical worker's bag such as this, along with other medical devices and materials:

Copyright UNICEF https://shop.unicef.ca/emergency-first-aid-kit

Alternate Attack Vectors

At the beginning of this paper I made a prediction; identity verification fraud will be reduced by tying the biometric to the identity, resulting in higher prices for fraudulently obtained identities. It's highly likely malicious people/organized crime will attempt to insert different identities into the birth registration process. Examples include:

- Using women claiming to have a baby they have with them who isn't theirs
- Forcing and/or paying birth registration personnel to register a baby and parents
- In the future, inserting human clones into the birth registration process
- Inserting false identities into the civil registration database from within the civil registration system

How can these be mitigated? Potential solutions include:

- Use of metadata to screen out fraudulent people including timing, data of birth, location, if the birth was premature, person who registered the birth, etc. Examples include:
    - Matching a birth mother to previous births
        - E.g. if a woman is registering a birth 3-6 months after having another birth registered and the child is full term then business processes would be used to determine all births the woman has had and investigate them
    - Matching potential fraudulent births to the person who entered the birth looking for patterns
    - Designing the authentication methods for the person registering people to determine if they are under any type of stress and thus flagging the entries will allowing them to be made to protect the worker

- Having special business, technical and reporting processes for adding in any births, name or gender changes
  - It should be very hard for any additional entries to be made into the system
  - These should require the registrar of the systems permission with their digital signature and authorization to make
  - They should also be publicly reported

A corrupt civil registration management will find ways to bypass internal and external control systems. Funding agencies, who are paying for a new age civil registration system to be implemented in developing countries, can design the civil registration's biometric readers, data collection/transmission devices, training, business processes, technical internal software processes and reporting processes to mitigate some of these risks.

Cross-Border Attack Vectors

People cross borders for a variety of reasons, some legitimate and others not. Here are two scenarios to consider:

No cross-border sharing of identity information
If an identity in one country, who's biometrically tied to their government's identity and their parents' identities, crosses a border claiming to be someone else, then without cross-border sharing of civil registration data or, by tying the civil registration to identity and authentication data which is shared, then porous border control will result. Therefore, biometrics on their own are not a panacea for border control.

Cross-border sharing of identity information
If an identity, biometrically tied to their identity and their parents' identities in one country, crosses a border claiming to be someone else, they will likely apply for work, government benefits or education. All of these, in the future, will require identity verification from the civil registration/vital stats service. They won't be in the database.

As a result, they will likely lie, claiming to have been born in a remote portion of the country and missed in the civil registration processes. If the country has legal arrangements with neighbouring countries, then special business/legal processes can be taken.

The person in question might have to give their consent for their biometrics to be searched in the neighbouring countries. If they refuse to give their consent, they can be deported.

If they agree, then their biometrics can be searched against the other countries vital stats databases to see if they exist. If they are found to exist in another country's systems then different business processes will be used as opposed to if they are not found in the databases.

What Happens When There are No Fingerprints or Iris Biometrics Available?

Some babies will be born that don't have fingers or eyes. Further, people may have life events where they lose limbs and/or eyes. Use cases need to be built acknowledging this. Other biometrics can be considered and entered against the name for the identity in the civil registration database.

Training Requirements

In urban centres, it's more likely that medical personnel of some sort will be used to obtain baby biometrics. However, out in remote villages, this may or may not be the case. Therefore, to properly enroll a newborn requires some training to use the devices listed above.

Questions to be answered include:

- Biometric enrollment training processes
- Device operation requirements
- Training the device to understand the user if voice is used to enter data
- Business process training
- Detecting fraud training
- Telecommunications training
- Device failure notification
- Lost device reporting training
- Certification training

Using New Age Civil Registration for Emergency Response

I was the identity architect for a government's citizen identity and authentication system. One of the questions the team discussed was how to identify people in a disaster situation? Let's hypothetically assume that a combined biometric reader/data entry/telecommunications device is created that is low cost and rugged. Now let's apply this to a disaster recovery operation a government and/or third-party NGO's might be involved with.

The same units used for registration could be configured to be just readers. Disaster recovery personnel could then find survivors, obtain their biometrics and now know who they are. If the civil registration system was used to create entries in a separate identity and authentication system, similar to the one the team I worked on designed for a government, then the government/NGOs would then be instantly able to determine their contact, health information, etc.

Rescue workers finding children on their own would be instantly able to determine who their parents/legal guardians are.

Recovery teams working on identifying dead people, using the same units, would be able to quickly determine who they are. If biometrics are available, these could then be matched against the civil registration database.

All of what I've described above can assist survivors and rescuers/recovery personnel for most types of natural disasters. However, I suspect that there is one type of natural disaster that this won't work in…electromagnetic pulse events (EMP). If the government has created EMP proof data centres, then the actual civil registration data will survive and be intact. That's the good news.

The potentially bad news is that the telecommunications will likely be destroyed. This is dependant upon the EMP proof satellite systems, cell towers, telco and electrical distribution. Today, if this type of event was to occur, it would likely take months or longer to recover.

It's a New Age – A Challenge to Enterprises and Individuals

We are at the beginning of a new identity age. Our old ways of doing things, i.e. using paper and/or electronic records not directly tied to the identity, no longer work. If we can securely and inexpensively design units, telecommunication processes and civil registration systems to work well for remote areas, then this can likely be easily scaled for urban areas.

Health care and government workers on the front lines, out where "shit happens", are one of the most important resources in designing a new age civil registration system. They can provide the exact use cases to then design the devices mentioned in this paper.

This paper challenges technology, biometric and telecommunications enterprises and individuals to design a combined biometric reader, data entry and telecommunications device mentioned in this paper. The world needs this type of device to verify and register identities, be they newborns, infants, children or adults. The same device can also be used in disaster response efforts.

It's time to rise up to the new age and use our abilities and knowledge to create a new age civil registration system that will work 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."