What New Age Civil Registration Systems Won't Do

Author: Guy Huntington, President, Huntington Ventures Ltd.
Date: Created September 2018/ Updated Feb 2020

Note to Reader:

I have been writing about rethinking civil registration systems since 2006

- "The Challenges with Identity Verification"

Over the last year and a bit, I have written 32 papers, including two proposals, on the impacts from the technological tsunami. Here's a listing of them, by subject area, with links to each one:

- Thought Papers
  - Artificial Intelligence & Legal Identification – A Thought Paper
    - Artificial Intelligence & Legal Identification
  - Human Migration, Physical and Digital Legal Identity – A Thought Paper
    - Human Migration, Physical and Digital Legal Identity
  - Digital Twins/Virtual Selves, Identity, Security and Death – A Thought Paper
    - Digital Twins/Virtual Selves, Identity, Security and Death
- Proposals and Discussion Paper:
  - Bot Legal Identity Proposal
    - Proposals for Identification of Bots (Physical and Virtual Robots)
  - Human Legal Identity Proposal
    - Proposals Paper – Incremental Approach to Implementing New Age Legal Identity
  - Background Information on Legal Identity, Data, Consent and Federation
    - Background Information on Legal Identity, Data, Consent and Federation
- Example story of an identity's lifecycle
  - The Identity Lifecycle of Jane Doe
- Technological Tsunami Wave of Change
  - Harnessing the Technological Tsunami Wave of Change
- Legal Privacy Framework for the Tsunami Age
  - Legal Privacy Framework for the Tsunami Age
- One-page summary
  - One Pager - The Age of AI, AR, VR, Robotics and Human Cloning
- Technological Tsunami and IAM
  - Technological Tsunami & Future of IAM

- New age identity, data, and consent
  - Privacy Gone – AI, AR, VR, Robotics and Personal Data
  - I Know Who You Are & What You're Feeling - Achieving Privacy in a Non-Private World
  - Consent Principles in the New Age – Including Sex
  - Policy Principles for AI, AR, VR, Robotics and Cloning – A Thought Paper
  - Legal Person: Humans, Clones, Virtual and Physical AI Robotics – New Identity Principles
- Kids and Parents Privacy
  - Young Children Data Privacy Challenges in the Tsunami Age
  - Kids Privacy in Non-Private World - Why Even Super Hero's Won't Work
  - Children & Parent Privacy in the Tsunami Age
- Robotics, Clones, and Identity
  - Legally Identifying Robots?
  - Rapidly Scaling Robot Identification?
  - Virtual Sex, Identity, Data & Consent
  - I'm Not a Robot
- New age civil registration legal identity framework
  - "Why the New Age Requires Rethinking Civil Registration Systems"
  - "What New Age Civil Registration Won't Do."
- New Age Assurance
  - "New Age Assurance – Rethinking Identity, Data, Consent & Credential"
- Deploying AI, AR, VR, robotics, identity, data and consent in challenging locations
  - "Where Shit Happens"
- Protecting the civil registration/vital stats infrastructure
  - "When Our Legal Identity System Goes, "Poof!"
- New age architecture principles summary
  - "New Age Architecture Principles Summary"
- 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"
- Creating Estonia Version 2.0
  - "Creating Estonia Version 2.0 – Adjusting for Changes From 1999 to 2018"
- New age civil registration/vital stats design, implementation & Maintenance Vision
  - "Guy's New Age Civil Registration/Vital Stats Design, Implementation & Maintenance Vision"

All papers are available off my website at https://www.hvl.net/papers.htm.

TABLE OF CONTENTS

Executive Summary

The paper begins by discussing the non-private world we are quickly creating. Governments, particularly police and intelligence agencies, will want to collect as much information about you as they can to determine if you are a potential threat. The danger is allowing these agencies to use the new technologies without putting in safeguards.

To counteract this, the paper identifies what a new age civil registration system won't do:

- Biometrics/Behavior Data
  - Won't use biometrics/behavior data able to profile you
  - Clones Will be Legally Identified but Not Identified as a Clone
  - Biometric/Behavior Data Will Be Stored Off-Line and Not Used On-line
  - Won't Use Any More Biometrics/Behavioral Data Other Than to Legally Identify a Person
  - No Biometrics Will Be Shared with Other Government Agencies, Third Parties or Other Jurisdictions
  - Changes to Any Biometric/Behavioral Data Within the Database Can't Be Easily Done
- Digital Identity
  - The New Age Civil Registration System Won't be Centrally Managing the Digital Identity
- Verifying an Identity via Biometrics/Behavior Data
  - Won't Accept Usage of Weak Biometric Readers
  - Won't Use Weak Security and/or Business Practices to Connect to Biometric/Behavioral Data Readers
  - Won't Accept Death Registrations Without a Biometric Unless Otherwise Unobtainable
- System Level
  - Won't Contain Any Other Identity Information Other Than That Provided for Initial Registration
  - Yes or No Answers ONLY, Unless Otherwise Prescribed by Law
  - Robotic Registration Data Won't Be Released Without Owner or Legal Law Requirements
  - New Age Civil Registration Service Will Not Be Directly Connected with Other Government Identity Systems
  - Doesn't Allow for Mass Requests to Troll the Database of Identities
  - No Authentication
  - Won't Work on Its Own

It ends with the statement:

Citizens and privacy groups should ensure governments adhere to the principles contained within this paper. These are all legal stepping stones to create privacy in a non-private world.

What New Age Civil Registration Systems Won't Do

Introduction

The paper "Why The New Age Requires Rethinking Civil Registration Systems" describes the incoming technological tsunami composed of:

- Artificial Intelligence (AI)
- Augmented Reality (AR)
- Virtual Reality (VR)
- Robotics (both virtual and physical)
- Genetic engineering
- Nanotechnology
- Wireless

The paper goes on to describe why a new age civil registration services is required. So, what's the point of this paper?

As the paper "Privacy Gone – AI, AR, VR, Robotics and Personal Data" and "I Know Who You Are & What You're Feeling – Achieving Privacy in a Non-Private World" explains, we are quickly creating what I call a "Non-Private" world. This has serious impacts to our personal privacy.

Industry sectors like retail, entertainment, education and healthcare will quickly adopt the emerging technology to provide personal, finely-tuned, goods and services. Governments will also adopt this to do the same. However, the sword that cuts for you can also cut against you.

Governments, particularly police and intelligence agencies, will want to collect as much information about you as they can to determine if you are a potential threat. The danger is allowing these agencies to use the new technologies without putting in safeguards.

This applies to the new age civil registration service. Thus, to mitigate some of these risks, the purpose of this paper is to identify what the new age service won't do.

Biometrics/Behavior Data

Won't use biometrics/behavior data able to profile you

Some biometrics/behavior data are able to profile people, e.g. DNA. There is a danger a malicious government could take this information, profile certain types of people and use the data to mistreat or even kill them. Therefore, the premise is no biometric/behavior data will be used to legally identify people which has the ability to profile people.

In other papers, I lay out research to confirm fingerprints and iris are enough to differentiate human clones. Assuming this research confirms this, hese two biometrics will be used.

Clones Will be Legally Identified but Not Identified as a Clone

As stated in other papers, Boyalife, a company currently cloning 100,000 cows a year working towards 1 million, had their CEO s publicly stated in 2015 they could clone humans but weren't. Thus, the age of human cloning is now upon us.

Cloned people are people who also deserve their privacy. Thus, the role of the new age civil registration service is to only perform identity verification AND NOTHING ELSE. The underlying database should not be able to be searched looking for cloned people.

Thus, the birth registration will only be able to legally identify a person. Let's say Jane Doe clones herself producing Jane Doe 1 and 2. Jane Doe 1 and 2 will be entered into the birth registration as Jane Doe 1 and Jane Doe 2 with biometrics provided able to legally differentiate them from each other and the rest of the planet's population. Their mother will be listed as Jane Doe. However, there will be no mention they are clones. This mitigates the risk in the future of governments trolling the database looking for cloned people.

Biometric/Behavior Data Will Be Stored Off-Line and Not Used On-line

The biometric data is the heart of being able to legally identify a person. Thus, the great danger is a malicious person or enterprise is able to successfully hack their way into the central biometric database either obtaining the data and/or altering it (an example of this type of attack is illustrated here).

To mitigate this risk, the data will be stored offline in a secure area with only limited, secure access.

While this will help mitigate the risk, it won't help in providing a higher identity assurance to enterprises like banks et al who want to legally confirm it's Jane Doe wanting to open a new bank account with them. Thus, a possible solution is to use derived data from the biometrics and have it available online. Research will need to be done to confirm this is a viable solution.

Won't Use Any More Biometrics/Behavioral Data Other Than to Legally Identify a Person

The new age civil registration service won't use any more biometrics/behavioral data other than the minimum, scientifically proved to differentiate clones and people from the rest of the planet's population. This prevents the building up of a mother of all databases, thus increasing likelihood of attack.

No Biometrics Will Be Shared with Other Government Agencies, Third Parties or Other Jurisdictions

The biometrics are a one-way in system. They MUST never be allowed to leave the underlying database. While the identities can be searched, under law, by other government ministries, people and/or other jurisdictions, there must be no way the biometric themselves will be revealed. This will mitigate the risk of biometric data leakage.

Changes to Any Biometric/Behavioral Data Within the Database Can't Be Easily Done

The new age civil registration system MUST make it very hard to change any biometric/behavioral data within the database. There must be a number of checks and balances to dissuade any malicious administrator to easily make changes to the underlying biometric data.

Digital Identity

The New Age Civil Registration System Won't be Centrally Managing the Digital Identity

I've written in other papers Sovrin/Blockchain be used for the legal digital identity of the person or robot. I've also noted potential problems with this approach because of the use of a secret key which recent cybercurrency fraud has found not difficult to maliciously obtain.

Regardless of which technology is selected, the premise is the citizen, robot or robot's owner should be in control of their legal digital identity, except where otherwise prescribed by laws/regulations, e.g. incarceration. Thus, the new age civil registration service must, in effect, get out of the way of the citizen, robot or their owner who will decide when and where to use their digital identities (both legal and anonymous).

HOWEVER, the new age civil service system must be able to validate the digital certificate they signed the digital attestations with. Thus, when a citizen, robot or robot owner decides to use the digital identity, the civil registration service will attest the digital signature is valid.

In summary, the new age civil registration service MUST NOT centrally manage the citizen's or robot's digital identity.

Verifying an Identity via Biometrics/Behavior Data

Won't Accept Usage of Weak Biometric Readers

For high identity assurance, the new age civil service will use biometrics/behavior data to verify the identity. However, biometric/behavioral data readers can be spoofed. Further, today's best reader can quickly become tomorrow's turd due to rapid technology changes.

What's required is a global independent testing agency to continuously test readers and identify one's now spoof-able. Globally, all civil service systems must change within a prescribed period of the type of readers acceptable. This will mitigate the risk of using weak readers, allowing others to impersonate a person legally.

Won't Use Weak Security and/or Business Practices to Connect to Biometric/Behavioral Data Readers

Third parties, like banks, will likely be using biometric readers to obtain a person's biometrics to send to the new age civil registration service for confirmation the identity is who they claim to be. There are a number of potential attack vectors ranging from the person administering the biometric reader to the actual reader itself to the communication system being used between the bank and the new age civil registration service.

All of these potential attack vectors must have risk mitigation measures in place. However, as previously noted, today's best security solution can quickly become tomorrow's turd due to technology changes.

Thus, globally, continuous testing must be done to see if there are new weaknesses. If there are, all new age civil registration services must be notified and, within an agreed upon time, changes made. This mitigates the risk of a new age civil registration service having weak security and/or business processes, allowing a malicious person to masquerade as another.

Won't Accept Death Registrations Without a Biometric Unless Otherwise Unobtainable

With the rise of cloning, it presents new challenges in validating a person's identity. This includes death. Hypothetically, as an example, let's say Jane Doe 1 clone kills Jane Doe 2 clone yet claiming it's Jane Doe 1. If the biometrics are available at death, they must be used to verify an identity.

System Level

Won't Contain Any Other Identity Information Other Than That Provided for Initial Registration

The purpose of the new age civil registration system is for identity verification only. It MUST NOT be allowed to morph into a regional or national population register with contact information, which can be used to track an identity.

Yes or No Answers ONLY, Unless Otherwise Prescribed by Law

The new age civil registration system MUST ONLY provide yes or no answers to the identity verification. If required, by law, the legal identity information of the parents, date and where the identity was born can be given out. Here are two examples:

Acme Bank wants to verify Jane Doe's identity to create a bank account for her. With Jane's consent, she provides her biometrics which are securely sent to the new age civil registration service. The new age civil registration service provides the bank with a yes.

Jane Doe has been incarcerated. As part of the legal process, she is forced to provide her biometrics to the new age civil registration service. By law, the state can obtain her full legal description from the service. Note however, the service does not contain any contact information etc. about Jane.

Robotic Registration Data Won't Be Released Without Owner or Legal Law Requirements

Similar to the above example, robotic legal identification won't be released without the owner's (and likely in the future the robot's own) consent unless otherwise prescribed by laws and regulations,

New Age Civil Registration Service Will Not Be Directly Connected with Other Government Identity Systems

The new age civil registration service must exist on its own network. If another government service wants to verify an identity via the new age civil registration service it must do so via identity federation.

Doesn't Allow for Mass Requests to Troll the Database of Identities

The new age civil registration system MUST NOT allow any person, administrator, or government entity to troll the database by using mass requests. Careful consideration will have to be given to prevent trolling when automated robotic registration requests are given, blindingly fast.

No Authentication

The new age civil registration service MUST NOT perform any authentication services for citizens and/or robots. Its sole purpose is to provide legal identity verification.

Won't Work on Its Own

The new age civil registration service now needs to be securely connected, globally, to all other civil registration services. While the administration, maintenance, operations and laws/regulations will be local, it MUST be able to be legally searched by other jurisdictions, as and when required by law. Robotic registration is a good example. Therefore, the new age civil registration service MUST not work on its own.

Summary

The planet is in a sea change as the incoming technological tsunami approaches. Old legal frameworks for identity, data and consent now no longer work. This requires a new civil registration system which assists in the citizen having the ability to live privately in a "non-private" world.

However, governments must be limited in how they are allowed to create the new age civil registration system. Some temptations, like integrating this service with other systems and databases which are able to track a citizen MUST be avoided. Therefore, this paper outlines things a new age system won't be able to do.

Citizens and privacy groups should ensure governments adhere to the principles contained within this paper. These are all legal stepping stones to create privacy in a non-private world.

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."

Guy consults globally on the incoming technological tsunami wave of change.