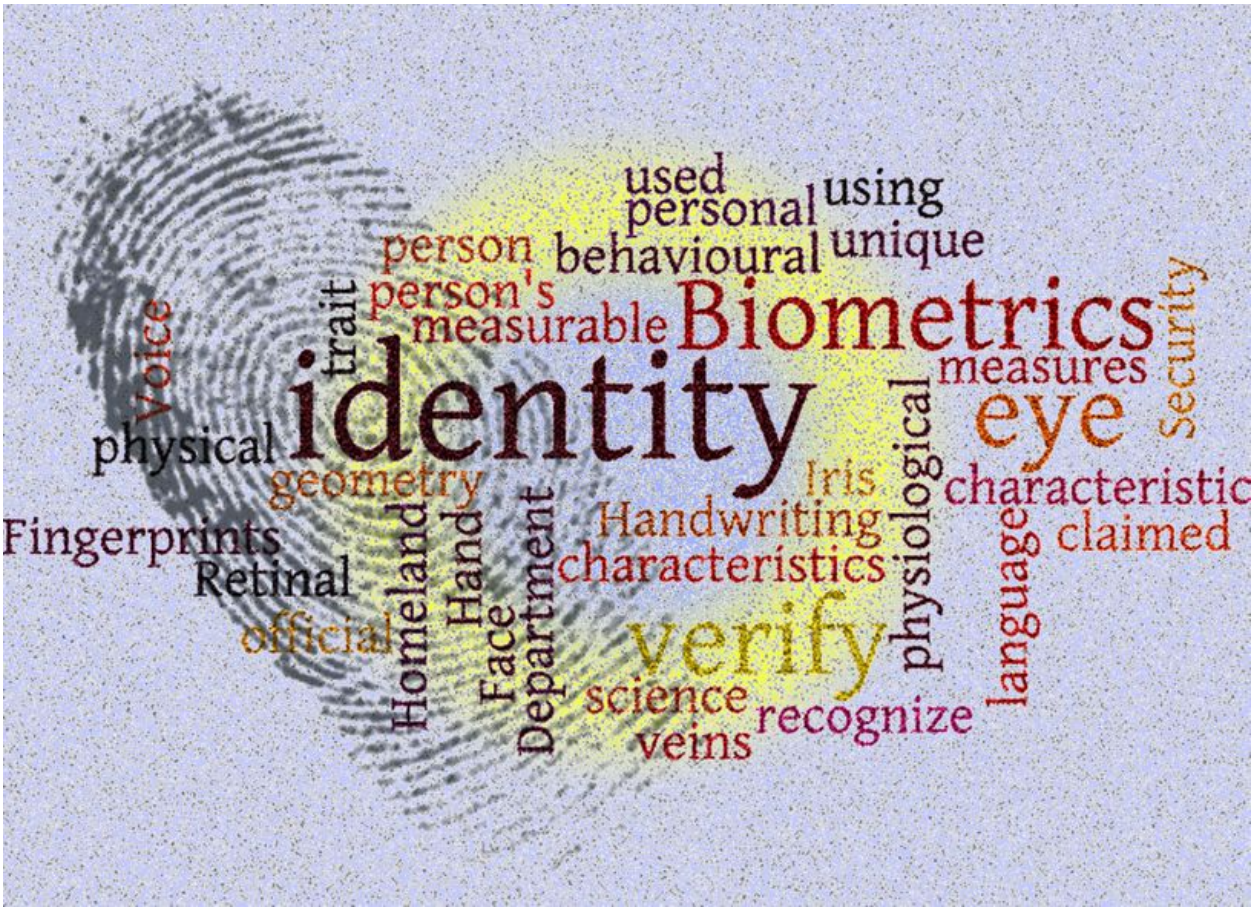
Why We Need New Biometric Laws Protecting Our Privacy



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
  - "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 new biometric laws.

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

Why We Need New Biometric Laws Protecting Our Privacy

Biometrics are currently the rage. For example, Planet Biometrics, announces, daily, new biometric developments and markets. From traditional markets like driver's licenses and passports to new ones such as banks, cars and shopping malls, the use of biometrics is exploding. Yet, all is not golden…

Equal Error Rates (ERR)

Biometrics are not all created equally. There is something called the "Equal Error Rate" (also known as the "Crossover Error Rate"), i.e. where false acceptance = false rejection. This is a measure of the accuracy of a biometric. And here is where the complexity of biometrics begins...

Try to find independent research on equal error rates. For some, like fingerprints and facial recognition, they are readily available. For many others they are hard to come by. Yet, even where they exist, they can be "tweaked" depending on how the use cases are written. That's why many biometric vendors publish their own equal error rates that may or may not be accurate, depending on how the biometric is used.

Some biometrics, like DNA, fingerprints and iris have low equal error rates. This lends them to be used in identity verification. Others, have relatively higher equal error rates that lend themselves towards authentication e.g. voice or, identification e.g. identifying an individual out of a crowd with facial recognition.

Yet, even using a biometric with a high degree of accuracy, e.g. fingerprints or iris might not be reliable. Why? The readers.

Biometric Readers

Not all biometric readers are created equally. Many are prone to spoofing. For example, if you read this paper from last year, it demonstrates many different ways to foil biometric readers. Most citizens are blissfully unaware of this as they use their smartphones, iPads or laptops with different biometric readers.

Then there is the use of the biometric data to be considered…

Biometric Data

We are on the verge of a medical revolution regarding use of the internet of things with our bodies. This research paper, from 2016, documents the exploding industry. Examples include the following:

- Last fall, the US FDA approved their first ever pill that diagnoses if the use has taken it
- Devices like Fitbits are now common, sending data in real time about your physical activities
- Many people now send in samples of their DNA to genealogy companies
- Glucose internet of things monitoring is now becoming more common

Yet, there is a major problem. How is our privacy being protected when we supply our biometrics for verification, identification, authentication or the data from biometric internet of things devices?

Privacy

Answer – Most jurisdictions have laws that pertain to some biometrics. However, there are few laws and regulations speaking directly to how various biometrics can be used, stored, shared, etc.

The result – we, as citizens, are mostly at the mercy of vendors and enterprises that use our biometrics. A simple example…

You have a smartphone that uses one or more biometrics. If you want to change the phone vendor, how do you know how your old biometrics will be stored, archived and/or deleted? Is there any process in place where you can demand the vendor to permanently delete the old biometrics? What laws apply here to assist you?

Taking all of the above together, it's time, we as citizens demand new laws and regulations protecting our biometrics. There should be one central set of laws pertaining to biometrics that other laws can refer to.

With the laws, must come regulations stating how biometrics can be obtained, transmitted, stored, used, shared, archived and deleted. We are in a time of fast-moving technical change resulting in challenges for doing this. Therefore, the biometric laws and regulations needs to be changed as conditions change.

We also need independent testing done of various biometrics, their readers, transmission and storage. This then provides a benchmark for vendors to be measured up against. Continuous testing of biometric spoofing should be mandated by law.

Summary:

Biometrics are not secret. Pieces of you fall off you every minute e.g. skin cells containing your DNA. We leave our fingerprints every time we touch something. Our face, voice, iris, etc. are easily obtainable by technology. This means that enterprises relying solely on a biometric to identify or authenticate you is not good. Depending on risk, additional means should be used, such as something you know and/or something you have.

We are in the midst of a major technical revolution that leverages biometrics, biometric readers and their data to offer us new services. However, the old adage "Caveat emptor" applies. It's time we created new biometric laws and regulations protecting our privacy. Readers can refer to a paper I wrote last Fall "Biometrics and Governments" where I documented the underlying principles that should be used to create these new laws:

- 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 for something other than identity verification 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

If you like the intent of this short paper, please forward it to others to get the discussion going.

Thanks!!!!!!!

Regards,

Guy Huntington

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."