Identity Federation:
Biometrics and Governments

Author: Guy Huntington, President, Huntington Ventures Ltd.
Date: May 2018

Table of Contents

Executive Summary

The paper begins by reviewing historically how identities are verified e.g. birth certificates, driver's licenses, passports, and identity cards. It then discusses these are no longer working as well due to technological changes allowing people to more easily masquerade as another.

To address this, the paper then lays out modern identity assurance principles protecting the biometrics a citizen provides for identity verification as well as for authentication and then discusses each one.

Then biometrics are discussed. The paper first refers to a 2005 paper suggesting that more empirical studies are required to validate commonly held assumptions about biometrics being unique to identify an individual. It then moves onto a discussion of three biometric techniques viable for human identification: fingerprints, iris and DNA.

A set of recommendations are then given, using the identity assurance principles as a guideline. This includes new laws and regulations for biometrics used including creation of:

- Compulsory central government identity verification service
- Optional central government authentication service which the citizen may or may not opt to subscribe to
- Laws and regulations pertaining to citizen rights in any biometric used by governments and/or third parties for authentication
- Independent bodies able to determine biometric equal error rates as well as continually test devices used to capture a biometric to see if the device can be easily fooled
- Inter-government standards

We live in an increasingly small world with rapid technological changes. Our existing identity verification systems were designed for the early 1900s. This was long before the rise of the internet with the fast, easy movement of people between government borders, electronic identity federation between enterprises and genetic cloning.

The use of high identity assurance, i.e. strong identity verification, is required to accomplish things like citizens easily being able to use digital signatures, vote online, conduct large financial transactions, etc. It requires a trusted government issued identity, from the date of birth onwards through an identity's life. We must re-design our systems to answer the question "How do I know if you are really you?" while protecting the citizen's privacy and their biometrics.

Introduction

In today's digital world, identities are often passed from one enterprise to another, often in the form of an attestation by an authoritative party that then provides attributes about the identity to relying parties. At the heart of every identity transaction is the question "Is the identity who they claim to be?" The answer is dependent upon risk, of which there are varying degrees.

In many cases, there is low risk. For example, a relying party might simply trust that the identity is unique, i.e. they have a unique email address.

Other relying parties might want to ascertain that the identity is likely who they claim to be. The authoritative party providing the identity federation assertion is now more liable if they haven't verified the identity, i.e. by viewing and/or recording a government issued document such as a driver's license or a passport.

As the risk rises, the relying party will expect the authoritative source to have done more identity verification. This often means electronic checking of the identity's government issued documents as well as a check against name change and death records.

All of the above use traditional forms of identification developed over the late 1800's through the 1900s such as birth certificates, driver's licenses, passports, and identity cards. It has worked well, providing ways for government, third parties and private citizens to ascertain the identity presenting themselves is who they claim to be.

Governments and large enterprises adopt ways of verifying identities based on risk, i.e. identity assurance. Typically, it is on a scale of 1-4 with an identity assurance level of 1 being a low assurance with little verification and a level of 3 or 4 having electronic document verification and usually obtainment of some biometric from the identity. However, in today's world, these forms of identity verification are no longer working as well. Why?

People are now easily able to produce excellent looking birth certificates by using inexpensive printing equipment. With the price point dropping for obtaining very realistic face masks to use when obtaining a driver's license, the use of facial recognition isn't as valuable as it once was.

Other countries around the world have many people illegally crossing their borders and/or working in the country, often with no identity documents. In refugee camps, biometrics are now becoming more common as a method of identification.

The point of this paper is that the underlying process for creating the initial identity of a person, i.e. a birth certificate, is flawed. It doesn't tie the identity created physically to the birth record. As a result, identity verification systems that rely upon these methods, i.e. drivers' licenses, passports, and identity cards, are easier to fraudulently obtain. This increases risk to enterprises and citizens who rely upon them.

Modern Identity Assurance Principles

In today's world, what is missing is a robust set of laws and regulations protecting a citizen's biometrics that can be used for identity verification as well as authentication. As a result, citizens are rightfully afraid of how their biometrics will be used. So, what principles can be used?

- 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

One physical identity per citizen

The underlying premise of this paper is that each citizen will have only one physical identity, to which is attached their birth, name change, marriage, and death records. The citizen's physical identity at birth is tied to the birth record via biometrics, which can differentiate the person from anyone else on the planet.

A citizen is able to have multiple personas

Citizens often want to live anonymously. They may also have one or many different personas. For instance, Jane Doe might want to be known as Cathy Smith, Gamer Girl, etc. Thus, the identity assurance principle is that while a citizen has only one physical identity, they should be able to have multiple personas physically and/or digitally.

A citizen should have ways of anonymously identifying themselves

There are many situations where a citizen may want to anonymously attest something about themselves; e.g. a person entering a bar or trying to buy cigarettes where there is a minimum age requirement. The government, police, etc. don't need to know that the person is entering the bar or buying cigarettes. The citizen should be able to anonymously provide a biometric which is then electronically sent to the national identity service and an answer sent back indicating whether the person is of legal age or not.

Biometrics will be obtained at birth or in a citizen's early years that uniquely verifies the identity

Any birth registration system must be designed for the future and not the past. The old premise that a citizen is physically unique is now hypothetically in question due to the arrival of genetic cloning. Therefore, any biometrics obtained at birth need to be able to differentiate a person from another who might be cloned in the future or from a genetic twin.

Biometrics used in identity verification must be able to differentiate between genetic twins and human clones

In the spring of 2018, Chinese scientists announced they had successfully cloned monkeys[1]. Thus, what was once thought of as science fiction, i.e. cloning humans, is now nearly upon us. Therefore, regardless of if human cloning is legal or not, the vital statistics services must be able to differentiate between two or more human clones as well as between genetic twins.

Identity verification biometrics 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

One of the fears many citizens have is that the government will be able to use their biometrics inappropriately for things like racial profiling, ethnic cleansing, doing unauthorized research, etc. To address this, each government must adopt very rigorous laws protecting the citizen's biometrics from any unauthorized use including use of the biometrics for research, etc. Countries must adopt global standards for this. No biometric used for identity verification should be able to be exported and/or shared out of the underlying database.

[1] https://www.theatlantic.com/science/archive/2018/01/china-monkey-clones-zhongzhong-huahua/551318/

Biometrics used for identity verification must be securely stored

Any biometrics the government collects must be securely stored. This might include storing the identity information on a separate network with rigorous security.

Governments must not build the "mother of all citizen identity" databases

The attractiveness of attackers trying to obtain access to government identity databases is proportional to the lucrativeness of the identity information contained within. As a result, the national identity verification database should only contain a minimal amount of information about the citizen. Other more sensitive information such as health, credit cards, legal, etc. should be stored in different government databases. Citizens need to know that the government is not accumulating all the information about them, including their biometrics, in one "mother of all 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

Citizens need to know that the biometrics obtained from them for identity verification purposes are only used for identity verification and will not be shared with other governments or third parties nor used for any other purpose including research, etc.

The identity verification service should have the ability of anonymously confirming an identity

The service needs the ability to simply attest that an identity exists without having to reveal a citizen's identity information to a relying party unless requested with the citizen's consent, or when requested under a law that requires the verification service to reply with the identity information.

Any biometric used for authentication purposes, by either governments and/or third parties, must be governed by laws prescribing the following:

Obtaining of recorded citizen consent to obtain and use the biometric

The citizen must be in control of their biometrics and when they are given to government agencies and/or third parties. This starts with obtaining a record of their consent.

The consent must clearly state how the biometric will be obtained, stored, used for identity verification, archived, and eventually destroyed

The laws and regulations need to specify how the biometric will be obtained, stored, used, archived, and eventually destroyed. This will help bring order to an existing chaotic marketplace in which citizens are not currently in control of their biometrics.

Secure storage of any biometrics used to verify the identity

The laws and regulations should specify standards for the secure storage of a citizen's biometrics that governments and/or third parties use for identity authentication. Every enterprise must be accountable for protecting a citizen's biometrics.

No transmission or sharing of the biometrics with other parties without the express consent of the identity

Citizens need to know that a biometric they have provided with their consent to be used for authentication purposes will not be shared with other parties unless they have given consent.

No use of the biometrics for medical research, profiling, marketing, etc. without the express consent of the citizen

A citizen's consent is required if the government agency or third party is going to use the biometric for any other purpose than for authentication.

A process exists for citizens to request that their biometrics can be removed from government and third-party databases

For any biometric other than those used by the government for identity verification, the citizen should have a process where they can request their biometrics be removed from databases, i.e. they are rescinding their consent. The laws and regulations must specify this process and ensure that it is done in a timely manner.

Biometrics

Biometrics are not all the same and some old assumptions about biometrics, such as fingerprints being unique amongst all people, haven't been fully empirically tested. In 2005, Michael J. Saks and Jonathan J. Koehler published a paper in Science titled "The Coming Paradigm Shift in Forensic Identification Science", in which they begin to question the assumed accuracy of several different forensic identity techniques (http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.462.3185&rep=rep1&type=pdf).

In this paper, Saks and Koehler state:

> *"Simply put, we envision a paradigm shift in the traditional forensic identification sciences in which untested assumptions and semi-informed guesswork are replaced by a sound scientific foundation and justifiable protocols. Although obstacles exist both inside and outside forensic science, the time is ripe for the traditional forensic sciences to replace antiquated assumptions of uniqueness and perfection with a more defensible empirical and probabilistic foundation."*

Given this, let's take a deeper dive into three of the most common ways of identifying a person from another: fingerprints, iris recognition, and DNA.

Fingerprints 

There has been an assumption, since the late 1800',s that fingerprints are unique for each individual. However, during the last 20 years, this has been brought into question due to a lack of empirical data. In this presentation by Dr. Anil Jain of Michigan State University, the empirical accuracy of fingerprints is questioned:
http://biometrics.cse.msu.edu/Presentations/AnilJain_UniquenessOfFingerprints_NAS05.pdf

Fingerprints are also one of the ways to differentiate two genetic twins (On the similarity of identical twin fingerprints by Anil K. Jain, Salil Prabhakar, Sharath Pankanti:
https://pdfs.semanticscholar.org/e559/32e400516ddb00069864e60b3980250d1590.pdf

Additionally, it has been thought that fingerprints change from when a person is born and therefore are not reliable as a unique form of identity verification. However, in this 2014 paper, this assumption is now starting to be discredited: Recognizing Infants and Toddlers Using Fingerprints: Increasing the Vaccination Coverage by Anil K. Jain, Kai Cao and Sunpreet S. Arora (http://biometrics.cse.msu.edu/Publications/Fingerprint/JainCaoArora_RecognizingInfantsandToddlersusingFingerprints_IJCB14.pdf).

In summary, more empirical studies need to be done to confirm the accuracy of this technique across large populations as well as how samples are collected.

Iris Recognition

The potential use of the iris as a means of identification was first suggested in the 1940s. In the 1990s, the first algorithm was patented by John Daugman. Today, India uses iris recognition and fingerprints to identify more than 1 billion people.

Daugman published a paper in 2006 entitled "Probing the Uniqueness and Randomness of Iris Codes: Results From 200 Billion Iris Pair Comparisons" (http://www.cl.cam.ac.uk/~jgd1000/ProcIEEEnov2006Daugman.pdf), in which he stated:

> *"For example, in the U.K. with a national population of about 60 million, an "all-against-all" comparison of IrisCodes (totaling about 1015 pairings) as envisioned to detect any multiple identities when issuing the proposed biometric identity cards, could be performed using a decision threshold as high as 0.22 without expecting to make any accidental false matches. At this threshold, the false nonmatch rate, using today's better iris cameras (assuming good acquisition and cooperative subjects) would be below 1%. In everyday biometric transactions in which an identity is first asserted and then verified without exhaustive database search, matches with a very forgiving Hamming distance as high as about 0.32 could be accepted safely."*

Therefore, as a means of identity verification, the iris scan is viable across a large population. However, as a means of authentication, it is prone to masquerading; as shown in the following article, for example: Hacker Finds a Simple Way to Fool IRIS Biometric Security Systems (http://thehackernews.com/2015/03/iris-biometric-security-bypass.html).

Another drawback to using iris scans in citizen identification is that it doesn't work well with infants since they frequently close their eyes.

DNA 

In the 1980s, Sir Alec Jeffreys realized that DNA could be used to identify people (http://www.biochemsoctrans.org/content/ppbiost/15/3/309.full.pdf), and his work lead to the use of DNA in forensics. Since then, rapid advances in DNA technology has led to:

- Complete human genome sequencing (https://en.wikipedia.org/wiki/Human_Genome_Project)
- Many large databases using DNA to identify criminals (http://www.sciencedirect.com/science/article/pii/S0379073800004357)
- Using a subset of the DNA to identify people (DNA profiling) (https://en.wikipedia.org/wiki/DNA_profiling)
- Rapid DNA profiles (http://www.evidencemagazine.com/index.php?option=com_content&task=view&id=1115)

It is now possible to differentiate genetic twins using DNA in addition to fingerprints (see 2014's "Finding the needle in the haystack: Differentiating "identical" twins in paternity testing and forensics by ultra-deep next generation sequencing: http://www.sciencedirect.com/science/article/pii/S1872497313002275).

Here is a fact sheet containing current knowledge about cloning: https://www.genome.gov/25020028/cloning-fact-sheet/

The main issue with the use of DNA as a biometric identifier is the public's fear of how it can be misused.

Recommendations

In today's world, it is like the Wild West with respect to citizens' biometrics. Vendors come out with biometric identification and authentication techniques and then quickly market them. There are few reputable agencies validating equal error rates or testing the authentication devices to see if they can be easily fooled.

There is a lack of laws and regulations requiring citizen consent regarding the following:

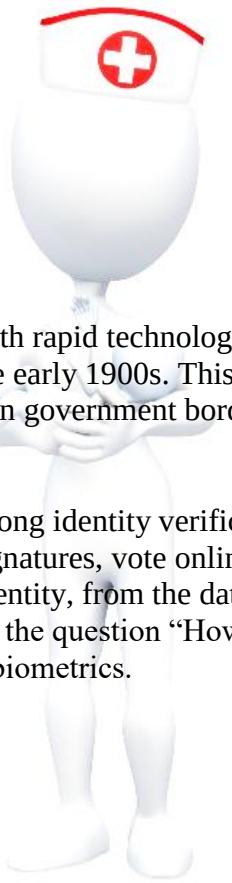
- Providing their biometrics
- How the biometrics will be used
- Mandating processes for a citizen to request removal and destroy of a biometric they provided

As a result, citizens are right to be leery of providing a piece of who they are, i.e. a biometric, to any government agency or third party.

Given all of the above, here are some recommendations regarding approach:

- Governments must develop new laws and regulations pertaining to the protection of a citizen's biometrics, using the principles listed in this paper
- The management of birth, name change, marriage, and death records should be centralized under one government agency/ministry responsible for identity verification
- All records should be securely stored in a network separate from other government networks to protect the privacy of the records/databases
- Birth records should be amended to include the following at birth of an infant:
    - DNA sample
    - Fingerprints
        - Longitudinal studies should be done to ensure that the new techniques for taking infant fingerprints are viable as the infant ages
- During the child's first year in school, an iris scan should be done and this record would be added to the identity verification database
    - There will be three biometrics to enable identity verification of a citizen
    - Obtaining the iris scan is now easy to do as opposed to when the citizen is an infant
- A national identity verification service should be created to only perform identity verification; the service will not use the biometrics for any other purpose.
- The government should create a national identity authentication service that a citizen can optionally join:
    - The citizen will provide biometrics to this service, with their consent, that can then be used to authenticate against.
    - The government will then federate this service with other government ministries and third parties.
    - The service should have the ability to provide anonymous authentication without releasing identity information.
    - The service can also provide recent addresses and other identity information with the citizen's consent to use it.

        - For example, if a citizen chooses to do so, they could update their new address or phone number once to the service and then have it pushed out to other ministries and/or third parties.
        - However, note that this is an optional service that a citizen can choose to subscribe to or not. Some citizens may choose to not use this service, which is their right.
        - Citizens must have the ability to leave this service if they so desire.
- Today, people move between different government jurisdictions all the time. Therefore, instead of one government establishing their own identity verification laws and regulations, it makes sense for different jurisdictions to coordinate their laws and regulations.
    - This is required when identity federation occurs between two or more different government jurisdictions for a citizen's identity
    - It also applies when federation occurs between different levels of government and the identity is attested to by the national identity verification service
    - Finally, it also applies to third parties who are federating with the national identity verification service
- Governments and/or trusted third parties need to assemble an on-going, independent, review of different identity verification and authentication techniques. They must report on equal error rates as well as the ability to fool different authentication devices. This provides citizens with context when they decide whether to use a given authentication technology or not as well as providing the industry with some benchmarks to measure against.



Summary

We live in an increasingly small world with rapid technological changes. Our existing identity verification systems were designed for the early 1900s. This was long before the rise of the internet with the fast, easy movement of people between government borders, electronic identity federation between enterprises and genetic cloning.

The use of high identity assurance, i.e. strong identity verification, is required to accomplish things like citizens easily being able to use digital signatures, vote online, conduct large financial transactions, etc. It requires a trusted government issued identity, from the date of birth onwards through an identity's life. We must re-design our systems to answer the question "How do I know if you are really you?" while protecting the citizen's privacy and their biometrics.

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."