"Rethinking Biometric Identification"

Executive Summary

There are two main challenges with today's use of biometrics:

- Biometrics are not revocable and re-issuable
- Mitigating the risk of storage of biometrics in enterprise systems being successfully hacked

Two potential solutions are offered, which require brighter minds than this author, Guy Huntington, in determining if the ideas are viable. If so, the commercial applications are huge, as are the potential of creating global standards to address problems of fraud for the end user and the enterprise.

Anonymous Biometric Identifiers

In 2015, I came across this draft paper by Rud Bolle out of the Netherlands, "Anonymous Biometric Identifiers – Revisited" (https://hvl.net/pdf/BolleAnonymousBiometricIdentifiersRevisited2015.pdf). It offered the following possibilities:

- Creating biometrics which can be given to a person which are not only digitized versions of it, BUT ALSO anonymized
- Allows for the possibility of biometrics being revoked and re-issued

As an old, very experienced identity architect, who isn't comfortable with today's wide spread use of biometrics, because of the limitations of them being maliciously obtained and then used in replay attacks, I was drawn to it. However, it's one thing of talk about it, and another of reproducing it, around the planet, through a wide variety of different biometric registration devices, and then confirming the biometric at say a retailer's till.

I've written about potentially leveraging this, on page 27 of this rethinking of human legal identity paper, "Secure, Network Based, Legal Self-Sovereign Identity (LSSI)" - https://hvl.net/pdf/SecureNetworkBasedLSSIPaperDec62020.pdf as well as in this deck for rethinking human identity via banks "Digital Banking & Legal Identities" - https://hvl.net/pdf/DigitalBankingIdentityDeckMar92021.pdf. However, all of this is fluff until we learn if it's operationally feasible around the planet.

Not Storing Actual Biometrics in an Enterprise Database

In this deck already referenced - https://hvl.net/pdf/DigitalBankingIdentityDeckMar92021.pdf, I propose the idea of not storing biometrics within an enterprise. Instead I'm proposing:

- Standardized biometric registration procedures
- Over time automate this to ensure best, standardized registration with high accuracy
- Adopt a biometric template which digitizes each type of biometric
- Then apply a standardized algorithm to anonymize them e.g. producing a value of say XYZ
- Discard the actual biometric, and only store the value, e.g. XYZ

Again, as mentioned above, all of this is fluff, until it can be proven to be operationally feasible around the planet.

Which is Why I Need Your Help

I'm an old, very experienced identity architect, program and project manager, who's led many complicated global identity projects. Down in the operational weeds, is where good ideas survive and dumb ones don't. So, my ideas above are just that…ideas. I need brighter brains than me to work with me, telling me what's possible and what's not. Assuming they are viable, then we can decide how to roll this out around the planet as either standards, commercial products or combinations of the above.

There's Also This Curve to Keep in Mind

A friend of mine, Pat Scannell, produced this curve (https://hvl.net/pdf/PatScannellHockeyStickShapedCurve.pdf) , which I absolutely love, as well as scaring the shit out of me! Why? It means rapid new innovation is going to keep on occurring. HOWEVER, it also means today's best legal identity framework (composed of governance, business processes, technology and end user) is being attacked, each new hour, with new attack vectors. This is something for which most enterprises don't have the resources to defend themselves against.

Applying this to biometrics and legal identification, it means they'll continuously come under attack. Which in turn requires creating a framework able to quickly respond. On page 6 of this paper, https://hvl.net/pdf/SecureNetworkBasedLSSIPaperDec62020.pdf, you'll see a global, non-profit, who's job it is to continually do threat analysis. In the deck, it also states Newco must be able to do this. Yes – it's a major challenge.