Huntington Ventures Ltd.

The Business of Identity Management

New Age Assurance – Rethinking Identity, Data, Consent & Credential

Author: Guy Huntington, President, Huntington Ventures Ltd.
Date: April 2019

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 year, I have written 22 papers. Here's a listing of them, by subject area, with links to each one:

- 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
- One-page summary
  - One Pager - The Age of AI, AR, VR, Robotics and Human Cloning
- New age identity, data and consent
  - Privacy Gone – AI, AR, VR, Robotics and Personal Data
  - Kids Privacy in Non-Private World - Why Even Super Hero's Won't Work
  - 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
- 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

.

Executive Summary

The paper begins with a description of what assurance is and why it's been developed for identity and credential risk.

It moves on to discuss rethinking assurance regarding the following areas:

- Identity
- Data
- Consent
- Credentials

For each one it illustrates how a new approach can be taken. The paper provides an example of zones of trust to illustrate a hypothetical data assurance model.

The paper ends with the statement:

Citizens, privacy groups, government and industry leaders, working towards new global legal frameworks, should also ensure a rethink is done for assurance. This is yet another stepping stone to creating an environment where citizens can act privately in a non-private world.

New Age Assurance – Rethinking Identity, Data, Consent & Credential

Introduction

We live in the age of an approaching technological tsunami composed of:

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

As the other 20 papers I've written show, it's not only rethinking of how we work, live and play BUT it's also creating what I call a "Non-Private' world. It requires new legal tools allowing us to choose to live privately in a non-private world.

The new legal framework involves completely rethinking identity, data and consent. Further, as the papers show, it also means each jurisdictions law's regarding these must be the same AND also be globally enforceable.

With the non-private world and new legal tools, it also allows for rethinking our ideas of assurance. Many people reading this paper won't know what it is.

Assurance is a measure of trust. Most governments around the planet have identity and credential assurance ratings. This is a measure of confidence, i.e. trust, an identity presenting themselves to the government with identity documents and/or a credential they're using, is who they claim to be.

The assurance usually uses different levels, which are numbered, with the low numbers indicating low trust and the higher ones, increasing trust. Therefore, an assurance level of 0 or 1 indicates low trust, while a 3, 4 or 5 indicates higher trust.

Why do governments use this? Over the last 100 years, different types of identity documents have been created, as well as different ways of authenticating, both in person and online. Let's use a birth certificate as an example.

When they were created in the 1800's, they were hard to reproduce. So, if Jane Doe was presenting it claiming to be her, there was a high chance it was Jane. Fast forward to the late 1900's. Technology had advanced with printing technology becoming high quality at a cheap price. Therefore, birth certificates were no longer a good proof it might be Jane Doe. i.e. Sally Smith might be masquerading as Jane.

The same also applies to credentials. The use of passwords as a means of proving it was Jane online became less likely as malware came into being.

This resulted in governments creating assurance standards for identity and credentials. Other industries adopted them and often refer to them in legal contracts between two or more partners.

Thus, Acme Inc. who's entering into a contract with Business Inc., where Acme Inc's employees will be contracting to Business Inc. with a high degree of risk involved, might sign a contract stating that identity assurance level 3 of Jurisdictions' A identity assurance, is required to proof Acme Inc's employees. If there is a problem later on with one of Acme Inc.'s employees, and Business Inc. finds out they weren't who they claimed to be, Business Inc. could take Acme Inc. to court stating Acme Inc. didn't do a proper job of identity proofing the employee.

Today, most identity assurance schemes use biometrics for higher levels of identity assurance with birth certificates being a low level. There's an unsaid assumption that higher levels of identity assurance are mostly required when a person becomes an adult.

As the paper "Kids Privacy in a Non-Private World – Where Even Superhero's Won't Work" and "Why the New Age Requires Rethinking Civil Registration Systems" illustrate, these assumptions are no longer valid.

Further, as the papers "I Know Who You Are & What You're Feeling – Achieving Privacy in a Non-Private World", "Privacy Gone – AI, AR, VR Robotics and Personal Data" and "Consent Principles in the New Age – Including Sex" illustrate, our old ideas of data and consent need to change. This also applies to ideas of assurance. That's what this paper will explore.

Rethinking Identity Assurance

As the paper "Why the New Age Requires Rethinking Civil Registration Systems" shows, a person will have a biometric taken at birth to be used in the birth registry. Thus, right from birth, a person has a high degree of identity assurance.

Further, the paper also shows how during the first year of school, the person would supply their iris scan. Thus, the person would have two biometrics, with a low equal error rate, i.e. high degree of biometric accuracy, which can be used, in a court of law, to say Jane Doe is really Jane Doe and not Jane Doe Clone 1, 2 or 3 [Note: The papers suggest research be done to confirm the use of a baby's fingerprints are valid and also that fingerprints and iris are enough to differentiate human clones].

The papers also suggest, at birth, the new age civil registration service will grant the person with two digital identifiers:

- A full legal identification
- Anonymous identification indicating they are a human and are either underage or of age of majority
-

I've suggested in the papers that Sovrin/Blockchain be used for this. It puts control of the person's identity into their own hands. However, there are problems with this technology.

It relies upon a secret key. As the cryptocurrency market has already shown, it's not hard for malicious people to obtain the secret key, via malware, phishing attacks, etc. Thus, the papers discuss it only being used for low to medium risk scenarios.

The papers also discuss, when a person comes of legal age, granting them the ability to digitally sign documents legally. This is what Estonia and other countries have been doing for a number of years.

At the same time a person comes of legal age, the papers also suggest taking a digital photo of Jane, which the new age civil registration service signs. Jane can use this to prove she's of legal age without having to release her identity. For example, she can enter a bar using this technology.

The papers also discuss that biometrics are not all "golden". Even if a biometric, like a fingerprint or iris, with a high degree of accuracy is used, it might not be the person they are claiming to be. Why not? Biometric readers can be spoofed. Thus, Alice might be successful as masquerading as Jane. Therefore, the papers call out for secure, controlled conditions, with approved biometric readers, to obtain and confirm a person's legal identity.

Summing all of the above up, it means we can rethink identity assurance. Hypothetically, low levels of trust can use the digital identity provided by the identity. Medium levels of trust can use Jane's digital id, plus Jane's digitally signed picture plus Jane's digital signature. High levels of trust can use Jane's biometrics, obtained in controlled, secure conditions.

The papers also note the requirement to have delegate ability to manage your digital identity and/or do so on behalf of others, e.g. kids and people requiring power of attorney. The identity assurance framework should apply to these groups too.

Before leaving identity assurance, I want to note the new age comes with LOTS of new behavioral data illustrated in the two papers "I Know Who You Are & What You're Feeling – Achieving Privacy in a Non-Private World" and "Privacy Gone – AI, AR, VR Robotics and Personal Data". As this technology advances, with accompanying research, it seems highly likely behavioral data will enter into new age identity assurance frameworks.

The new legal identity toolkit offers new ways of rethinking identity assurance.

Rethinking Data Assurance

The papers "I Know Who You Are & What You're Feeling – Achieving Privacy in a Non-Private World" and "Privacy Gone – AI, AR, VR Robotics and Personal Data" discuss the gigabits/second each person will be either generating and/or receiving. Much of this data is highly sensitive, i.e.it contains behavioral/biometric data.

Our old ideas about data privacy are effectively made useless by the new technology. Therefore, the papers call out for new data laws, where the citizen owns and controls data about them. This puts in the citizen's hands, control of data based on trust.

The papers suggest "zones of trust" be used. It uses the following hypothetical example to illustrate this:

Jane Doe is walking down the street with her friends Erika, Neil and John, with each one applying zones of trust. Here are hypothetical zones of trust each of them selects:

- Jane – no trust, wants to act anonymously
- Erika - some trust – wants to release identity but not provide consent for data to be used
- Neil - allows both identity and data to be used, automatically providing his consent to pre-approved groups (people groups, industry segments, etc.)
- John - high trust – gives permission for identity and data to be used by anyone

Here's what could happen:

- Jane is able to walk down the street without others being able to tell who she is and what her feelings are. She's being private in a non-private world.
- Erika is letting others know it's her but nothing more. Other people and/or entities like retailers would have to ask her consent to process her data
- Neil lets others know who he is and automatically providing his consent for his data to be used to pre-approved people and/or groups
- John's identity and data are free to use by anyone

Citizens, as well as government and industry, will want to standardize the zones of trust, i.e. data assurance levels. They'll want a clear understanding of the various levels. This is not a bad idea at a high granularity level. What do I mean by "granularity"?

Data, and peoples' perceptions of it, vary according to personal, community, culture, regional, state and national levels. Thus, while a region might have values about data, a local community might choose to place different values they want imposed. The same applies to each individual. Let's use Jane Doe as an example…

She has selected an anonymous level of data assurance. She walks into Acme Store Inc. and decides to release both her identity and data for 1 minute to Acme Store Inc., allowing them to use their AI personalized shopping programs to offer her a custom price on a unique dress. At the end of the minute, Jane expects Acme Store Inc. to not keep the data. This is fine grained data control.

For business to function smoothly, they'll want to have a level global playing field, where high granular levels of data assurance are defined. Then, as regions, communities and people deem it necessary, they will be able to customize the data assurance within the level themselves.

To accomplish this requires new age legal tools of both identity and data which work in real time. For example, as Jane is walking down the street, people walking towards her, with AR glasses/lenses and biosensors in their clothes, will not be able to process data about Jane, since she's chosen a data assurance level of no-trust.

Careful legal and technical thought will need to be given addressing how this data, viewed a year later, will achieve the same goals.

The papers also note the requirement to have delegate ability to manage your data and/or do so on behalf of others, e.g. kids and people requiring power of attorney. The data assurance framework should apply to these groups too.

Rethinking Consent Assurance

The paper "Consent Principles in the New Age – Including Sex", illustrates different incoming tsunami waves of consent:

- First wave is caused by the Internet of Things (IoT)
- Second wave is caused by sexual consent
- Third wave is caused by AI, AR, VR and robotics

In the not so distant future, we will have hundreds or thousands of consents to grant and/or change, each year. That's why the paper recommends new consent management laws requiring the ability for each citizen to centrally manage their consents, if they so choose to.

It then shows how different consents have different trust levels. For example, granting consent for your fridge to communicate if the milk's going off or running low to a retailer, is different than granting consent for your biosensor clothing to transmit health information to your doctor. One is relatively low risk, while the other is high risk. Each level of risk requires different identity, credential and data assurance.

Consent assurance levels can range from complete trust, i.e. no informed consent, through to a well-informed consent. The identity and credential assurance levels for this will vary accordingly.

Similar to data assurance, citizens, as well as government and industry, will want to standardize the zones of trust, i.e. credential assurance levels. They'll want a clear understanding of the various levels.

Thus, similar to data assurance, there is a need to establish high granularity consent assurance levels, with the citizen's ability to finely tune them. Since real life is complex, with all sorts of different risk scenarios, the consent assurance architecture must be flexible. Here's an example:

Jane's parents are dropping her off at a local child care centre for an hour. They grant the child centre ability to manage her data for an hour. For this level of trust/assurance, they will use their digital ID to verify themselves to the centre, with application of a password credential to authenticate them to their centrally managed consent management service. For this level of trust, the child care centre worker or workers, then supply their digital ids as part of the consent assurance level.

However, Jane has a unique medical condition possibly requiring medical attention while she is at the child care centre. Therefore, her parent's want to authorize the childcare centre to have a one-hour access to Jane's medical data, if required. To create this consent, her parents have to provide stronger authentication, e.g. a behavioral/biometric credential, since it's Jane's medical data to grant the consent.

The papers also note the requirement to have delegate ability to manage your consent and/or do so on behalf of others, e.g. kids and people requiring power of attorney. The consent assurance framework should apply to these groups too.

Rethinking Credential Assurance

For the last several years, I have been thinking the credential marketplace is like the old wild west. Vendors appear with a new credential, touting its secure ability to authenticate an identity. There is little independent testing done to validate the claims, i.e. there's no marshal in town to vet things. Then there's the pace of change.

At this year's Davos meeting, Justin Trudeau said, "Think about it: The pace of change has never been this fast, yet it will never be this slow again." This results in today's best credential quickly becoming tomorrow's turd. People get burnt by using technology they think is safe.

The incoming technological tsunami is bringing with it behavioral and biometric data, not easily used in the past. The papers "I Know Who You Are & What You're Feeling – Achieving Privacy in a Non-Private World" and "Privacy Gone – AI, AR, VR Robotics and Personal Data" discuss this.

Without using much of one's imagination, one can see how this new technology will be used to authenticate people. As it explodes into the marketplace, so will the claims.

Given the above here's what's required to develop new, global, credential assurance standards:

- Independent, globally recognized test services to test behavioral/biometric methods including the readers
    - Thus, vendors will no longer be able to make claims which haven't been independently tested
- Standardized credential assurance levels
- Flexibility within the assurance levels, allowing for different methods to be used, where technically warranted
- Governments agreeing to jointly take independent testing results and implement changes to the credential standards, within pre-agreed amounts of time
    - Thus, as the pace of change increases, especially for medium to high risk situations, credentials now becoming a turd will be relatively rapidly changed

There is also the requirement to have the ability to authenticate on behalf of others, e.g. kids and people requiring power of attorney. The credential assurance framework should apply to these groups too.

Summary

To combat the incoming technological tsunami striking our planetary shores requires a new legal framework for identity, data and consent. These new legal tools also create new ways of thinking about assurance. The paper shows how assurance can be rethought for identity, data, consent and credentials.

Citizens, privacy groups, government and industry leaders, working towards new global legal frameworks, should also ensure a rethink is done for assurance. This is yet another stepping stone to creating an environment where citizens can act privately 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. 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 can be reached at:

guy@hvl.net
www.hvl.net
https://ca.linkedin.com/in/ghuntington

1-780-289-2776