

## Legal Privacy Framework for the Tsunami Age



Copyright: 123RF

**Author:** Guy Huntington, President, Huntington Ventures Ltd.  
**Date:** Created June 2019/Updated Feb 2020

## Table of Contents

<b>LEGAL PRIVACY FRAMEWORK FOR THE TSUNAMI AGE</b>	<b>1</b>
Table of Contents	2
Technological Tsunami Age Papers:	4
Notes About This Paper:	6
Why I Wrote This Paper	6
What Is This Paper?	6
The Goal of This Paper	6
Analogies Used in This Paper	6
Who's the Paper Aimed At	6
Executive Summary:	7
<b>LEGAL PRIVACY FRAMEWORK FOR THE TSUNAMI AGE</b>	<b>8</b>
Identity	8
Our Old Identity Legal Identification No Longer Works	8
Rethinking Civil Registration Systems Globally	9
Legal Physical Identity	9
Where Shit Happens	9
The Pace of Change Might Require Rethinking the Biometrics Used to Verify the Identity	10
Legal Digital Identity	10
Ability to Act Anonymously/Show They are Human	11
Control Over Their Identity	11
Legal Robotic Identity	12
Robotic Identification Identifying Them as a Robot	13
New Age Civil Registration Service Summary	13
Global Standards for Identity Assurance	14
Today, Many Existing Identity Assurance Standards Exist	14
New, Global Identity Assurance Standards	14
We Must Own & Control Our Data	15
New Age Data Premises	15
Women & Children Data Privacy	16
Large Multinational Vendors and Some Nation States Will Aggressively Push Back	16
Argument - The Data Horse is Out of the Barn	17
Today Isn't Going to be Like Tomorrow	18
Assuming the Creation of New Data Laws - What's Next?	18
Consent in the Tsunami Age	19
Our Existing Consent Legal Models Don't Work Well Regarding Privacy	19
New Age Consent Principles	20
Jane Doe Story	20
Hypothetical Zones of Trust	21
No Trust - Wants to Act Anonymously	21

Huntington Ventures Ltd.  
The Business of Identity Management

Some Trust – Wants to Release Identity but Not Provide Consent for Data to Be Used	21
Medium Trust – Allows Both Identity and Data to Be Used, Automatically Providing Her Consent	22
High Trust – Gives Permission for the Use of Her Identity and Data by Anyone	22
Let's Assume We Have A New Legal Consent Model – What's Next?	22
<b>Personal Identity &amp; Access Management (IAM) System</b>	<b>23</b>
IAM Premise	23
People Without Access to Technology	24
Legal Considerations About Personal IAM	24
Managing the Identity	24
Authentication Management	25
Consent Management	25
Federating the Identity and Data	25
Technical Considerations	26
Follow the Electrons	26
Endpoint	26
Transport Layer Security	27
Digital Certificates	27
DMZ Areas	27
Secure Transmission of the Data Internally	27
Legal Considerations Addressing Numerous Potential Attack Vectors	28
Personal IAM Applies to Robots as Well	29
Autonomous Robot Walks Down Street	29
Three Robots Acting in Singularity	29
<b>Summary</b>	<b>30</b>
<b>About the Author</b>	<b>31</b>

## Technological Tsunami Age Papers:

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 31 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:

- 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](#)

Huntington Ventures Ltd.  
The Business of Identity Management

- 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>.

## Notes About This Paper:

### Why I Wrote This Paper

Initially, I was wanting to expand my thoughts on a personal identity & access management (IAM) system, expressed in the paper "[Technological Tsunami & Future of IAM](#)." However, I realized most people wouldn't understand the underlying components required to enable a personal IAM system. So, in this paper, I first summarize the legal privacy components from the [other 24 papers I've written](#), and then discuss personal IAM systems.

### What Is This Paper?

It's a thought paper about a new legal privacy framework. Much of what I discuss in this paper doesn't exist yet. Therefore, I am shining the proverbial light on what's coming at us regarding privacy and, in this paper, outlining my thoughts on requirements.

As with any new type of thought, it must be debated and refined. I expect others to contemplate the ideas in this paper. Perhaps they'll improve the ideas or, come up with better ones.

### The Goal of This Paper

My underlying premise is we are rapidly entering an age of what I call a "non-private world." To create privacy in these unprecedented times requires people to get out of their old ways of thinking about privacy. Therefore, the goal of this paper is to make people think long and hard about what's required to live privately in a non-private world.

### Analogies Used in This Paper

The introduction section of this paper discusses the fact that unprecedented times not only requires a new legal privacy framework BUT, one that can be relatively rapidly changed. Thus, I use two different analogies in this paper. A layered cake, with components that can be relatively easily changed and, building foundations, which are solid and supportive, but can't be easily changed.

### Who's the Paper Aimed At

- Privacy experts including lawyers and privacy groups
- Boards and C-suites wanting to see what's coming regarding privacy laws
- Government leaders and administrators trying to keep up with fast moving changes regarding citizen privacy
- Enterprise architects wanting to see how system architecture will change in the coming years
- Companies making behavioral/biometric predicting systems
- Enterprises consuming consumer data
- Anyone interested in their privacy in a non-private world

## Executive Summary:

[I've written 24 papers](#) documenting how the incoming technological tsunami is rapidly creating what I call a “non-private world.” To allow us to live privately in a non-private world, requires a complete rethink of laws about identity, identity assurance, data, consent, and personal identity & access management devices. This thought paper summarizes them.

It begins by describing a rethought new age civil registration service. Biometrics will be collected at birth, from both baby and parents. A legal digital registration is then issued to the parents/legal guardians, which they can use to prove the baby's legal identity as well as being able to delegate it. It also discusses how robots need legal identities too.

The paper then describes creating a global identity assurance framework. It notes how new behavioral/biometric developments, from the steep hockey stick shaped curve of technology change, requires a flexible assurance framework. However, it also indicates how we mustn't knee-jerk to this, suggesting a global standards/research body be created to evaluate identity technology carefully.

It then moves on to data, stating 8 premises, including “Premise 1: Citizen owns their own data” and “Premise 2: Citizens should control their own data”. It's a foundational component of the new age privacy framework.

A challenge in the new age is the technology can be used on us, without our consent, not only to identify us but also to predict our behavior. Thus, a complete rethink of consent is required. The paper states new age consent principles including, “Different Risks Require Different Forms of Consent,” “Consent Zones of Trust” and, “Centrally See/Manage All Consents Given”. A hypothetical example of zones of trust is provided.

With all of the above components in place, the paper then moves on to discuss the need for a personal identity & access management framework, applicable to both humans and robots. It describes how each of us will be federating our identity and data via these devices. The paper discusses how legal automation software is required to manage consents and federation contracts. Importantly, it also outlines how people without technology will also be protected.

The paper then ends with an image of a person holding an umbrella for protecting watching a colossal tsunami wave approaching. That's us, in an unprecedented age, using our old legal privacy systems, which isn't going to work in the new age.

**The unprecedented age we live in requires global thinking, global laws, global enforcement, and when technology outdates them, an ability to rapidly change laws and regulations. It's our choice. Our privacy can be swept aside by the incoming waters or, we can work collaboratively together, creating new laws allowing us to live privately in a non-private world.**

## Legal Privacy Framework for the Tsunami Age

### Identity

#### Our Old Identity Legal Identification No Longer Works

The existing foundational document for a person's identity, e.g., their birth certificate, is now badly outdated. It uses technology from the 1800s, i.e., paper. Today, it's easily frauded. So much so, in security circles, it's called a "[breeder document](#)." With this, one can obtain all the other identity documents higher up the food chain, including driver's license, passport, etc.

Then there's human cloning. Science/ business has come a long way from Dolly the sheep, the first mammal cloned in 1996. Fast forward to today in China, [where Boyalife currently clones 100,000 cows a year working towards 1 million](#). In 2015, [their CEO publicly stated they could clone humans but weren't](#). In 2017, the [Economist published a spoof article imagining how the world would learn of the first human clone](#). Thus, the age of human cloning is now almost upon us.

In 2006, I published my first paper, "[The Challenges with Identity Verification](#)," in which I suggested birth registration use DNA to enable differentiation of clones. I took criticism from others who didn't like the idea of governments using a biometric able to profile people, e.g., DNA. After reflection, I agreed

Given all of this, what's a new foundational legal identity solution for an identity?



## Rethinking Civil Registration Systems Globally

The bedrock of the legal system is having an identity provable in a court of law. The science used to prove the identity is who they claim to be, must be reproducible and not easily masqueraded.

### Legal Physical Identity

In the paper “[Why The New Age Requires Rethinking Civil Registration Systems.](#)” I lay out the requirements for a new age physical identity. In summary, it requires:

- Researching to confirm:
  - The work of [Dr. Anil Jain](#), of Michigan State University, regarding the use of baby fingerprints
  - If fingerprints and iris biometrics are sufficient to differentiate human clones
- Assuming the research confirms this, then:
  - At birth, a child’s fingerprints would be obtained to register the identity
    - If the child doesn’t have fingers, then another biometric will be used
    - The child's parents' biometrics will also be collected, confirming their identities, and then their identity registration linked to the baby's registration
  - During the first year of school, a child’s iris scan would be collected and then used as the second biometric for legally identifying the child
    - If the child doesn’t have eyes, then another biometric will be used

Thus, biometrics are used to confirm the child or adult person's identity. However, as the paper states, biometrics are not all golden.

It's possible to hypothetically spoof a biometric reader and/or, intercept the data en route from the reader to the central civil registration data store. Thus, for high-risk identity assurance, controlled conditions, as stated by the new age civil registration service, must be used to obtain and verify the identity.

### Where Shit Happens

As the paper “[Where Shit Happens](#)” [Deploying AI, AR, VR, Robotics, Identity, Data & Consent in Challenging Parts of the Planet](#)” lays out, 49% of the planet's population doesn't have internet access, many don't have smartphones, and 1 billion people don't have a legal identity. These are places where, to put it bluntly, "shit happens." How is this new way of doing things going to work for these people?

One of the challenges I discuss in that paper is the use of biometrics as part of the birth registration process will drive up the cost for fake identities. In places where shit happens, the use of force, etc. will be used to get registrations done using other fingerprints. Further, bribery of civil registration service administrators can also occur. Thus, the paper discusses ways to mitigate these risks.

Hypothetically, let's assume the new age civil registration process works for birth registration. Jane Doe, the newborn, is registered. Granting of the legal digital identity occurs.

### ***The Pace of Change Might Require Rethinking the Biometrics Used to Verify the Identity***

In the paper "[Children & Parent Privacy in the Tsunami Age](#)," I outline the work of technology visionary [Pat Scannell](#). He states we are in an age with a hockey stick shaped curve of technology change, i.e., logarithmic. I concur. Given this, as time passes, it's highly likely either new biometrics and/or behavioral measurements will prove to be more useful than existing ones, demonstrating in a court of law, the identity is whom they claim to be.

It's an excellent example of both analogies referred to in the note to the reader section of this paper. The underlying biometrics must be scientifically proven to identify the person out of all other people on the planet and human clones. Thus, it's the foundational bedrock for identity. However, it's also like a layer cake. As new ways of measurement come into being, it might mean the foundational layer of the cake might need to be relatively quickly re-baked.

### ***Legal Digital Identity***

At the same time, during the creation of the baby's legal, physical identity, the new age civil registration service should grant the parent/legal guardian control of the newborn's digital identity. As the papers "[Why The New Age Requires Rethinking Civil Registration Systems](#)" and, "[Policy Principles for AI, AR, VR, Robotics & Cloning - A Thought Paper](#)" discuss, I suggest using Sovrin/Blockchain as the tool to use.

However, it too is not all golden. Why? Secret keys and the ability to delegate the identity.

Sovrin/Blockchain requires the identity to possess a secret key. The history of blockchain for cryptocurrencies highlights how it's not that hard for malicious people to obtain the secret key. Assuming this challenge remains (there are currently products emerging using biometrics to protect the secret key), the papers state the use of digital identity should work only for low to medium risk transactions.

Another need is for parents/legal guardians having the ability to delegate the child's identity to others. The Policy Principles paper illustrates this with grandparents, hospital, and school examples. Its likely changes will be required to Sovrin/Blockchain to make this work.

The digital legal identity might have to be changed if secret keys are lost, fraudulently obtained, etc. New legal, business and technical processes need to be invented, negating the use of the old legal digital identity and, replacing it with a new functional one. Thus, using the layered cake analogy, the new age civil registration service needs to have the ability to make changes to the digital identity portion of the cake layer.

Huntington Ventures Ltd.  
The Business of Identity Management

Regardless of the technology solution decided upon, at birth, the civil registration service grants the child's parents/legal guardians the child's digital identity. It can then be used by them, to prove the child's identity for services.

***Ability to Act Anonymously/Show They are Human***

The papers, “[Why The New Age Requires Rethinking Civil Registration Systems](#)” and, “[Policy Principles for AI, AR, VR, Robotics & Cloning - A Thought Paper](#)” discuss having the ability for a person to act anonymously and also show they are human legally.

Thus, at birth, the parents/legal guardians would be given:

- Digital attestation the child is underage and a human
- It could be via Sovrin/Blockchain or, some other method

***Control Over Their Identity***

The papers referenced above have a fundamental principle regarding the importance of a person being in legal control of their physical and digital identities. However, there are times when a person isn't in control of their legal identities. It includes:

- Legal minors
- People requiring others with Power of Attorney to legally act on their behalf
- Exceptions including arrest

I have another fundamental principle that a person can act and live anonymously if they so choose to.

Then there's robotic identities to consider.

### ***Legal Robotic Identity***

Robotics, both virtual and physical, are here now. The paper, "[I'm Not a Robot](#)" provides a high-level overview. As the planet begins to create thousands, millions and, in the future, billions of them, they too need legal identities.

I wrote a paper "[Legally Identifying Robots \(Robot Identification\)](#)," suggesting the use of a new age civil registration system. Then, after receiving a question about how we'd rapidly scale robotic registration at "insane speeds," I wrote, "[Rapidly Scaling Robot Identification?](#)"

The two papers propose the following:

- New age civil registration service be used to register identities
- Within each robotic code, creation of a "Robotic Identification Unit" (RIU)
- It must be secure and contain the robot's identification
- Submission of the robot's identity to the new age civil registration service
- The service would then, instantly, check with all other civil registration services globally to see if the robot's identity already exists
- Assuming it doesn't, the local civil registration service would then construct a legal identity for the robot
- Insertion of the new age civil registration service's identity into the robots RIU
- I suggest that something like Blockchain is used to publish the robot's identity
- Most of this process would be highly automated

In the papers, I discuss robotic termination. It isn't as straightforward as it might seem at first glance. Why?

Robots will likely outlive their owners. Replacement of physical parts means a robots lifespan it could be a very long time. Virtual robots can exist almost forever, assuming that computing space and the electrical grid is available.

I created yet another thought paper addressing this, "[Legal Person: Humans, Clones, Virtual and Physical AI Robotics – New Identity Principles](#)." In it, I propose some new age privacy principles relating to robots. Towards the end, I also talk about robotic singularity.

If you're old enough to recall the TV/Movie series "Star Trek," it had a race of computing beings called the "[Borg](#)". These were able to act together, in singularity. Today, we are in the early days of possibly producing singularity in robots.

There are no common agreed-upon standards for identifying robots, nor for robots acting in singularity. Given all of the above, laws need to be created, leveraging agreed upon science, to identify robots, both virtual and physical.

Huntington Ventures Ltd.  
The Business of Identity Management

[Robotic Identification Identifying Them as a Robot](#)

The papers referenced above, briefly discuss how robots also likely need anonymous identification indicating they are robots. The paper, “[Virtual Sex – Identity, Data & Consent](#)” provides an example of this. If Jane Doe’s in a virtual sex environment, she should be able to see who’s an AI generated robot and who are acting on behalf of a real person.

**[New Age Civil Registration Service Summary](#)**

All of the aforementioned likely needs to be incorporated into a new age civil registration service, globally. The service needs to adhere to similar laws in each jurisdiction with localized management.

Let’s hypothetically assume:

- Each person has:
  - A legal, physical identity, proofed via biometrics
  - Digital identity containing their legal birth registration information
  - Digital anonymous identity proving they are human
- Each robot has:
  - A legal identity
  - Digital anonymous identity proving they are a robot
- New age civil registration laws, business, and technical processes, the same globally, administered locally

What’s the next layer? Global identity assurance standards.

## Global Standards for Identity Assurance

### Today, Many Existing Identity Assurance Standards Exist

There are currently many different identity assurance standards, governments, and businesses use to verify identity. These range from low to high levels of trust. Given the ease with which a person can digitally move around the planet AND, the pace of technology change concerning behavior biometrics, it requires a shared global identity assurance framework.

### New, Global Identity Assurance Standards

In the paper “[New Age Assurance – Rethinking Identity, Data, Consent & Credential](#).” I discuss hypothetical different levels of trust for identity assurance. I discuss different hypothetical levels of trust for identity assurance. Perhaps more importantly, at the end of the discussion, I state:

“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.”

The legal framework for identity assurance must be reasonably flexible, allowing for new technologies to be inserted. There's a caution here.

Countries must not knee-jerk to new technologies. Instead, careful research must be done to ascertain the viability of new technologies. It must include things like replay attacks, etc.

Rather than have each nation-state researching the technology, I suggest assigning this to a global research/standards enterprise with the task of providing accurate benchmarks for any new behavioral/biometric technology used for identification. It must be independent of vendor claims.

In summary to date; we have established:

- Foundational layers of a legal physical and digital identity for both humans and robots
- Created global identity assurance standards

What’s the next layer? Data.

## We Must Own & Control Our Data

Shoshana Zuboff, in her book, "[The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power](#)," discusses "behavioral surplus":

"Surveillance capitalism," she writes, "unilaterally claims human experience as free raw material for translation into behavioural data. Although some of these data are applied to service improvement, the rest are declared as a proprietary *behavioural surplus*, fed into advanced manufacturing processes known as 'machine intelligence', and fabricated into *prediction products* that anticipate what you will do now, soon, and later. Finally, these prediction products are traded in a new kind of marketplace that I call *behavioural futures markets*. Surveillance capitalists have grown immensely wealthy from these trading operations, for many companies are willing to lay bets on our future behaviour."

## New Age Data Premises

One of the underlying premises in the papers I've written is we should own and control data about us. It must not be free, without our permission, for other enterprises or people to use, modeling us, and predicting our behavior.

In the paper "[Privacy Gone – AI, AR, VR, Robotics and Personal Data](#)," the executive summary states the following:

- Premise 1: Citizen owns their own data
- Premise 2: Citizens should control their own data
- Premise 3: Data consent must be informed
- Premise 4: Data consent should be centrally managed by the citizen
- Premise 5: Data consent process should be automated into zones of trust
- Premise 6: Data for legal minors and people requiring power of attorney MUST be carefully regulated by law
- Premise 7: Exceptions to the above premises MUST be carefully, legally regulated
- Premise 8: Global data laws/regulations required with global enforcement

Readers wanting more information about each premise should read the paper.

Huntington Ventures Ltd.  
The Business of Identity Management

### **Women & Children Data Privacy**

The tsunami age is rapidly eroding privacy for women and children. The paper, “[Children & Parent Privacy in the Tsunami Age](#)” references a Cracked Labs story from 2017 “[Corporate Surveillance in Everyday Life](#)” stating, “It depicts Acxiom and Oracle’s databases from 700 million to 2 billion people ranging from 3,000 to 30,000 attributes!” The Corporate Surveillance story also discusses how Facebook has over 50,000 attributes for its members.

The paper then illustrates the effects of the incoming tsunami wave on top of this. It starts with a woman ovulating and then proceeds through pregnancy, birth, toddlers/preschool, school, children's health, and adolescence. The paper provides many examples.

Thus, as the “[Privacy Gone](#)” paper states, “Premise 6: Data for legal minors and people requiring power of attorney MUST be carefully regulated by law.”

### **Large Multinational Vendors and Some Nation States Will Aggressively Push Back**

The threat of new global laws assigning ownership and control of a person's data about themselves to them will affect existing business models of large companies like Google, Facebook, Amazon, Alibaba, etc. Their assumption of either freely obtaining this data or, quickly acquiring consent to use the data, will now no longer be so easily done. Countries, like China, using behavioral/biometrics to do social control of their citizens, also will be threatened by these new laws.

As a result, there will be LOTS of pushback on any effort to discuss and implement these laws. The companies and governments opposed to this, have enormous fiscal and political resources to bring to bear, fighting and/or watering down new data laws in each jurisdiction.

Thus, the way to overcome this opposition is to mount a global effort to unify and change data laws. As long as the energies are limited to nation states, they will likely fail.



**Argument - The Data Horse is Out of the Barn**

One of the arguments against new data laws will be the data is already gone into many different databases, and it can't be undone. It's using the horse is already out of the barn argument. However, there is a legal precedent against this argument.

Shoshana Zuboff, in her book, "[The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power](#)," discusses the right to be forgotten.

“Google’s mission to “organize the world’s information and make it universally accessible and useful”—starting with the web—changed all of our lives. There have been enormous benefits, to be sure. But for individuals it has meant that information that would normally age and be forgotten now remains forever young, highlighted in the foreground of each person’s digital identity. The Spanish Data Protection Agency recognized that not all information is worthy of immortality. Some information should be forgotten because that is only human. Unsurprisingly, Google challenged the agency’s order before the Spanish High Court, which selected one of the ninety cases, that of attorney Mario Costeja Gonzalez, for referral to the Court of Justice of the European Union. There, after lengthy and dramatic deliberations, the Court of Justice announced its decision to assert the right to be forgotten as a fundamental principle of EU law in May of 2014.”

Thus, despite claims to the contrary, technology and technology companies, can be brought to bear to comply with new data laws.

## Today Isn't Going to be Like Tomorrow

At the end of "[Children & Parent Privacy in the Tsunami Age](#)," it states the following:

"When I discuss the need for new global laws, many roll their eyes thinking "Guy, what are you smoking? Don't you realize how the real world works? There's no way it can happen today!" They are right. However, today is different than tomorrow.

There are three reasons I'm confident the global moment for doing this is fast approaching:

- Hockey stick shaped pace of change curve
  - Globally speaking, it means tomorrow is definitely not going to be like today
  - The technology change will exacerbate business, social, cognitive and political change, showing us our old nation-state ways no longer work
- Global warming
  - These recent articles about [melting ice in Greenland](#) and [arctic permafrost](#) show our planet's climate is rapidly changing
  - It requires a coordinated global response, with laws enforcing it, in effect driving the planet together
- Job automation
  - The rise of AI and robotics means, over the next years, increasing amounts of people will lose their jobs with none to replace it
  - As the numbers increase, it too will create a global need to change the way we live, work and play

**What could be more important than protecting our children and the environment? It's time to recognize we live in an unprecedented age, where children and parents' privacy is gone. We can't outrun the incoming tsunami wave. It's time for global action."**

## Assuming the Creation of New Data Laws - What's Next?

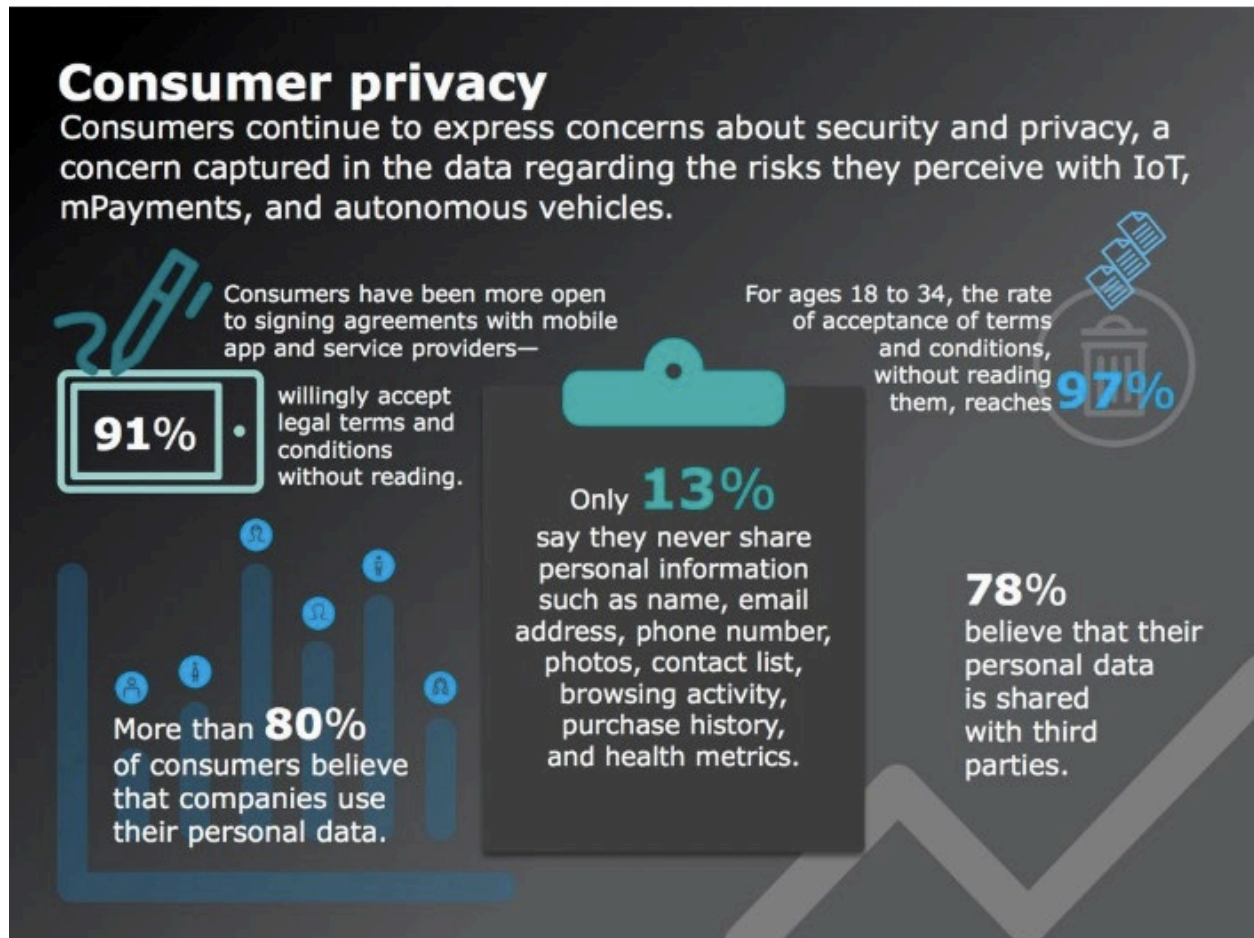
Let's hypothetically assume that we now have new, global laws allowing each citizen owning and controlling their data. What's the next layer? Consent.

## Consent in the Tsunami Age

### Our Existing Consent Legal Models Don't Work Well Regarding Privacy

Our existing laws and processes regarding consent aren't working from a privacy perspective. In the paper "[Children & Parent Privacy in the Tsunami Age](#)," I quote two examples:

- One is [this Guardian video on femtech and women's periods](#), where two women didn't realize where their period data was going
- The other is this excellent Deloitte image, from the Business Insider story, "[You're not alone, no one reads terms of service agreements](#)."



Deloitte

Throughout the "[Children & Parent Privacy in the Tsunami Age](#)" paper, I document how the already extensive data on billions of people, residing in commercial databases, will grow more personal. The advent of behavioral/biometrics will result in companies, governments, and other people able to model and predict our behavior. It's unprecedented in our times.

## New Age Consent Principles

In the paper, "[Consent Principles in the Tsunami Age](#)," it states new age consent principles:

- Different Risks Require Different Forms of Consent
- Consent Zones of Trust
- Centrally See/Manage All Consents Given
- Change Consents Where Allowable by Law
- Consent Management
- Consent Transfer Policies
- Managing Minor Consents
- Managing Power of Attorney Consents
- Robotic Consent
- Chain of Identity/Data Custody Via Consents
- All Consents Shall be Governed by a Central Consent Law/Regulation
- Consent Laws Need to be the Same Globally

Rather than detailing them, readers wanting to understand each principle should read the paper. However, I will reproduce here the hypothetical zones of trust. Why?

Obtaining people's behavior/biometric data, without their consent, is easily done in the technological tsunami age. The consent paper addresses this by hypothetically proposing several different zones of trust for Jane Doe.

### *Jane Doe Story*

Come with me on a short journey into the world a few years from now where Jane is walking down a street. She's wearing AR glasses or lenses and has a communication wristband around her arm also monitors body functions.

As she steps out the door, there are hundreds of miniature cameras on the street. They can instantly tell it's Jane walking by her face, her gait, and the emotions she's displaying. The municipality where she lives might display a message "Hi Jane! There's a winter storm coming tonight. Please ensure your car is off the street such we can clean the street once the storm is over."

As she's walking, she stares at a new car driving by. Her eyeblinks/second and where she stares are all recorded. Since she stared for a while at the new car, in her glasses pops up a customized message for the new car, inviting her to come in for a test drive.

As she approaches Acme Store Inc., they'll have seen her coming long before she gets to the store. They'll know how many other times she walked by the store, what her emotions were, what advertising worked to bring her into the store, etc.

They'll display a customized message in her AR glass/lens; "Jane! Wonderful warm winter mauve mittens 30% off!"

Huntington Ventures Ltd.  
The Business of Identity Management

She decides to walk into the store, greeted immediately by her own AI generated personal sales assistant. It knows LOTS about Jane and tailors what they tell her based on all her history.

While walking down the street, Jane's communication device is continuously monitoring her body functions. It noticed a persistent rise in her blood pressure and thus sends a message, from Jane's health insurance company, to address this.

### ***Hypothetical Zones of Trust***

Jane MUST be able to determine her level of trust. It should range from the ability to act anonymously, though to automatically providing consent for their identity and biometric/behavioral data to be used by governments and third parties. Let's see what happens to Jane using the following hypothetical levels of trust:

#### ***No Trust – Wants to Act Anonymously***

Jane doesn't want the municipal systems or the stores to know it's her walking down the street. Hypothetically, she would tell her lens or, personal identity and access management system, she wants to act anonymously.

The lens or, personal identity and access management system, would broadcast this to the municipal systems as well as the stores. Both systems would not be able to process the data identifying Jane. Thus, as Jane approaches Acme Store Inc., the advertising would be generic.

If Jane decides to enter Acme, there would be no customized AI robotic assistant to assist her. She will have to ask for assistance if she decides she needs it.

#### ***Some Trust – Wants to Release Identity but Not Provide Consent for Data to Be Used***

Jane decides she is willing to release her identity. However, she doesn't want others to use her data without providing her consent. Hypothetically, Jane might pre-set in her personal identity and access management system configuration, allowing the municipality and Acme to know who she is by name but not be able to process data.

As Jane walks down the street, she might see a message in her AR lens from the municipality saying "Good Morning Jane!". When she approaches Acme is might present advertising in her AR lens with her name on it. As she enters Acme, she will see advertising saying, "Jane, 30% off!" Acme Stores, however, can't use the data from Jane to customize the advertising without her consent.

Jane would be prompted to provide her consent. Recording of her decisions must occur in Jane's central consent management service.

***Medium Trust – Allows Both Identity and Data to Be Used, Automatically Providing Her Consent***

Jane would likely pre-set the lens or, her personal identity and access management system, with automatic consent permission for specific categories, e.g., municipal, certain types of stores, etc. As she walks down the street, the municipality instantly knows it's Jane and also uses her historical and present data. It might send a message to Jane's lens saying "Winter storm coming later today. Please ensure your car is removed off the road since you're on the main thoroughfare requiring cleaning of the snow."

As she approaches Acme, the store would likely display in Jane's lens customized advertising saying "Warm winter gloves, in your favorite color, now on sale!" Jane enters Acme. At the door, a virtual AI assistant appears. It greets her by name, "Hi Jane!" and proceeds to show her several different glove styles based on her historical buying patterns.

As Jane looks around the store, her glance might stop for a second at the dresses. Her heart rate and skin temperature might increase. The AI assistant instantly notices this, compares it to her buying patterns, and offers a 20% discount for her on specific dresses.

Note the first time Jane comes in contact with the municipality, Acme Stores, etc. her consent would be automatically given and logged into her central consent management system.

***High Trust – Gives Permission for the Use of Her Identity and Data by Anyone***

Jane hypothetically pre-sets the AR lens or, her personal identity and access management system, to broadcast she is permitting her name and data to be used by anyone. As she walks down the street, passing a car which she looks at, her AR lens displays car advertising. When Jane passes a restaurant and looks in the window, the restaurant sees she was there once a year ago. It knows what food was ordered, where she sat, what she looked at while eating, etc. It might display in Jane's AR lens advertising around the type of food she likes with a welcome back discount.

Note: Jane would automatically provide consent for use of her identity and data. As she encounters new stores, etc., her permission would be given and logged into her personal consent management service.

***Let's Assume We Have A New Legal Consent Model – What's Next?***

Hypothetically, we now have:

- Foundational identity layer containing new laws for humans and robots
- New age, global identity assurance layer
- New data laws where we own and control our data
- New age, worldwide consent laws allowing us to manage our consent and providing zones of trust

The next piece is a personal identity and access management system.

## Personal Identity & Access Management (IAM) System

### IAM Premise

In the paper “[Technological Tsunami & Future of IAM](#)”, in the section ‘Jane Doe’s IAM System,’ states the following:

**I have a premise, in the not so distant future, due to the technological tsunami wave, each of us will have our own IAM system:**

- It may be created ourselves (via things like opensource foundations/companies) or, perhaps offered by telco suppliers, Google, Facebook, Amazon, Microsoft, etc.
- We will use it to approve and create who we’ll send our identity and data to
- It will also react dynamically with other IAM systems as we come into contact with them virtually or physically
- It also applies to kids.
  - Kids require their parents/legal guardians’ permission to provide identity information. Additionally, they must also approve the use of the kids/other's IAM system with fine-grained control
- The result? Effectively, we'll be federating our identity/data with other enterprises
  - I suspect OpenID Connect or, some modified version of it, will be used to federate Jane Doe's IAM system with others
  - There's another option, i.e., a "federation hub"
    - It could act on Jane's behalf, with other enterprises
- Given the sheer number of IAM systems Jane will be interacting with, legal automation software will likely be used
  - It will establish initial contracts between Jane Doe and the enterprises or other people's IAM systems she will be interacting with
- Consent will become a significant issue for Jane to manage due to the sheer number of them.
  - In the paper “[Consent Principles in the New Age – Including Sex](#)” I lay out requirements for new age consent laws
  - Given these laws don’t currently exist, the use cases below suggest what the IAM systems should do
  - All of them recommend leveraging [Kantara User-Managed Access and User-Managed Access Federation](#)
- I foresee a growing interest in enterprises wanting to act as Jane's IAM system on her behalf.
- The personal IAM is also applicable to robots

However, before diving into a personal IAM system, let’s first of all address people who don’t have any technology. Thus, they won’t have any personal IAM system.



### People Without Access to Technology

Here's a sample use case:

A mother and child are walking down the same street Jane Doe did earlier in this paper. The road contains hundreds or more miniature cameras. People walking towards them also will have technology able to identify them, their emotions, and even predict their behavior. The woman and child have no technology. How will their privacy be protected?

**My thoughts are, by law, if a person doesn't have any technology, all other identity and access systems, including miniature cameras et al., won't be able to process the information on them. Use of people's identity, behavior, and biometrics MUST REQUIRE THEIR CONSENT BE GIVEN.**

There will be exceptions, e.g., identifying people in a crisis. However, this is the thin edge of the slippery slope of lack of privacy. In particular, governments may want to use this to justify social, political, and behavioral monitoring. Global laws need to be created, limiting, and controlling the use of the exceptions.

### Legal Considerations About Personal IAM

A personal IAM system hypothetically has many legal considerations.

#### *Managing the Identity*

A person of legal age controls their government-issued digital legal identity. What they decide to do with it is at their discretion. The use of their personal IAM system to manage this, therefore, requires some legal minimum standards addressing, but not limited to:

- Authorization for their identity to be used
- Delegation of their identity to others
- Chain of custody for their identity
- Archival policies covering the use of their identity



### **Authentication Management**

How does the IAM system know it's the person who owns and controls it, who are configuring and changing their personal IAM system? Thought must be given to the establishment of minimum authentication standards used to achieve this.

Note: The creation of new behavioral/biometric authentication mechanisms will likely occur due to the hockey stick shaped curve earlier discussed. Thus, any new laws/regulations of personal IAM minimum authentication standards need to be flexible to adjust rapidly. However, any new claim needs to be scientifically proven and also tested to see how it can be potentially spoofed.

Therefore, the global enterprise recommended in the Global Identity Assurance section of this document, to independently test biometrics/behavioral technology, should also be responsible for authentication measures. Based on their considered recommendations, laws can then be adjusted.

### **Consent Management**

The legal consent management principles of consent management, outlined in the consent section of this paper, need to be administered by the personal IAM system. Thus, there should be minimum legal standards for personal IAM systems to meet including, but not limited to:

- Chain of custody
- Archival policies
- Based on risk, administering proper identity and credential assurance for consent
- Properly configuring zones of trust
- The personal IAM may, or may not, be the place where the person's UMA/UMA Fed are stored and administered from

### **Federating the Identity and Data**

Federation is first and foremost a legal agreement between two or more parties. The agreement typically states things like identity and credential assurance, use of data, etc.

As I see it, a personal IAM system federating with one, hundreds or thousands of others, enterprises and governments, presents new challenges. These include, but aren't limited to:

- Managing the legal agreements on a large scale
- Automating much of the legal agreements, using the zones of consent, as and where applicable
- Stating what data a person will automatically send to pre-configured zones of trust, industry segments, specific people, etc.
- Managing changes to federation agreements as the user decides to change their identity, data, and zones of trust
- Notification processes between the personal IAM and federation partners
- Termination clauses and processes when the person wants to cease sending their identity and/or data to one or more federation partners

### Technical Considerations

To make the use cases with Jane Doe work requires a personal IAM system to be able to continuously transmit its preferences and/or be polled by other systems.

### Follow the Electrons

I always tell my project teams, follow the electrons, to map out endpoints, security attack vectors, and protocols used. Let's hypothetically follow Jane Doe's electrons from her personal IAM system.

### Endpoint

Where does Jane Doe's personal IAM system exist? There are several possible locations for it including, but not limited to:

- Within Jane Doe's body on a microchip
- A wearable device Jane is wearing. It could include, but isn't limited to:
  - Smart glasses
  - Smart lenses
  - Clothing
  - Wrap around wrist communicators
  - Exercise devices
  - Etc.
- A traditional smartphone

Regardless of where Jane's device for housing her personal IAM system exists, IT MUST BE SECURE. In the paper "[Technological Tsunami & Future of IAM](#)," I discuss IoT devices security including, but not limited to:

- Identity registration
- Weak security within the device
- IoT firmware updates
- Outdated IoT components
- Deprovisioning the device

Hardening of the device endpoint MUST occur. Further, due to the hockey stick shaped curve of technological change, today's best-hardened endpoint might become tomorrow's turd. Therefore, legal regulations about these devices should require minimum standards for endpoint hardening, with time allotments for updating weakened endpoint security.

Huntington Ventures Ltd.  
The Business of Identity Management

### Transport Layer Security

As the electrons flow out of the device endpoint, the handshake between the endpoint device and prospective federation partners endpoints MUST BE SECURE. The use of Transport Layer Security (TLS) protocol should occur. However, different TLS versions use different cipher suites. Not all of them are secure. Given the hockey stick shaped technology curve, today's best cipher suite might also become tomorrow's turd.

Therefore, legal regulations for these devices should state acceptable cipher suites. Regulations should also state periods for changing out old cipher suites which are now no longer secure.

### Digital Certificates

The personal IAM system should likely have:

- A digital certificate to digitally sign communication between the personal IAM system and the federation partners
- It could be the one issued by the civil registration service to the identity

However, how will this work with legal minors? They won't be issued a government digital certificate to sign legal documents until they reach the age of majority. Careful thought needs to be given technically and legally to address this challenge.

As well, if a digital certificate expires or, needs to be changed out, then legal, business and technical processes need to be developed for this.

### DMZ Areas

A good security architecture leverages demilitarized zones. For non-technical readers, imagine a border area between two countries. As you leave the security zone of one country, you enter a “de-militarized zone” and then enter the other countries border. The borders are analogous to firewalls/load balancers. Enterprises will often create a DMZ to examine incoming and outgoing data.

With the advent of artificial intelligence (AI), the DMZ should be screening both incoming and outgoing data. It should be alerting the user if any privacy problems are developing.

The miniaturization of devices via nanotechnology, plus the advent of 5G wireless, means this type of architecture can now make its way into the personal IAM device.

### Secure Transmission of the Data Internally

In good network design, after passing through the DMZ, identity data is encrypted within an enterprise's network. The use of this architecture should occur within the personal IAM device.

Huntington Ventures Ltd.  
The Business of Identity Management

***Legal Considerations Addressing Numerous Potential Attack Vectors***

Adding all this up, as Jane Doe walks down the street, there are numerous attack vectors, via her personal IAM system. As technology develops, attack vectors can and will change. Thus, Jane Doe's federation legal agreements should likely specify minimum standards, addressing each of the areas described above.:

- Endpoint security
- TLS security
- Digital Certificates
- DMZ standards
- Internal identity/data security
- Etc.

Jane Doe's federation partners will also likely demand, as part of the federation contract, minimum standards for things including, but not limited to:

- Identity registration
- Security within the personal IAM device
- Firmware updates
- Replacing outdated IoT components
- Deprovisioning the device

By specifying these in the contract, the federation partners can be somewhat assured:

- The devices are secure preventing malicious people from obtaining access to the device and then either sending false information and/or intercepting data from within the device
- Device endpoints and transmission of the data is secure
- Personal IAM devices are correctly registered and deprovisioned from the federation partners' systems
- Any firmware change is promptly made to ensure the security is kept up to date

### **Personal IAM Applies to Robots as Well**

Over time, as robotic technology develops, I suspect they too will require their personal IAM system, using standards described above for human's federation contracts. It should include robotic singularity. Here are two sample use cases to consider.

#### ***Autonomous Robot Walks Down Street***

An autonomous robot walks down a street. Just as in the human, Jane Doe example, it will encounter hundreds or more of miniature cameras on cars, buildings, people and also, other robots walking toward them. In the future, a robot may closely resemble a human..

Who configures the robot's IAM system? What decisions are the robots? Must it share, by law, that it's a robot to others via the IAM system? What kind of robotic privacy should there be?

#### ***Three Robots Acting in Singularity***

Robots 1, 2, and 3 are acting together in singularity. Thus, anything robot 1 learns, does, experiences, etc. is instantly absorbed and acknowledged by the other two robots.

It poses several challenges regarding robotic identity and access management, including, but not limited to:

- How is each robot uniquely identified?
- Is there a legal way to determine if a robot is acting in singularity?
- How does identification, authentication, and authorization apply to the three robots?
- Does a federation partner know that any data sent to robot 1, automatically makes its way to robots 2 and 3?
- How are federation agreements arranged for robots acting in singularity?
- What kind of privacy laws need to be created, protecting a person or another robot, not part of the singularity?
- How will all of this be enforced technically, business process and legally?

## Summary

In some of the papers, I use this image:



That's us, holding up our old legal privacy framework, i.e., the umbrella, protecting us from the incoming technological wave. The surprising thing is most of us can't see the wave approaching. We carry on, working with our old framework, while around us, the puddle rapidly grows.

Currently, the technological tsunami wave is driving us. It's rapidly creating what I call a "non-private world." We become enslaved by the technology, companies, and governments leveraging this.

It's time we took control of our privacy and future back into our own legal hands. Doing so requires new judicial dikes, able to channel the technological waters swiftly. It requires a complete rethink, creating a new legal privacy framework.

This paper has outlined the components of the new legal privacy framework:

- Identifying people and robots by rethinking the planet's civil registration systems
- Global standards for identity assurance
- People owning and controlling data about them
- New age consent
- Personal identity and access management systems for people and robots

**The unprecedented age we live in requires global thinking, global laws, global enforcement, and when technology outdates them, an ability to rapidly change laws and regulations. It's our choice. Our privacy can be swept aside by the incoming waters or, we can work collaboratively together, creating new laws allowing us to live privately in a non-private world.**



Huntington Ventures Ltd.  
The Business of Identity Management

### 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.

