Consent Principles in the New Age – Including Sex

Author: Guy Huntington, President, Huntington Ventures Ltd.
Date: Created November 2018/Updated March 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

Consent Principles in the New Age – Including Sex

Executive Summary

A tsunami of technological change is rapidly approaching and it's affecting our consent. The tsunami is caused by the convergence of:

- Artificial intelligence (AI)
- Augmented reality (AR)
- Virtual reality (VR)
- Robotics (both virtual and physical)
- Genetic engineering
- Nanotechnology
- Wireless communication

There are three waves coming at us:

- 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

To meet the tsunami challenge, the paper shows the components of a new age consent legal framework:

- Centrally see/manage all consents given
- Change consents where allowable by law
- Consent management
- Consent management transfer policies
- Managing minor consent
- Managing power of attorney consent
- 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

An example of consent management in the age of AI/AR/VR/physical environments is given.

The technological tsunami wave is approaching and we don't have the right legal toolkit to deal with this.

Introduction

A tsunami of technological change is rapidly approaching and it's affecting our consent. The tsunami is caused by the convergence of:

- Artificial intelligence (AI)
- Augmented reality (AR)
- Virtual reality (VR)
- Robotics (both virtual and physical)
- Genetic engineering
- Nanotechnology
- Wireless communication

First Consent Wave – IoT Devices

The first consent change waves approaching our shore are the Internet of Things (IoT). People are beginning to acquire numerous IoT devices. For each one, they provide their consent. Let's use Jane Doe as an example…

Jane has an IoT watch, bought a smart fridge, washer and dryer, and her doctor has prescribed her a medical device able to send continuous information about her body. Jane realizes she has a problem. What is it? Each device requires consent and her consents change. Let's take a closer look.

- Watch:
  - Jane wants to share her exercise information with some new fitness friends and her trainer. She does this within the watch application.
- Appliances:
  - Jane wants to connect her smart appliances to her favorite stores such when the fridge runs low on certain items or, her clothes begin to wear, they'll be automatically restocked. She does this within the appliance app.
- Medical device:
  - Jane has to give her consent approval to her doctor to receive the biomedical information. She also wants to send it to her partner. She has to do this within her health plan application.

What Jane's realizing is she's beginning to manage many different consents in different places. She has to recall the login/passwords for each app. Whenever she wants to make a consent change (e.g. adding a fitness friend to her group where the data's shared) she has to go to each app to do this. She's quickly understanding, as the number of IoT devices she owns grows, it's going to become unmanageable. She wishes she could centrally manage them.

She's also beginning to become uncomfortable with the security. Her watch, appliances and medical device's all have the same level of security, i.e. username and password. She thinks some of her data, e.g. medical information, should have a much higher level of security than the others. What she doesn't want to happen is someone to obtain her username and password to change consents for the medical device or, to masquerade as her partner and mis-use it.

Second Consent Wave – Sexual Consent

The rise of women's movements, planetary wide, brings with it a need to prove consent before sex. As a result, today, there's an emerging industry on sexual consent applications. However, there is currently a debate going on as to whether or not these are legally valid:

- "Does 'yes' mean 'yes?' Can you give consent to have sex to an app?"
- "Why consent apps don't work, according to criminal lawyers"

Regardless of the legal efficacy, people are using them. Let's go back to Jane Doe.

She wants to have sex with a partner she just met. They use a sexual consent app to confirm this is what they want to do. Jane has to manage these consents in yet another application. If anything comes up a year from now about if she gave her consent or not, she'll have to recall the login information, access the app and find her consent history. Once again, she's wondering why she can't manage all her consents from one place?

Third Consent Wave – AI, AR, VR and Robotics

Wired Magazine recently published an article "AR WILL SPARK THE NEXT BIG TECH PLATFORM—CALL IT MIRRORWORLD". It depicts a revolution where artificial intelligence (AI), augmented reality (AR), virtual reality (VR) and miniature 360-degree cameras, blur the realities with the physical world.

Come with me on 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 select a customized message which is displayed in her AR glass/lens; "Jane! Wonderful warm winter mauve mittens 30% off!"

She decides to walk into the store. She's immediately greeted by her own AI generated personal sales assistant. They know LOTS about Jane and tailor what they tell her based on all her past history.

While walking down the street, Jane's communication device is constantly 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.

This is only but one small example of the tsunami wave coming. Now, put yourself in Jane's shoes. She interacted with several different parties:

- Municipality
- Marketing firm displaying the car advertisement
- Car sales company
- Acme Stores advertising
- Acme Stores AI sales assistant
- Health insurance company

For each one, she should have had to give her legal consent for the following:

- Her identity to be used
- Her data to be used

Similar to the earlier medical IoT example, her levels of consent risk also vary. Her store purchasing behaviour/history and her medical data, are higher risk than the municipality letting her know snow is coming and asking her to move her car.

Jane now has literally hundreds or thousands of consents to manage. She needs the ability to:

- Centrally manage all her consents
- Pre-authorize consents
    - She doesn't want to be bombarded as she walks down the street with consent requests
- Enforce different levels of identity and credential trust based on risk
- Live and act anonymously if she so chooses

It's Even More Complicated…

The AI/AR/VR/physical environment and robotics revolution affects legal minors as well as adults. To illustrate this let's have Jane Doe, who's a legal minor, wanting to do what her friends are talking about, i.e. having virtual sex. Note: If you're not familiar with this, read the paper "Virtual Sex, Identity, Data and Consent".

As the paper illustrates, Jane will want to get around the system to do this. She'll try to use Sally Smith's digital identity, who is of age of consent, and use Sally's AR/VR, touch, smell, devices, etc. to masquerade as Sally, entering the VR sex environment.

The paper also illustrates Jane could be in one legal jurisdiction, her partner, or partners, in other jurisdictions, some of them may be AI generated, and the VR sex environment in yet another jurisdiction. Each jurisdiction has their own, unique, age of consent laws.

A major component of protecting the child is the ability to determine the identity, their age and have informed legal consent. As well, the replay section of the document highlights Jane's need to provide her consent for replay, storage, sharing, etc.

Tsunami Wave Legal Toolkit

The tsunami wave is approaching and we don't have the right legal toolkit to deal with this.

There are three main legal toolkit components:

- New identity framework
  - Readers should review the following for a detailed discussion on this:
    - "Legal Person: Humans, Clones, Virtual and Physical AI Robotics – New Identity Principles"
    - "Policy Principles for AI, AR, VR, Robotics & Cloning - A Thought Paper"
- New data framework
  - Readers should review the following for a detailed discussion on this:
    - "Policy Principles for AI, AR, VR, Robotics & Cloning - A Thought Paper"

- New consent framework
  - **That's what this paper is about!**
  - Readers can also review it in "Policy Principles for AI, AR, VR, Robotics & Cloning - A Thought Paper"

This tsunami technological revolution means one can't have one component without the other two.

Consent Legal Framework Principles

In the not too distant future, due to the rise of AI/AR/VR/physical environments plus the Internet of Things, Jane Doe will likely be managing hundreds or many more consents. These will span across disparate enterprises, devices, networks and operating systems. As a result, Jane will want to:

Centrally See/Manage All Consents Given

This is possible using the protocols Kantara User Managed Access (UMA) and User Managed Access Federation (UMA Fed). It allows Jane to centrally see as well as manage all her consents, regardless of the platform/application/device used.

Jane may want to set up this central consent managed service herself, or use one provided by other enterprises and/or government. However, there are currently no laws/regulations in place mandating use of this to allow for Jane's control of her consent.

Change Consents Where Allowable by Law

When Jane's born, her parents/legal guardians are granted, by law, the ability to manage Jane's identity and data. Jane's parents arrange to have Jane stay for a month with her grandparents. Her parents decide to grant legal consent to her grandparents to manage Jane's identity and/or data to differing degrees of granularity.

For example, they might grant consent to the grandparents to allow them to manage Jane's identity and data with medical providers. This would be done via the central consent managed service her parents use. If they want to change this to her uncle, instead of her grandparents, they would do so via the consent managed service.

However, there are considerations need to be taken into consideration when crafting new laws/regulations. For example, the identity and credential assurance required for Jane's parents to allow someone to see the output of a fridge IoT device, is much different than granting someone potential control over Jane's identity and data. Therefore, the laws/regulations need to specify categories of risk and assign minimal identity and credential assurance required.

There are many instances where the consent should be recorded BUT it can't be changed. For example, when Jane Doe applies for a passport, she must provide her consent for a background check, etc. This type of consent should be recorded in the central consent registry, BUT not be allowable for Jane to change the consent. Therefore, the consent laws/regulations need to specify what types of services these are.

When any police, or other legal agency, want to view Jane Doe's consent management service, an order by a judge should be required, according to the consent laws/regulations.

Consent Management

When Jane Doe uses her consent management service, she MUST be confident the service is secure. This includes, but isn't limited to:

- Identity and credential assurance required
- Endpoints used by the consent managed service and the other endpoints where the consent will be applied
- TLS used to secure the communication channel
- Encryption of the actual consent
- Digital signatures used for the consent
- Storage standards for the consent managed service
- Archival polices for the consent managed service

The laws/regulations should specify minimal standards for consent managed service providers based on risk. Further, since technology changes, the laws/regulations should be designed to be quickly changed when new technology arrives obsoleting what was once thought to be secure practices.

Consent Transfer Policies

Jane Doe wants to transfer her consent managed service from Consent Managed Service Provider (CMSP) 1 to CMSP 2. Jane wants to be assured the transfer is secure and, if required, ensure her previous consent managed service records will be available for some time. This requires laws/regulations specifying minimum standards for the transfer process, archival policies and data retention times.

These consents could be used in a court of law for criminal or civil suits as well as by police agencies. The laws therefore need to spell out the conditions upon which police agencies can obtain access to these records.

We therefore need to develop consent transfer use cases, derive guiding principles and use these to create new consent transfer laws/regulations.

Managing Minor Consents

In the use cases given above, Jane Doe's parents assigned consent managing her identity and data ability to her grandparents and her uncle. The central consent managed service needs to be able to display, in one place, all of Jane Doe, the minor's, consents. The central consent managed service should specify granting of the ability to manage her consent from her parents to the grandparents, uncle and hospital, AS WELL AS displaying all consents given by these entities.

If Jane Doe's legal custody changes, so must her new custodians' abilities to grant consent. The new age civil registration laws/regulations AND the consent laws/regulations should specify the process for doing this.

When Jane Do reaches legal age, the central consent managed service should transfer over to her control. All of the above needs to be specified by new age consent laws/regulations.

Finally, the principles and use cases derived may or may not also require changes to the central consent management protocol, Kantara UMA and UMA Fed.

Managing Power of Attorney Consents

In her old age, Jane Doe requires others to act as power of attorney on her behalf. The person, or people, assigned to this, must have laws/regulations governing how they will be assigned to manage Jane's central managed consent service.

Additionally, they must have the ability to delegate consent to others as prescribed by laws/regulations. As with minors, the central consent managed service should specify granting of the ability to manage her consent to others AS WELL AS displaying all consents given by these entities.

If Jane Doe's legal power of attorney people change, so must her new custodians' abilities to grant consent. The new age civil registration laws/regulations AND the consent laws/regulations should specify the process for doing this.

Robotic Consent

In the paper "Policy Principles for AI, AR, VR, Robotics & Cloning - A Thought Paper" and "Virtual Sex, Identity, Data and Consent", it lays out how Jane can manage both virtual and physical robots via her consent. The tsunami wave approaching means, in the not too distant future, we will have millions and then billons of robots to manage consents with.

Entities like Sophia the robot and one's produced by Sanctuary, are only the early days of robots able to act and think like us. In the paper "Legal Person: Humans, Clones, Virtual and Physical AI Robotics – New Identity Principles" it states, in the not too distant future, these types of entities might be able to legally function on their own. Therefore, readers of this paper need to expand their thinking beyond humans controlling robots and apply this to a new age consent legal framework where there is a plethora of robots, some acting on our behalf and others independently.

Chain of Identity/Data Custody Via Consents

When Jane Doe's parents grant their consent to her grandparents and uncle to use her digital identity and manage her data, there must be a clear legal trail of custody shown. The same applies when her grandparents give their consent to have Jane's identity and data managed by the hospital. Consent management of the citizen is therefore extremely important in the new age. It must work in each jurisdiction AND around the planet, seamlessly.

All Consents Shall be Governed by a Central Consent Law/Regulation

As stated in the "Centrally See/Manage All Consents Given" section of this document, **my premise is there should be one law governing consent all other laws point to.** As technology changes, the consent laws and regulations should be relatively quickly updated as well.

Consent Laws Need to be the Same Globally

Jane Doe lives in a world of nation states. Each has their own national laws. Within many of them, are states/provinces, each with their own laws. This system has worked relatively well for the last few hundred years. However, with the rise of cell phones, wireless and the internet, it's now no longer working so well. Consider cybercrime…

According to the World Economic Forum's "Fighting cybercrime – what happens to the law when the law cannot be enforced?" in the US only 5% of cybercrimes are successfully prosecuted! Why such a low rate?

The prime reason is jurisdictions. As the CSO article "Why it's so hard to prosecute cyber criminals" states, "It's hard enough to successfully prosecute a cyber criminal if they originate in the same jurisdiction as the victim, but close to impossible when both reside in different locations." Come with me on a journey, only a few years into the future…

The advent of AI/AR/VR/physical environments will blur not only the lines between virtual and physical realities, but also blur lines between jurisdictions. In effect, the planet "shrinks" from a business, social, political, legal and criminal perspective. People's highly personal data, and there'll be LOTS of it, will fly around the planet at the speed of an electron.

Jane can be watched identified, her emotions determined, as she walks down the street, into a store or wherever. It will do Jane Doe no good, if she's walking down the street in one country, feeling secure about herself because the nation she lives in adheres to new age privacy laws, when her data is being sent to other nation states where it's easily, criminally mis-used. So, what's the answer?

We need global principles, driving consistent global laws, across all jurisdictions. This might seem a fanciful statement, yet without this, crime rates will continue to increase. When their systems are breached, industry will pay for this via financial losses, civil lawsuits and criminal charges. Governments will feel increasing pressure from citizens to do something. Yet, they are mostly powerless to do so on their own without collaborating with others.

This applies to consent. Let's go back to Jane Doe, the person who wants to access a virtual sex environment.

Jane MUST provide her legal consent to enter/participate in the environment. She may or may not specify the type of sexual acts allowed with her in the environment. This too requires her informed consent. The replay ability also needs her consent as does who the session can be shared with.

Recall Jane might be in one jurisdiction, partners in other jurisdictions and the VR sex environment hosted in another. Therefore, to protect Jane and the other participants, it requires common managed consent laws/regulations implemented globally. These must clearly state the consent rules as well as providing common legal rules for laying civil and/or criminal charges.

My thoughts are different industry sectors producing AI/AR/VR/physical environments, and also those consuming them, will be motivated to have a level, legal playing field. Early adopter governments will also feel motivated to collaborate, as they realize virtual robots easily move across their borders. By combining these groups with privacy/technology experts, use cases can be established, principles elucidated resulting in new common laws/regulations implemented.

One cannot boil the global political ocean. However, one can methodically create a new global model in a few countries, implement it and bring others to adopt it. Industry is a prime driving factor with the new technology.

An Example of Consent Management in the Age of AI/AR/VR/Physical Environments

Let's return to the example of Jane Doe walking down the street. Jane MUST be able to determine her level of trust. This 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 she wants to act anonymously.

The lens 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 would 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 but doesn't want to release her data to be used without providing her consent. Hypothetically, Jane might pre-set it such the municipality and Acme are approved 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. Her decisions must be recorded 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 with automatic consent permission for certain 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 a main thoroughfare requiring cleaning of the snow."

As she approaches Acme, the store would likely display in Jane's lens a 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 historic 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 certain 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 Identity and Data to be Used by Anyone

Jane hypothetically pre-sets the AR lens to broadcast she is giving permission for her name and data to be used by anyone. As she walks down the street, passing a car which she looks at, it her AR lens displays car advertising. When Jane passes a restaurant and looks in the window for more than 1 second, the restaurant sees she's been there once a year ago, knows what she 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 her identity and data to be used. As she encounters new stores, etc., her consent would be given and logged into her personal consent management service.

Consent Trust Summary

These are just some of the mind-boggling things this revolution will bring. Citizens want convenience and personalization which the technologies offer. HOWEVER, privacy can quickly erode. My thinking is countries should work with industry to come up with an acceptable number of risk levels, while enabling industry to leverage the new tools, easily, in an acceptable manner.

Summary

As the technological tsunami approaches, this paper has shown a new legal consent framework is required. It must allow citizens to manage their identity and data, seamlessly, regardless of where on the planet they are located.

A new age consent legal framework must implement new laws and regulations covering consent management services via the Kantara protocols "User Managed Access" and "User Managed Access Federation." However, the protocols alone can't solve the problem.

Different levels of consent risk require different levels of trust. Therefore, as the paper shows, laws and regulations are required stipulating minimum levels of trust for different levels of risk.

They must also set minimum levels for security laid out in the consent management section. The users providing their legal consent need to be assured by the laws of the lands their consent is secure all the way from the user's device through to the consent management service and on to the application, database or system for which the consent is destined.

The new AI/AR/VR/physical environments require a new age trust framework. The paper shows how Jane Doe hypothetically gives different levels of consent trust to function as she walks down a street. Without a secure, easy to use consent legal framework:

- Citizens will be confused by "oddles" of different consent requests
- Industry won't have good user experiences to deliver to their customers
- Governments will be faced with criminals using weak consent management services to use against citizens

Finally, the paper also shows how one jurisdiction can no longer go it on their own, creating their own unique consent laws and regulations. It requires global consent principles translated into global consent laws and regulations.

We as a planet have a choice to make. We can stand around watching the technological tsunami approaching our shores. This will result in almost a complete loss of citizen identity and data privacy.

Conversely, we can act now. We can see the wave coming. It's time to create a new age consent legal framework. This is one of the three critical legal dikes to control the incoming wave of change.

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."