"Privacy Gone – AI, AR, VR, Robotics and Personal Data"

Author: Guy Huntington, President, Huntington Ventures Ltd.
Date: Created 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

Executive Summary:

The paper begins with the example of Jane Doe walking down a street in the not so distant future. She's wearing AR glasses/lenses and has a wrist band communicator able to monitor her body functions. She interacts with the municipality, advertisers, car company and Acme Store Inc. Each second she's generating gigabits of behavioral/biometric data about herself which can be used to identify her. It results in the title of this paper "Privacy Gone".

The paper benchmarks existing technology to see how near or far the technological tsunami waves are including:

- Smart dust
- Miniature cameras
- Augmented reality glasses & lenses
- Virtual reality headsets
- Cyborg insects
- Wristband communicator
- AI sales assistants
- Fifth generation networks
- Behavioral data

To meet "privacy gone" requires a new legal identity, data and consent framework. The paper illustrates premised required for the new data framework:

- 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

This is followed by a discussion, including a hypothetical example with Jane Doe to illustrate them.

It ends with this statement:

We have a choice as citizens of this planet. We can:

- **Simply watch the incoming tsunami technological waves come in and see our privacy be swept away, i.e. privacy gone or,**
- **We can work with industry, governments and privacy groups to create a new global legal data, identity and consent framework**

We have only a limited time to choose.

"Privacy Gone – AI, AR, VR, Robotics and Personal Data"

Introduction

In the paper "Consent Principles in the New Age – Including Sex", I use the example of Jane Doe walking down a street in the not so distant future, wearing AR glasses/contact lenses with a wristband communicator around her arm monitoring her body functions. The street Jane's walking down has thousands of miniature cameras embedded in most things, e.g. poles, cars, other people's clothes, buildings etc. From the first few steps Jane takes out her front door, she'll be recognized by her gait, mannerisms, face, etc.

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.

Each second, Jane will likely be receiving and/or generating gigabits of data. The data contains her emotions, eye blinks, body functions, where she looks, what she looked at, how long she looked for, etc.

It's an age where our old ideas of privacy and anonymity no longer work, i.e. the title of this paper "privacy gone". **Before discussing data, and what needs to be done to protect ourselves in this new age, let's first benchmark where the technology is today**.

Today's Technology

Smart Dust

Forbe's Sep 2018 article "**Smart Dust Is Coming. Are You Ready?**" begins by stating:
"Imagine a world where wireless devices are as small as a grain of salt. These miniaturized devices have sensors, cameras and communication mechanisms to transmit the data they collect back to a base in order to process. Today, you no longer have to imagine it: microelectromechanical systems (MEMS), often called motes, are real and they very well could be coming to a neighborhood near you."

MEMS have been around since transistors in the late 1940's. By the 1990's they had advanced to become widely used in things like cars. In 2016, UC Berkley announced "Sprinkling of neural dust opens door to electroceuticals". These are "the first dust-sized, wireless sensors that can be implanted in the body, bringing closer the day when a Fitbit-like device could monitor internal nerves, muscles or organs in real time."

As the Forbes' article states;
"The potential of smart dust to collect information about any environment in incredible detail could impact plenty of things in a variety of industries from safety to compliance to productivity. It's like multiplying the internet of things technology millions or billions of times over."

It goes on to talk about privacy being one of the major concerns, as billions of these devices are spread over an area.

Miniature Cameras

Cameras are shrinking. This Futurity article published a year ago "Under a millimeter wide and powered by light, these tiny cameras could hide almost anywhere" shows where it's heading. They're shrinking towards the size of silicon chips (this example was a square millimeter).

Meanwhile, today's marketplace is abuzz with small-ish 360 degree cameras So Jane walking down a street won't be tracked with hundreds or thousands of today's camera technology…yet.

Augmented Reality (AR) Glasses & Lenses

The technology is just emerging for AR glasses to become used outside the industrial, medical environments. As the article "The best augmented reality glasses 2019: Snap, Vuzix, Microsoft, North & more" illustrates, there are now lots of choices.

However, it's still early days in the AR contact lens space. Companies doing work in this space include Mojo with a recent announcement "Google Backs Mojo Vision's 'Invisible Computing' Augmented Reality Platform in $58 Million Funding Round". Other companies doing research in this space include Sony, Samsung and others.

Given the above, Jane could be wearing a pair of AR glasses today as she steps outside her house. Smart contact lenses are likely a few years away.

Virtual Reality (VR) Headsets

There are many VR headsets on the market today. Industries driving this technology include gaming and pornography (I've described this in Virtual Sex- Identity, Data and Consent). Jane isn't likely to walk down the street wearing this technology BUT she will be able to use it for things like virtual sex today.

Cyborg Insects

Cyborgs are beings with both organic and biomechanical parts. The concept, created in the 1960's evolved to 2010 when a company, Backyard Brains, released a RoboRoach kit. Designed for students, it allows them to control a cockroach.

Since then, the research has advanced, illustrated by "Controllable Cyborg Beetles for Swarming Search and Rescue". As the chips continue to shrink, one doesn't have to use much imagination to see how insects could relatively soon be used to record video and environmental activity around them.

Wristband Communicator

There are glimpses of change in how we communicate. The Nubia Alpha is a wrap around the wrist smart phone. It's being released in April. Couple this with ever decreasing MEMS. One can see, within a few years, Jane will be walking down the street with a wrist band she uses to communicate as well as monitoring her body functions.

AI Sales Assistants

Remember Princess Leia's hologram from Star Wars in 1977? More than 20 years later, the technology is now appearing to produce this. Today, companies like Ricoh and others, produce virtual sales people. Thus, in the not too distant future, Jane could enter Acme Stores Inc., see a personalized AI generated sales assistant, which would follow her around offering customized advice.

Fifth Generation (5G) Networks

5G networks are just not beginning to be deployed. They offer gigabit speeds. How much speed is required?

This article from 2016 "Why The Internet Pipes Will Burst When Virtual Reality Takes Off" stated "humans can process an equivalent of nearly 5.2 gigabits per second of sound and light" for static images. With eye movement "…assuming no head or body rotation, the eye can receive 720 million pixels for each of 2 eyes, at 36 bits per pixel for full color and at 60 frames per second: that's 3.1 trillion (tera) bits! Today's compression standards can reduce that by a factor of 300 and even if future compression could reach a factor of 600 (which is the goal of future video standards), that still means we need 5.2 gigabits per second of network throughput; maybe more."

So, in the not too distant future, Jane walking down a street will likely be generating and/or receiving data at Gbit/sec.

Behavioral Data

The Guardian has published three noteworthy articles on behavioral date:

- "We underestimate the threat of facial recognition technology at our peril" discussed the use in Australia of a national face recognition system and referenced what was being done in China
- "Are you being scanned? How facial recognition technology follows you, even as you shop" highlighted the use of facial recognition to determine people's moods.
- Don't look now: why you should be worried about machines reading your emotions" discussed the "emotion detection" industry

Today, if there's a CCTV camera nearby where Jane's walking down a street, it's easy to imagine her emotions, gait, etc. being used to identify her.

Last year Forbes article "The Measurement Gap: Augmented Reality In Retail" highlighted the problem there wasn't yet enough data to measure AR in retail. However, this is beginning to change. Retinad is one of the first companies pioneering analytics in both AR and VR.

So, in a few years or less, as Jane enters the store, it's highly likely the AI sales assistant will have all her past buying, emotional behavior data to draw upon.

Technology Summary

Given all of the above, in about 5 or so years, most of the examples given above for Jane walking down a street will not only be possible, but likely be in the process of deployment to use. As AI, AR, VR and robotics are deployed, "privacy gone" is not a far-fetched statement.

New Legal Data, Identity and Consent Framework

Who Owns Your Data?

The "old school" way of looking at data is thinking of data about Jane Doe sitting in some account about her, e.g. retail, tax, health records, etc. and building protection rights for Jane's data. This no longer works in the incoming AI, AR, VR, robotics tsunami wave approaching us.

With the thousands, millions and billions of miniatures 360-degree cameras, tied to the AR glasses/lenses, every second, simply walking down a street will reveal LOTS about you AND be able to identify you. They'll likely be hundreds or thousands of entities consuming the data.

This will include other people and their small miniature cameras they'll be wearing in their clothes, who are walking down the same street as Jane. It will also include municipalities, retail stores, medical insurers, police, etc.

Each second, the gigabits of data will be recorded by the different devices and stored in other locations and/or jurisdictions. So, Jane walking down a street might have her data recorded in several of hundreds of different systems. This requires a rethink of our data laws.

Premise 1: Citizen Owns Their Own Data

Citizens MUST own their own data. It's about them. Any new laws must use this as a premise to create a new legal framework. So, regardless of which entity is recording their behavioral/biometric data, the citizen is the owner of the data, regardless of where it's stored, in whatever jurisdiction.

Premise 2: Citizens Should Control Their Own Data

Citizens MUST control their own data. Any use of the data must require their consent.

For example, when Jane Doe walks down the street, she's interacting with the following entities:

- 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

Premise 3: Data Consent Must Be Informed

A citizen must be informed as to what their consent for releasing their data will involve. For example, Jane Doe must understand by releasing her data, advertisers and car companies can use this data to send her customized messages. She also must provide her consent if the data is to be shared with other entities.

Premise 4: Data Consent Should Be Centrally Managed by the Citizen

Each citizen MUST have the ability to centrally manage their consents. There will likely be thousands of them each year. Thus, citizens must have the option of centrally managing their consents.

Premise 5: Data Consent Process Should be Automated into Zones of Trust

A citizen MUST have the ability to select their "trust levels" relating to their identity, behavioral/biometric and other data. This must range from no trust, i.e. anonymity, through to complete trust, i.e. releasing identity and data to anyone. See the example at the end of this section.

Premise 6: Data for Legal Minors and People Requiring Power of Attorney MUST be Carefully Regulated by Law

The identity, behavioral/biometric and other data about a child or a person who has others legally acting on their behalf MUST be carefully, legally regulated.

Premise 7: Exceptions to the Above Premises MUST be Carefully, Legally Regulated

There are many examples in real life, where exceptions have to be made to the existing premises. These include:

- Medical emergencies
- Disasters
- Police incidents

However, these are the beginnings of slippery legal slopes if governments, police and enterprises take advantage of these to extend their use of the data without the citizen's permission and/or by extending the permissions so broadly as to negate a person's privacy.

Thus, any exception MUST be done by law with privacy groups participating in the creation of the laws.

Premise 8: Global Data Laws/Regulations Required with Global Enforcement

Citizens MUST have the ability to have their data protected regardless of which jurisdiction they are in, the jurisdiction of other entities they are dealing with or where their data is stored. Equally, they MUST have assurance the laws are equally enforced, regardless of jurisdiction.

Data Legal Framework Discussion

In "Policy Principles for AI, AR, VR, Robotics & Cloning - A Thought Paper" I stated I'm hopeful the work of Tim Berners-Lee's "Inrupt", enabling control over our data, will be fruitful. It provides an underlying plank in creating new laws where citizens are in control of their data. However, even if successful, it's not a magic wand.

The simple act of walking down a street creates LOTS of data about Jane, each second. When Jane's walking in a crowd of people, each of them is generating data per second about themselves as well as their relationship to the others.

Zones of Trust

Given this, it's highly likely zones of trust be created. Jane can select which zone of trust she feels comfortable with as she walks down the street. Here's a hypothetical example illustrating this:

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.

Walking in a Crowd

Now let's assume Jane is walking with Sally, Alice and John down a crowded street. Here are there trust levels:

- Jane – no trust
- Sally – some trust
- Alice – medium trust
- John – high trust

Each would be "broadcasting out" their trust levels. For each device monitoring their walking down the street, they would legally apply the trust levels and take action accordingly. Jane wouldn't be allowed to be identified while John would be totally identified and his data used.

Legal Minor's Consent Data

By law, most AI, AR, VR systems MUST NOT be able to process a child's identity. So, If Jane Doe's a minor walking down the street, she must not be identified.

There are exceptions:

- Education
- Health
- Emergencies
- Etc.

When Jane enters a school, her parents/legal guardians MUST provide their consent to the school to use Jane's legal identity and her behavioral/biometric and other data.

When they leave Jane with her grandparents, they'll be able to legally delegate Jane's data consent to the grandparents who in turn, may or may not have the ability to further delegate the consent. For example, if they take Jane to the doctor's to be checked, they might have the ability to delegate Jane's data consent to the doctor. In a medical emergency, the attending medical staff would have the legal ability to instantly obtain Jane's data, as prescribed by law and regulations.

Power of Attorney Consent

Let's say Jane required someone to manage her affairs. By law, the person or people designated will have the ability to manage Jane's identity and other data. They would also have the ability to delegate this to others, as Jane's parents/legal guardians did in the previous example.

Zones of Trust and Police

As the Guardian article "We underestimate the threat of facial recognition technology at our peril" noted, police and nation states like the ability to fine tune their monitoring over a population. This is a very dangerous slippery slope.

At which point does warranted ability to identify and monitor Jane, each second, slide into a total invasion of her privacy when she has done nothing wrong? This leads into the next discussion…

Global Laws Mean Global Enforcement

The paper "Policy Principles for AI, AR, VR, Robotics & Cloning - A Thought Paper" has a section "Global Principles Require Global Implementation". It discusses the implementation of AI, AR, VR, robotics and cloning results in shrinking the planet. This results in global laws/regulations which are globally enforced.

One can see how existing nation states will fight this, to regain their own control. However, over time, industry will want to have a level legal playing field. I believe this will slowly drive into place common laws regarding identity, data and consent into all jurisdictions. Over time, legal standards will emerge regarding what rights police, security agencies and jurisdictions have regarding identity, data and consent.

Summary

The fast-approaching tidal wave of AI, AR, VR and robotics requires a new legal data framework. The first of the waves are already here, e.g. VR and emergence of new AR glasses. The next waves are fast approaching, e.g. miniature 360-degree cameras, AI hologram virtual assistants, smart dust, insect cyborgs, AR lenses and 5G networks. Within about 5 or so years, the full wave will be here. The example used of Jane walking down a street generating gigabits of personal information will become a reality. The result – privacy gone.

This tsunami requires new legal framework dikes to guide the incoming technological waves. They're composed of identity, data and consent.

The paper highlights the underlying premises required to build the new data framework laws and regulations:

- 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

A citizen's privacy is a fundamental principle of living in a democracy. Identity, data and consent are key underlying components of this.

We have a choice as citizens of this planet. We can:

- **Simply watch the incoming tsunami technological waves come in and see our privacy be swept away, i.e. privacy gone or,**
- **We can work with industry, governments and privacy groups to create a new global legal data, identity and consent framework**

We have only a limited time to choose.

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."