I Know Who You Are & What You're Feeling – Achieving Privacy in a Non-Private World

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

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 and a bit, I have written 32 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:

- Thought Papers
  - Artificial Intelligence & Legal Identification – A Thought Paper
    - Artificial Intelligence & Legal Identification
  - 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
- 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.

Executive Summary:

The paper begins, in the not so distant future, with Jane Doe walking down a crowded street with three friends. Each is wearing an AR glass/lens with wrist communicator and clothes monitoring their body functions. For every second they walk, they are broadcasting gigabytes of data. It contains their behavior/biometrics, emotions, what causes them, how they interact with each other and other people, stores, things, etc. on the street. People walking by them and toward them are also seeing portions of the data, while transmitting their own.

Their privacy is gone. It creates what I call a "non-private world".

Before leaping to new legal requirements, the paper does a review of where existing behavioral/biometric technology is today. It concludes new laws and regulations are required to protect the citizen.

The paper then moves to a discussion about the principles required and then dives down into specific requirements for behavioral/biometric data:

- Devices used
- Data transmission
- Data registration
- Data storage
- Data viewing
- Data sharing
- Data removal
- Data breach
- Applications, enterprises, people & robots using behavioral/biometric data
- Ability to relatively rapidly change global laws/regulations
- Global enforcement

It presents a hypothetical example of zones of trust for Jane and her three friends walking down the street.

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

The paper ends with:

Jane must be in control of her privacy in a "non-private world" including her behavioral/biometric data. Otherwise, she'll have no say in people, robots, enterprises, retailers, police, etc. saying "I know who you are and what you're feeling."

I Know Who You Are & What You're Feeling – Achieving Privacy in a Non-Private World

Introduction

In the Not So Distant Future:
As Jane Doe is walking down the street with her friends Erika, Neil and John, each one of them is wearing an AR glass/lens with wrist communicator and clothes monitoring their body functions. For every second they walk, they are broadcasting gigabytes of data. It contains their behavior/biometrics, emotions, what causes them, how they interact with each other and other people, stores, things, etc. on the street. People walking by them and toward them are also seeing portions of the data, while transmitting their own.

Result:

- It's a world where their privacy is gone
- The amount of data being generated will be stored in several, hundreds or thousands of different databases and systems in different jurisdictions planet wide
- It's what I call a "non-private world"

Before diving into requirements for new laws and regulations enabling a new privacy, let's first benchmark where the technology is today for behavioral and biometric data and use of it.

Note: For an understanding of where the AR/VR and 360 degree camera technology is, please refer to "Privacy Gone - AI, AR, VR, Robotics and Personal Data."

Behavioral Technology

Facial Recognition

Facial recognition research began in the mid 1960's. By the mid 1990's it had evolved to "pick out faces in noisy or chaotic "street" environments." In 2006, the results of the "Face Recognition Grand Challenge" showed a 100 fold increase in accuracy of the algorithms as compared to the 1990's AND the ability to differentiate identical twins.

In 2018, a paper published results comparing human face recognition forensic examiners versus face recognition algorithms. It stated, "The best machine performed in the range of the best humans: professional facial examiners. However, optimal face identification was achieved only when humans and machines worked in collaboration."

Commercial use of this technology is now wide-spread. Uses include:

- In 2015, Facebook began to deploy "DeepFace", a system said to be 97% accurate
- 1n 2017, Apple began deploying FaceID
- Today, all Canadian airports use face recognition for foreign travelers
- China has one of the world's largest deployments, with 170 million CCTV cameras going towards 570 million, allowing people to check in at airports, pay for food and withdraw money from their bank account by only using their face

However, this all comes with a price:

- Facial recognition bias
- Non-regulated industry
- State monitoring

This has led to a small industry in anti-facial recognition technology including:

- Reflectacles
- CVdazzle

Emotion Recognition/Sentiment Analysis

Eye Tracking

The "process of measuring either the point of gave (where on is looking) or the motion of an eye relative to the head" has been around since the 1870's. Over the years since eye-tracking measurements usually involve using one of three ways:

- Measurement of the movement of an object (normally, a special contact lens) attached to the eye
- Optical tracking without direct contact to the eye
- Measurement of electric potentials using electrodes placed around the eyes

It was used in different industry sectors like Medicine and aerospace.

Fast forward to 2016/2017, when several eye tracking companies were bought up by Facebook, Google, Apple and others. Why? They were "eying" the future with virtual and augmented reality.

This February 2019 Forbes article "Seven Reasons Why Eye-tracking Will Fundamentally Change VR" lay out what the future looks like. Of all the reasons stated, perhaps the most powerful is "6. Deeper insights". Why?

"Eye-tracking analytics provide valuable insights into user attention which aids developers in understanding how their application is being used. What are users focusing on? Which detail generates the biggest negative reaction? Which the most positive?

On its own, this data allows us to understand key areas of focus and thereby influence how we design an experience; how we play with a user's attention and 'direct' for them in a medium which is not restricted to a simple frame. Taking it a step further, we can pair that attention data with a measure of a user's reaction to what they are seeing, to draw powerful data from an experience. This is where biometrics come into play. Fundamentally, the act of pulling on a VR headset gives us numerous touch-points with the body, which can be key to understanding user response.

For advertisers, the incorporation of eye-tracking offers a whole new set of potential metrics - a level of sophistication that marketers and creatives can use not only to understand the user, but also to shape the experience around them."

To understand what this means to retail, read the next few sections…

Facial Expressions

In the 1960's Paul Ekman and Carroll Izard pioneered the study of facial expressions, postulating one can tell a person's true emotions based on their facial expression. Others disputed this, arguing the expressions determined have more to do with the observer's interpretation than the person experiencing and displaying them.

Since then, research has gone into understanding how the 43 face muscles display emotion. In this 2014 Guardian article, it discusses how scientists mapped 21 different emotions to face expressions:

"Happy, sad, fearful, angry, surprised, disgusted, happily surprised, happily disgusted, sadly fearful, sadly angry, sadly surprised, sadly disgusted, fearfully angry, fearfully surprised, fearfully disgusted, angrily surprised, angrily disgusted, disgustedly surprised, appalled, hatred, awed."

So, how's it being used today and what does the future look like?

- Car companies are working with Affectiva Inc. to monitor driver's emotions and fatuge while driving
- This article describes how Walmart is planning on using customer facial expressions in its stores.
- Here's where VR is using facial expressions to customize the experiences
- Recognizing human facial expressions with machine learning shows where machine learning is playing a role in facial recognitions
- Research is becoming more automated into facial expressions

ECG/EMG/EEG

- Measurement of the heart, Electrocardiography (ECG), began in the late 1800's
- Measurement of muscle activity, Electromyography (EMG,) began in the mid 1960's
- Measurement of electrical activity in the brain, Electroencephalography (EEG), began in the late 1800's

All of the above have numerous medical applications. They can predict the health of the body. However, what used to be measured in the doctor's office is now moving out to wearable technology:

- ECG
  - This article reviews wearable technology built into shirts and wristband devices
- EMG
  - Here's an example of an EMG device in a person's clothes
- EEG
  - Here's a list of some of the EEG wearable device sensors

What's driving this? It's VR and AR. This ranges from:

- Health
- Entertainment
- Gaming
- Education
- Retail
- Sex - The virtual sex industry will likely become a user of these technologies to fine tune a user's sexual experience.

GSR (Galvanic Skin Response)

In the late 1870's a researcher discovered a link between a person's mental activity and their galvanic skin response. Since then, much research has occurred.

Imotions states:

> "While sweat secretion plays a major role for thermoregulation and sensory discrimination, changes in skin conductance are also triggered robustly by emotional stimulation [1]: the higher the arousal, the higher the skin conductance.
>
> The amount of sweat glands varies across the human body, but is the highest in hand and foot regions (200–600 sweat glands per cm2 [6]), where the GSR signal is typically collected from [7].
>
> Skin conductance is not under conscious control. Instead, it is modulated autonomously by sympathetic activity which drives aspects of human behavior, as well as cognitive and emotional states [3]. Skin conductance therefore offers direct insights into autonomous emotional regulation."

Electrodermal activity is well used clinically. Today however, just like EEG, ECG and EMG, it's moved into wearable technology including products from Microsoft and others.

Why are companies using GSR? The answer is AR and VR. Here's a case study showing how powerful GSR and EEG are in understanding the emotional response of a user.

Gait

A person's motion through the use of their limbs, i.e. gait, has been measured since the 1800's. Over the last decade, it's been researched to determine emotions.

Where's this being used now? VR/AR and police:

- Rehabilitation
- Medical
- Police

Signature Recognition

The first signature recognition system was developed in 1965. With the decline in writing due to computers and the development of more accurate biometrics, it's use has declined. However, there has been research done on using digital signatures for authentication with some companies introducing them.

Typing Recognition

The detailed timing information which describes exactly when each key was pressed and when it was released to identify a person has been used since 1975. This paper from 2004, outlined the challenges with using this.

Fast forward to last year. This article "AI-based typing biometrics might be authentication's next big thing" discusses the use of AI to raise the accuracy from 60-70% to reportedly over 99%. A company, typingDNA, is using this for authentication.

Behavioral Example 1:

Let's assume Jane Doe walks into Acme Store Inc. while wearing her AR glasses/lens with her wristband communicator and clothing able to monitor her body functions. As she walks down an aisle, her gaze turns to some clothes and stays focused there for a few seconds. Jane's pulse quickens, picked up by the wristband. Her face is monitored by Acme's many 360-degree miniature cameras. Taken together, they "know" Jane's emotions, compare this to her old buying history, and immediately offer a discount on the clothes to entice Jane to buy it. She sees this in her AR glass/lens display.

The whole process started with Jane gazing at the clothes for time period. Acme Store Inc. will use the data from the devices and feed it into applications like Retinad to process AI decisions. Retailers now know exactly what Jane is feeling and can cater to this. **This is the revolution retailers are working towards**.

The same type of data will be used in many other industries to entice and captivate the person, including virtual sex. As a person gazes longingly at another virtual image, the gaze plus increased heart rate, blood pressure and EEG activity will be processed and used to finely tune the user experience. I've written about this in "Virtual Sex – Identity, Data and Consent."

I suspect, but don't know, these technologies will actually increase peoples' addictive behaviors.

Behavioral Example 2:

Jane Doe is walking down a crowded street with her friends Erika, Neil and John. Each of them has an AR glass/lens, is wearing biosensor clothing and a wrist band communicator also able to monitor body functions.

As they step out into the crowded street, other people in the crowd begin capturing their presence using their devices as do Jane and her friends. Police and government agencies are also able to not only see them, but also identify them, their emotions and determine if they are a potential threat.

Acme Store Inc., "sees" all of them coming, long before they come to the store. For each one, they'll be able to determine how many other times they walked by the store, what their feelings were, what advertising worked to bring them into the store and what they bought. Each one will be receiving a finely tuned message offering them goods and services to draw them into the store.

Behavioral Technology Summary

It's a world where MANY others know your identity, your feelings and your history. It's what I described in another paper as "Privacy Gone". This incoming tsunami wave of technology requires new laws protecting our behavior data.

Biometric Technology

DNA

Deoxyribonucleic Acid, DNA, was first discovered in the mid 1800's. The project to completely map the more than 3 billion nucleotides in humans, the Human Genome Project, completed in 2003. Until recently, the fastest time it took to identify people via DNA was two hours. Recent research indicates it can now be done in approximately 3 minutes.

Ear

In 2005, scientists published a paper on use of the ear as a biometric for identification, claiming a 99.2% accuracy. In 2016, research was published on use of the ear to identify patients in global health claiming "Although an individual ear allowed for high re-identification rate (88.3%), when both left and right ears were paired together, our rate of re-identification amidst the pool of potential matches was 100%."

In 2018, NEC announced use of sound "measuring the differences in the shapes of ear cavities with sound that is inaudible to the human ear" with a reported accuracy greater than 99%. It's working on using this for authentication.

Eyes – Iris/Retina

Iris

John Daugman filed a patent in 1991 for iris recognition. Today, well over a billion people are registered using iris recognition. In May of last year, China was proposing to use iris recognition for its national ID scheme. In July of last year, scientists announced they had developed technology to determine if an iris being scanned was from a person alive or dead.
Readers interested in iris recognition present and future, should read this excellent by John Duagman.

Retina

The idea of using the retina as a biometric began in the 1930's. During the 1970's research and technology developed allowing for retinas to be used as a biometric. It has found usage in the medical community as well as for high security areas. The technology is affected by certain medical conditions and isn't as easy to use as iris scans. However, in February 2018, a paper was published proposing its use as an authentication system.

Fingerprint

The use of fingerprints for identification began in the mid 1800's. Today, fingerprints are widely used to identify. They are also widely used to authenticate people but have had problems with people being able to masquerade as others.

Hand Geometry

In 1985 David Sidlauskas, patented a hand geometry reader. This began the modern day industry of using hand geometry for identification. However, it is not as accurate as other biometrics. Therefore, programs like airports using hand geometry have been replaced by other biometrics. It's still used as part of a multimodal identification system.

Body Odor

In 2014, Spanish researchers published research "recognition rates over 85% which reveals that there exists discriminatory information in the hand odor and points at body odor as a promising biometric identifier."

Vein Matching

Vascular scanning began in the US in the 1980's. In 1997 Hitachi and other launched vein recognition products. The original US inventor, Joe Rice, formed a partnership with a Swiss company resulting in, Biowatch. It uses vein recognition to seamlessly authenticate.

"A Systematic Review of Finger Vein Recognition Techniques", published in August 2018, gives an excellent overview on current state of vein matching as well as examining areas where machine learning can assist.

Voice

Voice biometrics began in the US during the 1970's. Today, it's widely used planet wide as an authentication mechanism. As an example, last October, Apple patented a voice based biometrics access system.

However, voice has a lower rate of accuracy than some other biometrics such as fingerprints, iris and DNA. Thus, it can be spoofed:

- HSBC
- Finnish 2017 study
- Black Hat 2018

Biometric Technology Summary

The sheer numbers of biometrics obtained, stored and shared around the planet, used for identification and/or authentication is several billion. As the above shows, the technology keeps shifting and adapting. As well, new technologies allow older biometric technology to be spoofed. We require new laws and regulations protecting our biometrics.

New Behavior/Biometric Laws Protecting Our Privacy

In the not so distant future, Jane Doe is generating Gigabits of information about herself, including her behaviour and biometric information. From this, she can be identified, profiled and her feelings determined - for each second. From this, with artificial intelligence, she can receive extremely customized and personalized information which change as she changes, each second. Thus, her behavioral and biometric data, become the underlying tools used to build upon.

The data moves at the speed of an electron from Jane to many different other people and robots, both those in close proximity, e.g. those walking down the street towards her, as well as those on the other side of the planet. It also moves to different entities including commercial enterprises, governments and police/intelligence agencies. Thus, the issue of jurisdictions becomes very important to protect Jane.

At a high-level what Jane needs to protect her privacy are new age laws addressing her:

- Identity
- Consent
- Data

The papers:

- "Policy Principles for AI, AR, VR, Robotics & Cloning - A Thought Paper" addresses this from a principle level
- "Consent Principles in the New Age – Including Sex" addresses consent
- "Privacy Gone – AI, AR, VR, Robotics and Personal Data" addresses data

This paper does a deeper dive into Jane's underlying behavior and biometric data by presenting requirements which new laws need to address.

Behavior/Biometric Law Requirements

Underlying Principles

The principles stated in "Privacy Gone" apply here:

- 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

Note: Read the discussion of these principles in "Privacy Gone" for more information.

Specific Behavioral/Biometric Requirements

Devices Used

Behavior/biometric devices used MUST meet Global legal regulatory standards:

- Be able to receive from Jane her "zone of trust"
  - Refer to "Privacy Gone" for a hypothetical illustration of this
- Configure processing of the data based on "zone of trust"
- Meet global laws/regulations pertaining to:
  - Storage of data on the device
  - Device endpoint security
  - Device configuration
  - Device identification
  - Device authorization
  - Device signatures
  - Device encryption
  - Device retirement
  - Other?

Data Transmission

Data transmission requirements MUST meet Global legal regulatory standards:

- TLS levels used
  - Also specifying what algorithms are accepted
- Hashing algorithms supported
- Encryption algorithms supported
- Digital signatures supported
- Endpoint security standards
- Audit standards supported
- Reporting standards supported

Data Registration

Data registration requirements MUST meet Global legal regulatory standards:

- Informed user consent
- Device used
- Registration process
- Training/certification standards for any person, robot or AI involved in obtaining the registration
- Audit processes
- Reporting
- Archive
- Other?

Data Storage

Security storage requirements MUST meet Global legal regulatory standards:

- Encryption
- Hashing
- Use of digital signatures
- Access rights
- Modification
- Deletion
- Archive
- Reporting

Data Viewing/Comparison/Retrieval

Data viewing/comparison/retrieval requirements MUST meet Global legal regulatory standards:

- Informed consent levels for the data
- Identity/credential assurance for person, robot or entity accessing the data
- How the data will be used
- Reporting
- Notification

Data Sharing

Data sharing requirements MUST meet Global legal regulatory standards:

- Informed consent
- Identity/credential assurance for person, robot or entity sharing the data
- How the data will be transferred including:
    - Endpoint specification
    - Endpoint security
    - TLS levels used
        - Must specify algorithms supported
    - Hashing algorithms
    - Encryption algorithm
    - Digital signatures supported
- What the data sharing involves
- Audit
- Reporting
- Storage processes for the shared parties
- Archival processes for the shared parties
- Deletion processes for the shared parties
- Other?

Data Removal

Data removal requirements MUST meet Global legal regulatory standards:

- Informed consent
- Identity/credential assurance for person, robot or entity requesting data removal
- Removal processes
- Notification
- Archiving
- Audit
- Reporting
- Other?

Data Breach

Data breach requirements MUST meet Global legal regulatory standards:

- Data breach definition
- Data breach processes
- Notification
- Remediation
- Audit
- Reporting
- Others?

Applications, Enterprises, People & Robots Using Behavior/Biometric Data

Any application, enterprise, people and robots using behavioral/biometric data MUST meet Global legal regulatory standards:

- Strictly adhere to:
  - Zone of trust definitions
  - User informed consent
  - Process behavior/biometric data accordingly
  - Standards set above for devices, transmission, storage, viewing/comparison/retrieval, sharing, removal and breach
- Exceptions to the above MUST be according to laws and regulations

Ability to Relatively, Rapidly Change Global Laws/Regulations

At Davos, this past year, Justin Trudeau stated "Think about it: The pace of change has never been this fast, yet it will never be this slow again." He's right. As science and technology rapidly change, so too must laws and regulations pertaining to behavioral and biometric data.

Therefore, as technology changes, where warranted, globally, all jurisdictions must agree on processes to quickly make changes to existing behavioral/laws and regulations. These MUST be uniformly adopted and implemented to protect Jane Doe, regardless of where she lives or who's she's interacting with on the planet.

Global Enforcement

As the planet electronically "shrinks", Jane Doe and her three friends, walking down the street, will have their behavioral and biometric data instantly sent, each second, to people, entities, enterprises and governments in many different jurisdictions around the planet. Given this, how is Jane and her friends' behavioral/biometric information going to be legally protected? Without global enforcement, they are legally screwed.

In the paper "Privacy Gone" it states "Premise 8: Global data laws/regulations required with global enforcement". This is discussed in greater detail in "Policy Principles for AI, AR, VR, Robotics & Cloning - A Thought Paper" in 'Global Principles Require Global Implementation'.

While today, in an age of nation states running their own legal laws/regulations, the idea of having common laws/regulations for all jurisdiction might seem "fanciful", the reality is, it's now required. As stated in other papers, the way to achieve this is to get the willing early adopter jurisdictions to begin drafting common laws/regulations. Then, commercially entice other jurisdictions to participate if they want to participate in the economic advantages of the new age.

Example of Zones of Trust for Jane and Her Three Friends Walking Down the Street

Let's go back to Jane walking down the street with Erika, Neil and John, applying zones of trust, illustrated in the paper "Consent Principles in the New Age – Including Sex". Here are the zones of trust each of them selects:

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

Here's what hypothetically could happen:

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

Summary – Being Private in a Non-Private World

The technological tsunami's first waves are now on our planetary shore. As Jane walks down a street, any CCTV camera will likely be able to identify her using technology illustrated in this paper. Now come with me on a journey about 5 of so years in the future…

As Jane walks down a crowded street, many people on the street will have video capture capabilities in their AR glasses/lenses, wrist bands and clothes they're wearing. Each one will be analyzing the others. As Jane looks at a person, up will come identity information about the person, a rating scale of how they're feeling and information about them.

The miniature cameras and sensors will be deployed almost everywhere people go. It will lead to retailer's dream of intimately knowing Jane, her feelings, buying patterns and finely tuning this to deliver highly customized goods and services.

It will also be a privacy person's worst nightmare. Even if Jane isn't wearing any technology, simply her walking down a street will lead to enough knowledge to not only identify her, but also to determine her feelings. They'll be able to predict her future actions by comparing it to her past. Her privacy is gone. It's what I call a "non-private world".

This paper has examined the underlying behavioral and biometric technology used as a building block to identify and learn about a person, most intimately. It laid out specific requirements for behavioral and biometric laws and legislation to protect Jane.

It presented a hypothetical example of Jane and her three friends walking together down a crowded street. It showed how each of them, by using new laws/regulations for identity, data and consent, is in control of their privacy. It enables the person to determine their "privacy in a non-private world". Some can and will act anonymously while others will choose different degrees of trust.

As the waves begin to approach, we need new laws and regulations guiding the waters to safe privacy shores. These laws need to be globally implemented AND enforced. Regardless of the place on the planet where Jane lives, she must be protected.

Jane must be in control of her privacy in a "non-private world" including her behavioral/biometric data. Otherwise, she'll have no say in people, robots, enterprises, retailers, police, etc. saying "I know who you are and what you're feeling."

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.