"Kids' Privacy in a Non-Private World" – Why Even Super Hero's Won't Work

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

TABLE OF CONTENTS

Note to Reader: **3**

Executive Summary: **5**

"Kids' Privacy in a Non-Private World" – Why Even Super Hero's Won't Work **6**

Introduction **6**

Kids Can Act as Adults **7**
Virtual Selves 7
Virtual Sex 7

Consider School, Relatives and Healthcare **8**

Bottom Line: **8**

Privacy in a Non-Private World **9**
Requirements 9
Legal Identity Framework for Kids 10
At Birth 10
Biometrics 10
Unique Digital Legal Identity 10
For People Who Don't Have Technology 11
Parents/Legal Guardian Using the Digital Legal Identity to Verify Their Child 11
Anonymous, Human Legal Identification 12
When Child Enters Their First Year of School 12
Additional Biometric Added to the Civil Registration 12
Delegating Identity to the School 12
Legal Data Framework for Kids 13
Delegating Minor's Data Consent 13
Delegating Minor's Data to the School, Hospitals, etc. 13
Secure, Legal Chain of Data Custody 13
Legal Consent Framework for Kids 14
Managing Minor Consents 14
When Child Custody Changes 14
When Child Reaches Legal Age 14
Be Protected Against Bullying According to Laws/Regulations 14
Minor Walking Down the Street 15
Have Varying Degrees of Trust Approved by Their Parents/Legal Guardians 15

All This Sounds Good but Requires Global Enforcement to Work **16**

Summary - New Laws, New Tools, New Ways of Doing Things **17**

About the Author **18**

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:

This paper begins by examining the technological tsunami approaching our planetary shores:

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

It shows how kids, like adults, will live in a world where simply walking down a street will identify them, even if they're wearing a super hero costume. **It's a world I call "Non-Private". It throws out the door our old concepts of privacy.**

The paper moves into a discussion of the new framework for identity, data and consent:

- Legal identity framework
  - Physical identity at birth
  - Digital identity at birth
  - Legal anonymous digital identity showing you're a human and age of consent or not
- Legal data framework
  - Citizens own their own data
  - Citizens control their own data
  - Zones of trust determined by the citizen
- Legal consent framework
  - Ability to centrally manage all consents
  - Ability to delegate both legal digital identity and behavioral/biometric data
  - Ability for parents/legal guardians to delegate children's identity and behavioral/biometric data

The paper discusses ways to prevent cyberbullying as well as the requirement for global laws/regulations with global enforcement. It presents a hypothetical example illustrating how Jane can have privacy in a non-private world.

It ends with:

"We have a choice. We can simply watch the technological tsunami strike our shores, sweeping away our privacy with it, including those of our children. Or, we can work together to create the new legal dikes to guide the incoming technological waters. If we choose to do something, our kids won't need a super hero to protect them in the sea of life."

"Kids' Privacy in a Non-Private World" – Why Even Super Hero's Won't Work

Introduction

There's an incoming technological tsunami approaching our planetary shores. If left unchecked, it will sweep aside our existing privacy for kids. What's the tsunami?

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

The first wave is now here. The miniaturization of cameras will result in thousands of them being deployed almost anywhere you're going to go. Combined with existing AI face recognition technology, it can identify you by your gait, facial expression, even if you're not wearing any technology.

To combat facial recognition, some companies are now marketing face gear masking your face. However, this won't work against technologies like gait and mannerisms. **Thus, even if the kids are dressed like their favorite super hero, it won't work as AI becomes smarter, leveraging more than just face recognition, to identify a person or robot.**

The next waves are now here in their early stages. The combination of the tsunami technologies results in the creation of AI/AR/VR/robotic environments, where, for each second, gigabits of information are being generated about a person, as they walk down a street. What's in the information?

If you're wearing AR glasses/lenses, wrist band communicators, and any other biosensor devices in the clothes you're wearing, where you look, how long you look at, what excites you, makes you mad, etc. will all be tracked, each second. Combine this AI which will be instantly able to not only identify you, BUT also pull up any information about you on the planet in the public domain.

Note: Read the papers "I Know Who You Are & What You're Feeling – Achieving Privacy in a Non-Private World" and "Privacy Gone – AI, AR, VR, Robotics and Personal Data" to understand this in more detail.

The result? It's a world I call "Non-Private". It throws out the door our old concepts of privacy.

Here's the scary part…our kids will also lose their privacy. As they walk in a park, down a street or in a shopping mall, all of the above applies to them too. Their privacy will be gone.

Kids Can Act as Adults

With the technology, kids can now act like adults in this digital world.

Virtual Selves

Consider virtual selves. As the technology emerges, they'll be able to instantly create one or many versions of themselves. They may not look like them AND they almost certainly won't act like them.

As an example, go here to one of the leading companies, creating "personal artificial intelligence", Oben. Watch the short video. You'll see a virtual assistant able to speak in multiple languages. Companies like this, Google, Amazon, Microsoft, Facebook et al will enable these to do many different tasks for you. The virtual assistants are already much "smarter" than us.

Now come with me on a trip in the not so distant future when a young Jane Doe is able to access versions of this type of technology, creating older versions of herself and begin to do "adult functions".

Virtual Sex

She might create a virtual self, which looks and acts much older, to get it to buy her some cigarettes, alcohol, etc. Or, let's say Jane wants to do what her friends are talking about, i.e. having virtual sex. I've written about this in the paper "Virtual Sex – Identity, Data and Consent".

She can use the VR technology to access virtual sex environments and have sex with one or more partners, who might be located in many other parts of the planet. Some of them might not be "real" i.e. they are AI generated virtual selves. The VR sex environment might be located in yet other jurisdictions.

The result, Jane, who lives in one jurisdiction, might be declared of age by the laws where she lives, yet underage in other jurisdictions where one of her partners live or, vice-versa. How do Jane's parents/legal guardians try to protect Jane and control this? Answer – today they can't.

Consider School, Relatives and Healthcare

This is only the beginning of the revolution. Consider Jane in a digital future attending school, staying with her grandparents and going to the hospital. AI, AR, VR and robotics are just beginning to be used in these sectors.

As Jane enters a school, they'll want to use the technologies to teach Jane. She'll need parents/legal guardian approval to do so.

How will Jane be recognized in these environments, i.e. will others know she's Jane Doe or, simply a human underage or a student of the school? How will Jane be able to tell who the other participants in the environment are? What if they live in multiple jurisdictions, or are AI generated or combinations thereof. How's Jane going to know this? What information about Jane will be shared? Who owns the session data? How is it stored? How is it terminated?

When Jane stays with her grandparents her parents/legal guardians, her parents are likely going to need some ability to transfer management for Jane's legal and digital identities to the grandparents, in a way specifying what they can and can't do, legally with Jane in the digital world. Let's say Jane gets sick while with her grandparents and they take her to the doctor. How will they verify Jane's identity and also grant the doctor access to her medical records?

Now let's assume Jane is admitted to a hospital. Part of the treatment involves use of AI/AR/VR/robotics. The same types of problems exist as those in her school use of these technologies about her identity, data, consent, storage, sharing of the information and termination.

Bottom Line:

Even those kids in the picture at the beginning of this paper, wearing super hero's uniforms, won't be able to stop their identity, feelings et al being monitored and used. They too now live in a "Non-Private" world. So, how can they be protected?

Privacy in a Non-Private World

Requirements

To create privacy in a non-private world, requires the following:

- Legal identity framework
  - Physical identity at birth
  - Digital identity at birth
  - Legal anonymous digital identity showing you're a human and age of consent or not
- Legal data framework
  - Citizens own their own data
  - Citizens control their own data
  - Zones of trust determined by the citizen
- Legal consent framework
  - Ability to centrally manage all consents
  - Ability to delegate both legal digital identity and behavioral/biometric data
  - Ability for parents/legal guardians to delegate children's identity and behavioral/biometric data

A detailed discussion of the above occurs in the following papers:

- "Policy Principles for AI, AR, VR, Robotics & Cloning - A Thought Paper"
- "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"

This paper focusses only on kids and how to protect them in a non-private world.

Legal Identity Framework for Kids

At Birth

Biometrics

When Jane Doe is born, she is uniquely identified by biometrics. Why use biometrics? With the advent of human cloning, every identity needs to be uniquely, legally, identified. Biometrics are the tool to do this.

In other papers, I've suggested the use of fingerprints and iris to do this, subject to research confirming they are enough to legally differentiate human clones. Later in the principles, under new age civil registration system, I also state biometrics should not be used which can profile people, e.g. DNA. Biometrics should be stored offline to mitigate the risk of the central database being successfully hacked.

One of the challenges in using biometrics is the ability for the biometric reader to be spoofed. Therefore, I recommend tight control over readers and administrators taking the biometric readings.

There will be cases where a child doesn't have fingers. Thus, use cases need to be created for this and alternate biometrics selected.

On a final note, the use of behavioral biometrics may, or may not, have a role to play in uniquely identifying a human, legally, in the future.

Please review the paper "I Know Who You Are & What You're Feeling – Achieving Privacy in a Non-Private World" pertaining to the need for new laws/regulations pertaining to use of them for behavior and biometrics.

Unique Digital Legal Identity

When Jane Doe is registered in the new age civil registration system, at birth, she receives a legal digital identity.

The premise is a legal digital identity must be built upon a legally defensible physical identity. Thus, the biometric identification come first at birth, or registration, immediately followed by a digital identity.

In other papers, I suggest the use of Sovrin/Blockchain for this. It puts control of the citizen's legal identity in their hands.

One of the drawbacks of Sovrin/Blockchain is it relies upon a private key. These are currently not hard to maliciously obtain. Thus, if Sovrin/Blockchain is to be used for the digital identity, and there are no developments increasing the security of the private key, it can only be used for low to medium trust scenarios.

The digital identity needs to have the ability to be delegated. Throughout this paper, I use examples where Jane Doe's identity requires delegation. The principles should drive the technology.

Therefore, whatever technology is selected to do digital identity, must be able to be delegable, and also work with user managed consent services. It is highly likely either modifications will need to be done to existing technology, like Sovrin/Blockchain etc., or other technologies created solving the problem.

For People Who Don't Have Technology

There is currently 45% of the planet's population without internet access. Until a global plan for this is created, a digital identity for Janes parents and Jane will be meaningless. In the paper "Where Shit Happens - Deploying AI, AR, VR, Robotics, Identity, Data & Consent in Challenging Parts of the Planet", I describe a possible solution.

My premise is a physical card of some sort must be issued on the spot by the birth registration worker. Jane's parents/legal guardians can use this when they travel to other villages where there is connectivity and/or government offices, first aid posts, etc. to identify themselves as well as to manage their identities and data consent.

The card must be tied biometrically/behavior data in some way to Jane's parents/legal guardians. It must mitigate the risk of malicious people masquerading as another, i.e. using Jane's identity to obtain funding, etc.

Further, the unit the registration worked carries for the card, must be able to work with similar conditions/requirements to those described above for the biometric/behavioral unit used to register Jane. It must be secure.

Parents/Legal Guardian Using the Digital Legal Identity to Verify Their Child

Jane Doe's parents/legal guardians are granted consent from the new age civil registration service to act on her behalf using her digital identity. This is complex. Why?

There are a number of use cases where the parent/legal guardian will want to grant limited identity management of the child's identity. These include:

- Divorced/separate/co-custodial relationships
- Schools
- Medical treatment
- Grandparents/family members looking after the child
- Etc.

Therefore, Jane Doe's parents/legal guardians need the ability to authorize others, in limited fashion, allowing them to use Jane Doe's legal identity in AI/AR/VR/physical realities.

Anonymous, Human Legal Identification

Jane's parents would be given a digital attestation, which they can delegate, showing the child is a human. It also identifies them anonymously, i.e. without showing the child's name.

As an example, Jane's grandparents are looking after her. She wants to play in an AI/AR/VR environment. Jane's parents/legal guardians would have given permission to the grandparents to use Jane's anonymous legal identification, showing she's a human. The grandparents would register Jane anonymously in the AI/AR/VR environment, giving Jane access.

As Jane enters the environment she would likely be given visual cues letting her know who is another child versus an AI generated person.

When Child Enters Their First Year of School

Additional Biometric Added to the Civil Registration

When Jane Does enters her first year of school, if the iris is selected to be used as one of the biometrics, her iris would be scanned and added to Jane's birth record. Why the iris?

Iris and fingerprints have very low Equal Error Rates (ERR). This is a measure of accuracy for the biometric. In a court of law fingerprints and iris are two of the best biometrics used to identify a person (also including DNA which isn't recommended for use due to its profiling ability).
There will be cases where a child doesn't have eyes. Thus, use cases need to be created for this and alternate biometrics selected.

Delegating Identity to the School

Jane's parents/legal guardians will use Jane's digital identity to register her in the school. They also can delegate use of Jane's identity and/or her anonymous legal identity to the school. Why?

In the future, schools will leverage AI/AR/VR/physical realities to teach with. Teachers and/or other students in the environment may be on site or remote. The school needs to register Jane as a participant, while protecting her identity, unless her parents/legal guardians consent to providing her full name.

Thus, hypothetically, Jane can participate in the environment as an anonymous person while showing she is a human and not a AI generated robot. If the parents/legal guardian consent to provide her name, she would appear in the environment as Jane Doe.

Legal Data Framework for Kids

No minor's data can be used without the consent of their parents/legal guardian. Thus, Jane Doe's identity, biometric, behavioral or other data cannot be used without consent from the parents/legal guardians.

Note: Readers should refer to the paper "I Know Who You Are & What You're Feeling – Achieving Privacy in a Non-Private World" for a detailed discussion of new data law requirements for behavior/biometrics.

Delegating Minor's Data Consent

Jane Doe's parents/legal guardians might want to be able to delegate their consent to a grandparent or someone else. Jane's grandparents are looking after her. Jane's parents assign a time limited ability to the grandparents to manage Jane's identity and her data. She falls ill. Her grandparents take her to the hospital for treatment. They delegate their consent to the hospital, enabling the hospital to use Jane Doe's medical data.

Delegating Minor's Data to the School, Hospitals, etc.

When Jane Doe enters her first year of school, Jane's parents/legal guardians will also grant consent for Jane's data to be collected, used, shared and stored. The same applies to healthcare. However, it's likely going to become complex. Why?

As AI/AR/VR/physical/robotic environments are created and used in education and healthcare, everything going on in these environments is recorded, each second. This can be good and potentially bad.

Good, because it will help teachers, health professionals, etc. to go back and diagnose learning/health challenges. It's potentially bad since the data can be mis-used as time passes. Thus, it requires laws/regulations specifying how the data is stored, security around the data, access rights, sharing/archive/audit/termination policies, etc. The parents/legal guardians need to give their informed consent before allowing Jane's data to be used.

Secure, Legal Chain of Data Custody

There must be a chain of custody for Jane Doe's data. Her parents/legal guardians must have the ability to assign their consent on behalf of Jane to her grandparents which:

- Verifies
  - The parents/legal guardians' identities
  - Grandparents' identities
- Specifies:
  - What data consent is being assigned
  - Any time limits for the consent to apply

Legal Consent Framework for Kids

Note: Readers should refer to the paper "Consent Principles in the New Age – Including Sex" for a detailed discussion of what a consent management legal framework is.

Managing Minor Consents

In the use cases given above, Jane Doe's parents assigned consent managing her identity and data ability to her grandparents. 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 and hospital, AS WELL AS displaying all consents given by these entities.

When Child Custody Changes

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 Child Reaches Legal Age

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.

Be Protected Against Bullying According to Laws/Regulations

Jane Doe is being bullied by John and Sally Smith in an AI/AR/VR/physical environment. Her identity should be anonymous, unless otherwise consented to by her parents/legal guardians or their assigned legal delegates. What can be done to deter this?

The actions taken in this environment, by all participants, including AI generated robots, against Jane will be recorded. The length of time for the recording depends on the replay laws assigned to it. Replay is discussed further in the 'Replay Section' of the paper "Policy Principles for AI, AR, VR, Robotics & Cloning - A Thought Paper".

The types of bullying behaviors in these environments, against minors, can hypothetically be monitored by AI software. The level of AI monitoring can be seen as an invasion of one's privacy. On the other hand, it could detect bullying.

My thoughts are for educational/health environments, some type of AI monitoring software should be used, with the consent of the participants and/or their parents/legal guardians. It's akin in the old days of having a bully on the school grounds, where a teacher monitors the school yard and apprehends the bully. Outside of these "controlled" environments, AI monitoring likely shouldn't be allowed unless otherwise prescribed by laws/ regulations.

Regardless, bullying experts need to participate in creating global principles. These should be applied to creating new laws/regulations pertaining to AI/AR/VR/physical environments

Now let's put this all together…

Minor Walking Down the Street

In the paper "Privacy Gone – AI, AR, VR, Robotics and Personal Data", I use the example of Jane Doe walking down the street with her friends as adults. The example uses zones of trust which Jane and her friends determine. Let's take the same example and use them as kids below legal age.

Jane and her friends, Erika, Neil and John are walking down a street. Each is wearing AR glasses/lenses, a wrist band communicator, and clothes with bio sensors in them. There are several possible hypothetical examples.

One could be jurisdictional laws forbade any processing of any minor's data until they reach a certain age. In this case, there would be no trust. Their devices would transmit information stating they are legal minors. By law, all people walking towards them wearing devices, enterprises and governments wouldn't be able to process the data identifying them.

Have Varying Degrees of Trust Approved by Their Parents/Legal Guardians

Jane Doe, a teenager, is walking down the street by some stores. As she grows older, she wants to be able to shop on her own, etc. This poses challenges in assigning levels of trust to her.

Do we assign the same levels of trust an adult could have and let Jane's parents/legal guardians approve the levels? Are their restrictions should apply to Jane because she's a minor? What is the possible granularity of restrictions available, e.g. stores, retail, etc.?

The principles need to be hammered out at a global level, with child data privacy experts. These should be used to guide the technology and new laws/regulations required.

For this example, let's assume the laws allow for parents/legal guardians to determine zones of trust and/or when the child reaches a certain age, give them some legal responsibility. Here's what might happen:

- 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 parent's/legal guardian's 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

All This Sounds Good but Requires Global Enforcement to Work

In many of my other papers, I've written all of the news laws and regulations won't be worth the paper and electrons used to create them, unless there is global enforcement of the laws and regulations. The example I use to illustrate this is the current 5% success rate in prosecuting cybercrime. Why so low? Jurisdictions. Entities conduct their crimes from other jurisdictions where it's hard, or impossible, to prosecute.

Now picture Jane Doe the chid, who's had something bad happen to her. The malicious people will likely be in one or more other jurisdictions on the planet. Jane will be legally screwed unless there are global laws with global enforcement, protecting her.

Summary - New Laws, New Tools, New Ways of Doing Things

The new identity, data and consent legal framework offers new tools to citizens, including children, their parents and/or legal guardians. It enables a person to have privacy in a non-private world.

As has been shown in the examples, Jane can be protected in this new age. However, implementing this requires a sea change on the planet to create new global laws pertaining to identity, data and consent. If you, as a reader, care about your kids, nieces, nephews, grandkids etc., then it's time you begin to educate others about why we need them.

We have a choice. We can simply watch the technological tsunami strike our shores, sweeping away our privacy with it, including those of our children. Or, we can work together to create the new legal dikes to guide the incoming technological waters. If we choose to do something, our kids won't need a super hero to protect them in the sea of life.

.

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."