Young Children’s Data Privacy Challenges in the Tsunami Age

Author: Guy Huntington, President, Huntington Ventures Ltd.
Date: Created July 2019/ Updated Feb 2020
# TABLE OF CONTENTS

**YOUNG CHILDREN’S DATA PRIVACY CHALLENGES IN THE TSUNAMI AGE**

Note to Reader: 4

Abstract 6

Databases on People & Children
- Personal Data is a Source for Marketing to a Pregnant Woman 7
- Commercial Databases on People and Children 8
- Example of How Data Makes Its Way into Commercial Databases 9

The Tsunami Age and Fetal Data 10

Consent Leads to Child Data Flow 11

Newborn Children – Challenges with Legal Identity
- Breeder Documents 12
- 1 Billion People Don’t Have a Legal Identity 12
- Physical and Digital Legal Digital Identities for Children 12
- Human Cloning 13
- We Need a Rethink of Legal Identity, Globally 14

Now the Child's Born and Registered - Nursery Child Data 15
- Who Can Use This Data? 15
- Home Assistant Monitoring Devices – “Virtual Assistants” 16
- What About the Child's Privacy When Using Virtual Assistants? 16

Toddlers to Preschool Aged Children
- Augmented and Virtual Reality for Young Children 17
- AR/VR/AI Uses in Education & Healthcare 18
- AR/VR Privacy Research 19
- AR/VR/AI Young Children Data 20
- Wearables for Young Children 20
- Robots in Preschool 20
- Robots for Kids at Home 21
- New Age Nursery/Preschool Child Data Privacy Policy Requirements 22

Pace of Change 23
- Unprecedented Change 23
- It Applies to Our Child Privacy Frameworks 24

How Do Existing Legal Frameworks Address This? 24
- European Union General Data Protection Plan (EU GDPR) 24
- US Children’s Online Privacy Protection Act (COPPA) 24
- The Problem is the Existing Legal Consent System is Broken 25

Merging of Offline and Online Worlds Creates New Legal Privacy Challenges 25
- Social Credit Monitoring 25
- Corporate Monitoring 26
Huntington Ventures Ltd.
The Business of Identity Management

| Patchwork Privacy Laws Planet Wide | 27 |
| Laws Need to be Enforced | 28 |

**New Legal Framework for Child Data Privacy**
- Data – We Should Own and Control It with Right to Erase It | 28
- Consent – Different Risk Assurance Levels and Zones of Trust | 29
  - Different Risks Require Different Types of Consent | 29
  - Zones of Trust | 30

**Summary** | 31

**About the Author** | 32
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
Huntington Ventures Ltd.
The Business of Identity Management

- 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 architecture principles summary
  - "New Age Architecture Principles Summary"

- Leveraging Blockchain and Sovrin

- 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.
Abstract
We are entering a technological tsunami wave of change. Caused by the combination of artificial intelligence (AI), augmented reality (AR), virtual reality (VR), robotics (both virtual and physical), nanotechnology and wireless, it's rapidly creating a "non-private world," The technology revolution extends from monitoring a women's periods, through to conception, pregnancy, birth, infancy and preschool.

The paper shows how the existing nation state laws protecting a young child’s data privacy are no longer sufficient. It does this by discussing:

- Existing large, global commercial databases being fed with child data, using a recent UK ICO fine to illustrate it
- Citing research showing up to 97% of people approving consent contracts without thoroughly reading them
- Existing child legal identification systems no longer meet the needs of today’s age
- Technology, such as fetal and infant monitoring, wearables, AR, VR and robotics, is affecting a child’s data privacy
- Creating a new age child privacy agreement for nurseries and preschools
- Logarithmic rate of technology change creating an unprecedented requirement to rethink our privacy laws
- EU General Data Protection Regulation (GDPR) and US Children's Online Privacy Protection Act consent laws
- Merging of Offline and Online Worlds Creates New Legal Privacy Challenges
- New legal framework for child data privacy including identity, data and consent with global enforcement
Databases on People & Children

Personal Data is a Source for Marketing to a Pregnant Woman
The 1984 paper “Life Status Changes and Changes in Consumer Preferences and Satisfaction,”\(^1\) researches lifestyle changes affecting what a person buys. “We have seen that the respondents who were undergoing life status change were more likely to be changing their brand preferences spontaneously, either as the result of direct effects of specific status changes or as the result of intervening changes in lifestyles.”

The use of this research then made its way into the marketing world.

The 2013 teaching case “Target: The Challenge of Data Mining” in *Journal of Critical Incidents*\(^2\), describes the story of a father going into a US Target store. He was complaining they were sending coupons for baby clothes and cribs coupons to his high school daughter, claiming she wasn’t pregnant. Later, he found out she was. Target knew before the parent. The use case states:

> “Gregg Steinhafel, Target's president, boasted to investors that "heightened focus on items and categories that appeal to specific guest segments such as mom and baby" (Target, 2012) were responsible for these successes. The segment focus relied heavily upon the ability to determine customer purchasing patterns through prior purchase behaviors and other demographic data. Target was one of the first major retailers to use predictive modeling (sophisticated data mining techniques) to identify customer segments and differentially market to those segments.”


Commercial Databases on People and Children
A Cracked Labs story from 2017, “Corporate Surveillance in Everyday Life,”³ provides a very detailed examination of commercial databases on people. It examines entities like Facebook, having over 50,000 attributes per person, through to large commercial databases like Acxiom and Oracle, containing thousands of attribute data on up to billions of people. These databases also include information on mothers and their infants.

As an example, in April of this year, The UK Information Commissioner’s Office (ICO) fined Bounty (UK) Limited, £400,000. Bounty was taking new mom’s and birth date, gender, addresses of infants, their names, pregnancy status, and sending millions of records to commercial databases.

“Bounty informed the Commissioner that during the period 1 June 2017 to 30 April 2018, based upon consent received during the member registration process, it shared a total of 35,027,373 personal data records with Acxiom (a marketing and profiling agency), Equifax (a credit reference agency), Indicia (a marketing agency) and Sky (a telecommunications company) for the purposes of direct electronic marketing. These organisations represented the four largest recipients out of a total of 39 organisations with which Bounty confirmed it shared personal data, with each record shared representing the personal data of an individual person. Whilst the data shared with each organisation varied slightly, in each case it comprised the majority, if not all of the data collected in respect of each individual.”⁴

³ https://crackedlabs.org/en/corporate-surveillance

Example of How Data Makes Its Way into Commercial Databases
When a woman is menstruating, she might use a variety of smartphone applications to track her periods. As women in the recent Guardian story found out, they didn’t understand who their period information was shared with. The reporter discusses how she answered a poll on an application about urinary tract infections (UTI). Two hours later, on Facebook, she views a personalized ad for treating UTI.

Her data flowed from the app to Facebook. Facebook and other companies acquire personal information from a variety of different vendors. Data could flow directly from the app provider to an entity like Facebook or, it could flow into a data broker, analyzed for behaviors, and auctioned in real time. In advertising, it’s called “programmatic advertising.” Companies, like Google, are leading experts in this area.

---

5 [https://www.womenshealthmag.com/health/g26787041/best-period-tracking-apps/](https://www.womenshealthmag.com/health/g26787041/best-period-tracking-apps/)


8 [https://www.thinkwithgoogle.com/marketing-resources/programmatic/](https://www.thinkwithgoogle.com/marketing-resources/programmatic/)
The Tsunami Age and Fetal Data
The 2014 paper “An Emerging Model of Maternity Care: Smartphone, Midwife, Doctor?”\(^9\) stated:

“The popularity of pregnancy-related apps could indicate a shift towards patient empowerment within maternity care provision. The traditional model of ‘shared maternity care’ needs to accommodate electronic devices into its functioning. Reliance on healthcare professionals may be reduced by the availability of interactive and personalised information delivered via a smartphone. This combined with the fact that smartphones are widely used by many women of childbearing age, is modifying maternity care and experiences of pregnancy. In this way, smartphones have the potential to take over some aspects of maternity care from healthcare professionals. Therefore it is important that healthcare professionals and policy-makers are aware of smartphones, apps and the way that they are influencing healthcare and altering health-seeking behaviour. In addition, there needs to be discussions around the need for regulation of information in ‘medical apps’ and the concern about misinformation and the role of the health professional.”

Fast forward to today, where there’s a wide variety of smartphone pregnancy apps a pregnant woman can select.\(^10\) She can also use an application service in conjunction with her medical provider\(^11\)

Meanwhile, monitoring technology is rapidly improving. As a result, an expecting mother today can buy technology to monitor her baby’s ECG and mobility as early as week 20.\(^12\)

---


\(^10\) https://www.healthline.com/health/best-pregnancy-apps#baby2body

\(^11\) https://getbabyscripts.com/

Consent Leads to Child Data Flow

When a pregnant woman provides her consent to the service, she likely doesn’t read the fine print. The study “The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services”\(^\text{13}\) states:

“Results reveal 74% skipped PP, selecting the ‘quick join’ clickwrap. Average adult reading speed (250-280 words per minute), suggests PP should have taken 29-32 minutes and TOS 15-17 minutes to read. For those that didn’t select the clickwrap, average PP reading time was 73 seconds. All participants were presented the TOS and had an average reading time of 51 seconds. Most participants agreed to the policies, 97% to PP and 93% to TOS, with decliners reading PP 30 seconds longer and TOS 90 seconds longer.”

It's confirmed by a Deloitte Survey “2017 Global Mobile Consumer Survey: US edition. The dawn of the next era in mobile.”\(^\text{14}\) stating:

“Consumers continue to express concerns about security and privacy captured in the data regarding the risks they perceive with IoT, mPayments, and autonomous vehicles. That said, consumers have been more open to signing agreements with mobile app and service providers—91 percent willingly accept legal terms and conditions without reading them before installing apps, registering Wi-Fi hotspots, accepting updates, and signing on to online services such as video streaming. For ages 18 to 34, the rate of acceptance of terms and conditions, without reading them, reaches 97 percent.”

Thus, if the pregnant mom gives consent, the data could make its way from the service to a commercial database. Data like the baby’s continuous ECG, could now be stored against the mother’s data.

This type of data, once only stored in health records, now exists in commercial databases, with the consent of the parent. Enterprises in the future will take advantage of it, using it to measure a person’s health, from before they were born to present, to then evaluate a person.

Was the mother aware of this when she gave her consent for the monitoring data to be shared? Did she consider possible long-term data privacy effects on her child?

---


Newborn Children – Challenges with Legal Identity
For the last few hundred years, governments around the world have evolved a system to legally register children's identities. In each local jurisdiction, the civil registration service registers a birth. It then uses technology from hundreds of years ago, i.e., paper, to produce a document verifying the child is who they claim to be. The birth certificate is a foundational legal document. With this, a person can then obtain other identity documents like driver's licenses, passports, etc.

The technological tsunami wave is causing four problems with the old child identity system:

- Breeder documents
- 1 billion people don’t have a legal identity
- Legal digital identities for children
- Human cloning

Breeder Documents
Technological improvements mean birth certificates are easy to fraudulently produce In security circles, it's called a "breeder document". Different countries have different strategies to begin addressing this, like the EU Origins project. As yet, there is no global standard for addressing it.

1 Billion People Don’t Have a Legal Identity
The World Bank estimates 1 billion people don’t have legal identities. Thus, these people are trapped from entering the modern world.

Physical and Digital Legal Digital Identities for Children
As the world digitizes, the need for children to have legal digital identities arises. One of the first countries to address digital identities for citizens, in general, was Estonia. In 1999, they created the “Identity Documents Act.” It states:

“5. Identity document requirement for Estonian citizens
   (1) An Estonian citizen staying (residing) permanently in Estonia shall hold an identity card.
   (2) An Estonian citizen specified in subsection (1) of this section who is under 15 years of age need not hold an identity card.”

---

16 http://www.origins-project.eu/
At this age, citizens must provide biometrics. Banks and other commercial entities trust the identity legally since the identity is biometrically verified via the government. In turn, the Estonia government issues a digital identity to the citizen, built on top of the biometrically trusted physical identity.

However, regarding children, there is no global standard for granting a child, from birth, a legal digital identity.

**Human Cloning**

Science and industry have rapidly moved from Dolly the Sheep, the first mammal cloned in 1996.¹⁹ Fast forward to today in China, where Boyalife currently clones 100,000 cows a year working towards 1 million.²⁰

Not all countries signed the United Nations Declaration on Human Cloning in 2005.²¹ Since then, CRISPR technology²² has evolved quickly. In 2015, Boyalife’s CEO publicly stated they could clone humans but weren’t.²³ Thus, the era of human cloning is now almost upon us. Any new civil registration system needs to be able to differentiate human clones.

---


We Need a Rethink of Legal Identity, Globally

The paper “Why the New Age Requires Rethinking Civil Registration Systems,”24 lays out the requirements for a new age physical/digital identity. In summary, it requires:

- Research to confirm:
  - The use of baby fingerprints as a unique legal identifier
    - Research on the use of baby fingerprints done by Dr. Anil Jain, Michigan State University25, and also at University of California San Diego26.
  - If fingerprints and iris biometrics are sufficient to differentiate human clones

- Assuming the research confirms this, then:
  - At birth, a child’s fingerprints would be obtained to register the identity
    - If the child doesn’t have fingers, then another biometric will be used
    - The child's parents' biometrics will also be collected, confirming their identities, and then their identity registration linked to the baby’s birth registration
  - During the first year of school, a child’s iris scan would be collected and then used as the second biometric for legally identifying the child

- Issuance at time of registration of two different types of legal digital identity
  - Legal full digital identity, and
  - Legal anonymous identity proving the person is a legal minor, and also a human
  - Both must have the ability to be delegated
  - The paper provides examples of both types of legal digital identities

---

24 https://www.hvl.net/pdf/Why%20The%20New%20Age%20Requires%20Rethinking%20Civil%20Registration%20Systems%20April%202019.pdf


26 https://health.ucsd.edu/news/releases/Pages/2018-09-12-researchers-develop-biometric-tool-for-newborn-fingerprinting.aspx
Now the Child’s Born and Registered - Nursery Child Data
Research papers on newborn wearables like “Wearable Sensor Systems for Infants” in 2015, and “The emerging market of smartphone-integrated infant physiologic monitors,” in 2017, have documented a growing marketplace for newborn wearables. Typically, they’re connected to smartphones, monitoring the baby, including the baby’s body position, breathing, skin temperature, and wake/sleep time.

Couple this with baby monitors. Today, a wide assortment of choices exists for parents, including audio and video. Research on low-cost infant monitoring for developing countries is also being done.

Who Can Use This Data?
Each second, wearables and monitors generate biometric/behavioral data. With very few parents reading the consent agreement, it’s likely the child’s data can be shared with multiple commercial databases.

Legal lines blur between what was once thought to be Jane Doe’s health records kept by her medical providers, and those of commercial databases. Since the parents gave their consent, are commercial databases able to use the data as they see fit?

27 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4367382/

28 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5310844/

29 https://www.wearable-technologies.com/2018/10/5-wearables-for-newborns-that-will-keep-you-stress-free-all-day-and-all-night-long/

30 https://www.pcmag.com/roundup/325834/the-best-baby-monitors

Home Assistant Monitoring Devices – “Virtual Assistants”
Today, many homes use virtual assistant technology.\textsuperscript{32} These devices record sound and conversations within the home. Thus, as the baby grows and begins to speak, their discussions will be captured by the devices. Data flows to the service provider’s cloud-based network and databases. There, the behavioral patterns are continually analyzed, stored, and used to market goods/services to the customer.

Research on how kids use this technology is emerging. In the UK, Childwise report in 2018\textsuperscript{33}:

“\textbf{The data shows that 42\% of children aged 9 to 16 access voice recognition gadgets at home - 36\% access Apple’s Siri, 20\% access Microsoft’s Cortana, 15\% access Amazon’s Alexa at home and 7\% access Google Assistant.”}

What About the Child’s Privacy When Using Virtual Assistants?
Given the growing widespread adoption of virtual home assistants, with the parents’ consent, all conversations in the home are now being analyzed, each second, for behavioral patterns. The data may, or may not be sold and used by other third parties. What are the short and long-term implications of this to a child’s data privacy?

\textsuperscript{32} \url{https://en.wikipedia.org/wiki/Virtual_assistant}
\textsuperscript{33} \url{http://www.childwise.co.uk/uploads/3/1/6/5/31656353/childwise_press_release_-_vr_2018.pdf}
Toddlers to Preschool Aged Children

Augmented and Virtual Reality for Young Children

Consider the arrival of virtual reality (VR) devices for kids in the home. Another Childwise study from 2018\(^\text{34}\) states:

“Children are taking to virtual reality with 25% having mobile VR equipment at home, 11% with Playstation VR, 10% have Oculus Rift and 6% have HTC Vive”

The price ranges of VR go from cheap cardboard glasses to expensive headsets.\(^\text{35}\) Augmented reality (AR) is also beginning to enter the home for kids.\(^\text{36}\)

Research is just emerging about the technology effects on children. The MIT Media Lab published in 2017 “‘Hey Google is it OK if I eat you?’- Initial Explorations in Child-Agent Interaction.”\(^\text{37}\)

In it they note:

“This research raises the following question: if these agents are becoming embedded in our lives, how could they influence children’s perception of intelligence and the way they make sense of the world?”

In the 2018 paper “Virtual Reality 101: What You Need to Know About Kids and VR,”\(^\text{38}\) it states 11 percent of parents reported their 8- to 17-year-olds experienced dizziness, 10 percent experienced a headache and 13 percent bumped into something.


\(^{35}\) [https://www.fatherly.com/gear/best-vr-headsets-for-the-whole-family/](https://www.fatherly.com/gear/best-vr-headsets-for-the-whole-family/)


\(^{38}\) [https://www.commonsensemedia.org/research/virtual-reality-101](https://www.commonsensemedia.org/research/virtual-reality-101)
In the 2015 article “The Dark Side of Video Games”39, ASU researcher, Katina Michael, explains about the addictive behavior of video games. She states:

“The next time you walk past your child’s door (whether he or she is a teenager or an adult living in your home), why don’t you spend ten full minutes together looking at how he or she is interacting with the virtual world through the computer device. In addition, ask about the music your child listens to and the movies he or she gets a buzz from. It is all one and the same: lyrics (auditory), multimedia (visual), consoles (touch and feel) enveloping the faculties of the human body. Immersing oneself in a whole lot of bad stuff is like immersing oneself in a cesspool. The problem with our life today is that we are swimming in the cesspool, surrounded by soft e-waste, and cannot see it for what it is. It is enveloping us on all sides and suffocating our freedom. We can only see things more clearly if we decide to get out of it, wash afresh, and then look with open eyes at what is before us. Yes, this does mean limiting our screen time.”

In only a few years, AR/VR technology has developed to leverage, second by second, behavioral/biometric technology, finely tuning the experience to the person. Then consider the dropping age profile of children who now have access to the technology. What are the short, mid and long term causes to the children?

**AR/VR/AI Uses in Education & Healthcare**

The paper “New Technologies and Autism: Can Augmented Reality (AR) increase the Motivations in Children with Autism?”40 documents 14 different research papers on the use of AR for autism. Companies, life Brain Power41, are working with Google Glass to deploy AR glasses for autistic/ADHD children.

Other research on the effects in healthcare, includes this example “Effect of virtual reality headset for pediatric fear and pain distraction during immunization.”42


AR/VR Privacy Research
In 2016, two German philosophers published “Real Virtuality: A Code of Ethical Conduct. Recommendations for Good Scientific Practice and the Consumers of VR-Technology.”\(^{43}\) It was “to present a first list of ethical concerns that may arise from research and personal use of virtual reality and related technology, and to offer concrete recommendations for minimizing those risks.”

The paper states:
“By tracking the details of one’s movements in VR, including eye movements, involuntary facial gestures, and other indicators of what researchers call low level intentions or “motor intentions” (Riva et al., 2011), private agencies will be able to acquire details about one’s interests and preferences in completely new ways (Coyle and Thorson, 2001).”

“Commercials in VR could even feature images of the target audience himself or herself using the product. The use of big data to “nudge” users (“Big Nudging”) combined with VR could have long-lasting effects, perhaps producing changes in users’ mental mechanisms themselves.”

“Users ought to be made aware that there is evidence that advertising tactics using embodiment technology such as VR can have a powerful unconscious influence on behavior.”

“4. Privacy
a. Users ought to be made aware that there is evidence that advertising tactics using embodiment technology, such as VR, can have a powerful unconscious influence on behavior. For example, a combination of “Big Nudging” strategies (collecting big data for the purposes of nudging the general public) with VR technology could have long-lasting effects, which might also affect underlying mental mechanisms themselves.

b. Data protection: users ought to be made aware of new risks involving surveillance, such as reading out “motor intentions” or a “kinematic fingerprint” during avatar use.”

“The ability to toggle between VR, AR, and SR may create situations in which users are not able to maintain an understanding of when their informed consent to share information is in effect. Users should be repeatedly reminded within VR that they have given informed consent.”


As the technology deploys into the home, and if it involves multiple players outside the home, it’s likely that, via the technology, sexual abuse and harassment of children will occur. How will parents, industry and legal regulators respond to this?

**AR/VR/AI Young Children Data**
Assuming parents gave their permission to the VR/AR learning/game supplier, the rich behavioral/biometric data can make its way into commercial databases. For example, Facebook owns Oculus, the VR manufacturer. Are children’s parents even thinking about this when they click on approving consent for their child to use the technology? Do they know where their child’s data goes and how it’s used?

**Wearables for Young Children**
The marketplace is becoming flooded with wearables for young kids.46 The price points are dropping, while features increase. Today, a parent can easily use the technology to track their child, with some, like Weenect,47 offering augmented reality radar.48 If parents approve the consent without reading it, it’s possible this rich geolocational/biometric/behavioral data can flow into large commercial databases.

**Robots in Preschool**
In China, some preschools use robotics, each day, to analyze a child as they enter the preschool.49 “The robot uses cameras and an infrared thermometer to look for signs of possible disease, ranging from red eyes or a sore throat to blisters and fevers. It can reportedly carry out these smart health checks in just 3 seconds: far more rapidly than a human physician would be able to greet a patient, let alone check them over for everything from conjunctivitis to hand, foot, and mouth disease.”

---


AR and VR are now being deployed into classrooms. Research papers like “The Effectiveness of Using Augmented Reality Apps in Teaching the English Alphabet to Kindergarten Children: A Case Study in the State of Kuwait,”\(^5^0\) provide examples on the use of the technology.

**Robots for Kids at Home**

Later this year, a robot for kids will be released.\(^5^1\) “Little Sophia can walk, talk, sing, play games and, like her big sister, even tell jokes! She is a programmable, educational companion for kids, that will inspire children to learn about coding, AI, science, technology, engineering and maths through a safe, interactive, human-robot experience.” The robot can do facial tracking and recognition.

Thus, home robots become yet another biometric/behavioral data collection point about the child and other family members. Depending on the consent given by the parents to the robot, it might be able to share the data with commercial databases.

\(^5^0\) [https://www.researchgate.net/publication/311781884_The_Effectiveness_of_Using_Augmented_Reality_Apps_in_Teaching_the_English_Alphabet_to_Kindergarten_Children_A_Case_Study_in_the_State_of_Kuwait](https://www.researchgate.net/publication/311781884_The_Effectiveness_of_Using_Augmented_Reality_Apps_in_Teaching_the_English_Alphabet_to_Kindergarten_Children_A_Case_Study_in_the_State_of_Kuwait)

\(^5^1\) [https://www.hansonrobotics.com/little-sophia-2/](https://www.hansonrobotics.com/little-sophia-2/)
New Age Nursery/Preschool Child Data Privacy Policy Requirements

Nursery and preschools child data privacy agreements, need to address the following implementation into their environment:

- AR/VR/AI
- Kids coming to preschool with their wearables
- Robots (both physical and virtual)

To create a new age, child data privacy policy requires answering the following questions:

- If the child can virtually interact with other kids and/or teachers around the planet, how does this implement privacy agreements? How is the child’s identity protected?
- Did the preschool accept the use of wearables as part of the privacy consent agreement Jane’s parents signed?
- Do parents have to inform the preschool their child has wearables?
- Is the child’s wearable data shared in real time with the preschool?
- How is the child’s AI/AR/health data shared with others, especially concerning commercial databases?
- What can the preschool do with this data?
- Who can see and use the child’s data from wearables, AR, VR, robots or other listening devices?
- Does the device always record even when it’s not being worn?
- How is VR/AR harassment monitored and stopped?
- What’s the user identity security for the AR/VR devices?
- What kind of explicit material and language is used in the programs?
- How is the content controlled?
- How are other VR/AR users identified?
- Can a user be anonymous in the VR/AR environment?
- What kind of informed consent is initially required?
- Is the user reminded of informed consent during the session use?
- How is the child’s physical safety ensured during the use of the technology?
- What’s the preschool’s data retention policy from these technologies?
- Has thought been given to long-term commercial use of the child’s data?
- Are there any time limits, per session, for the child using the technology?

Given the above, new age preschool privacy agreements do the nursery, preschool and parents need to be created. **Rather than each nursery and preschool themselves creating legal child privacy agreements, it makes sense for educational associations to fund new age legal child privacy templates.**
Pace of Change
Noted technology guru, Pat Scannell\(^2\), has a graphic illustrating the rate of change:

He postulates the pace of technology change is now logarithmic, far exceeding our cognitive abilities to keep up with it.

Unprecedented Change
Shoshanna Zuboff, in her book "The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power,"\(^3\) discusses the unprecedented change caused by surveillance technologies. She uses her home being struck by lightning as an example.

When her house was struck by lightning, she smelled smoke. She ran around closing doors to limit the smoke damage. As she ran out the doors holding photos, she then watched her house burn down. As Shoshanna puts it, “I was blind to conditions that were unprecedented in my experience.”

\(^2\) https://www.linkedin.com/in/patscannell

\(^3\) https://www.amazon.com/Age-Surveillance-Capitalism-Future-Frontier/dp/1610395697
It Applies to Our Child Privacy Frameworks
We view our children's privacy by using our existing frameworks to gauge what's coming at us. Like Shoshana running around the house closing doors to limit smoke damage, only to watch it burn down, technology renders obsolete our old ways of doing things.

Children's data begins in the womb and is now potentially flowing, each second, into commercial databases. In the not so distant future, external monitors will also be able to identify children, determine their emotions, and predict their behavior without them, or their parents, even knowing about it. It's unprecedented.

How Do Existing Legal Frameworks Address This?
Two examples are provided:
- European Union
- United States of America

European Union General Data Protection Plan (EU GDPR)
Article 8 of the EU GDPR states that consent is required below the age of 16 and that “Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.”

It importantly paves the way regarding possible legal remedies for erasing a child's data in the future in Article 17 Right to erasure ('right to be forgotten'). It allows a person to request their data be removed from databases.

US Children's Online Privacy Protection Act (COPPA)
The US COPPA requires parental consent from the parents for children under the age of 13.

In 2012, COPPA was amended providing more extensive documentation on the type of data collected including “Definition of Personal Information”. It includes geolocation information, photos, videos, IP addresses, and similar items found on computers or mobile devices.

“The rules also present a data retention and deletion requirement, which would mandate that data that is obtained from children is only kept for the amount of time necessary to achieve the purpose that it was collected for. The rules would also add the requirement that operators ensure that any third parties to whom a child’s information is disclosed have reasonable procedures in place to protect the information.”

55 https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule
57 https://www.natlawreview.com/article/ftc-will-propose-broader-children-s-online-privacy-safeguards
The US government is considering updating COPPA with the provision of an erasure button.58

The Problem is the Existing Legal Consent System is Broken
The existing consent system is broken. If the vast majority of parents provide their consent without reading the legal contracts, then a child’s data can easily flow into commercial databases, without the parents:

- Knowing it or,
- Realizing how the data can be used

Merging of Offline and Online Worlds Creates New Legal Privacy Challenges
In the not so distant future, a parent and child walking down a street, without any technology, will be easily identified, their behavior determined and compared to other times they’ve walked down the same street. How?

Social Credit Monitoring
Today, in China, the government is deploying social credit systems (SCS).59 Using behavioral/biometric monitoring through, soon to be over 500 million CCTV cameras, they identify, analyze and immediately respond to a person walking down the street. Thus, the parent and child will be identified, and their behaviour observed. It’s illustrated by this BBC report “China: "the world's biggest camera surveillance network".60

However, there is not yet one national SCS system. Instead, it’s composed of a variety of local government, and commercial SCS systems. This recent research paper “China’s social credit systems and public opinion: Explaining high levels of approval,”61 documents a survey of China’s “Internet-connected population distributions regarding age, gender, and region.” The paper states:

“While previous studies point out that the emerging SCS is designed as “state surveillance infrastructure” and as a tool for social management (Hoffman, 2017; Liang et al., 2018), this article underscores that these purposes are not foremost in the minds of Chinese citizens. Based on a national survey representative for the Internet-connected population in China, the study shows that SCSs are already widely used in China with more than 80% of respondents using a commercial SCS and 7% of respondents reporting

58 https://www.markey.senate.gov/imo/media/doc/Leg%20text%20--Markey-Hawley%203.11.19%20FINAL.pdf

59 https://en.wikipedia.org/wiki/Social_Credit_System

60 https://www.youtube.com/watch?v=pNf4-d6fDoY

61 https://journals.sagepub.com/doi/full/10.1177/1461444819826402
participation in a local government SCS. The findings show very high levels of approval across respondent groups. Interestingly, strong supporters of SCSs are more likely to be older, have a higher income, male, more highly educated, and live in urban areas.”

It also states:

“Our findings plausibly also reflect China’s authoritarian political context in which the survey was conducted. Interviewees were conceivably less concerned that SCSs provide data for surveillance and social control purposes since many would assume that the Chinese security apparatus is able to access to any such information already (e.g. Interview 6, June 2018; Interview 7, June 2018; and Interview 8, June 2018). One interviewee summarizes this view as follows: All data is accessible to the CCP already. For instance, during the registration for primary school, people must provide detailed family information. So, I do not think that there is any point in worrying about the Party having access to data through the SCS, because it is inevitable that all data is accessible to the CCP. (Interview 7, June 2018)”

Corporate Monitoring
This paper has outlined the corporate behavioral surveillance systems deployed. Thus, in the not so distant future, a parent and child walking down a street, will be identified, their emotions determined, and their behavior predicted, without their consent. The paper “Privacy Gone – AI, AR, VR, Robotics and Personal Data,”62 documents the current state of the monitoring technologies.

62 https://www.hvl.net/pdf/Privacy%20Gone%20March%202019.pdf
**Patchwork Privacy Laws Planet Wide**

The Brookings article “Why Protecting Privacy is a Losing Game Today – and How to Change the Game”\(^{63}\) highlights, from a US perspective, the existing patchwork legal framework for managing privacy. It states:

“More and more data about each of us is being generated faster and faster from more and more devices, and we can’t keep up. It’s a losing game both for individuals and for our legal system. If we don’t change the rules of the game soon, it will turn into a losing game for our economy and society.”

“As more devices and sensors are deployed in the environments we pass through as we carry on our days, privacy will become impossible if we are deemed to have surrendered our privacy simply by going about the world or sharing it with any other person.”

“We don’t get asked for consent to the terms of surveillance cameras on the streets or “beacons” in stores that pick up cell phone identifiers, and house guests aren’t generally asked if they agree to homeowners’ smart speakers picking up their speech. At best, a sign may be posted somewhere announcing that these devices are in place. As devices and sensors increasingly are deployed throughout the environments we pass through, some after-the-fact access and control can play a role, but old-fashioned notice and choice become impossible.”

“Businesses are able by and large to set the terms on which they collect and share this data. This is not a “market resolution” that works.”

Citing the Consumer Privacy Bill of Rights, developed in the Obama administration, it states:

“The bill of rights articulated seven basic principles that should be legally enforceable by the Federal Trade Commission: individual control, transparency, respect for the context in which the data was obtained, access and accuracy, focused collection, security, and accountability. These broad principles are rooted in longstanding and globally-accepted “fair information practices principles.”

It then goes on to describe a US solution based on the principles. However, the unprecedented nature of the technological tsunami, requires global laws, similar in wording, in each jurisdiction. Why?

**Electrons instantly travel across jurisdictional borders. In the not so distant future, our virtual selves will be able to live, work and play in many different jurisdictions. The old way of having different laws, in each jurisdiction, now no longer works.**

---

\(^{63}\) [https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/]
Laws Need to be Enforced
Companies operating outside the jurisdictions, and/or malicious criminals, can obtain the data and not comply with consent or data laws. The current rate of successfully prosecuting cybercrime is only 5%. Given this, while nation-state laws exist or, are created, protecting a child's privacy, the problem is enforcing them globally.

For example, if a child wants to erase their data held on them in many different commercial databases globally, how will they be able to do it? Without enforcement of common laws, globally, the child’s privacy and their data can’t be protected.

New Legal Framework for Child Data Privacy
Beyond the earlier stated proposed new child identity laws, what are the other components?

Data – We Should Own and Control It with Right to Erase It
The paper “Legal Privacy Framework for the Tsunami Age,” outlines new proposed data principles:

- 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
- Premise 9 – A person should have the legal right to request eraser of their personal data from existing databases

More information about each premise is provided in the paper “Privacy Gone – AI, AR, VR, Robotics and Personal Data.”

---

66 https://www.hvl.net/pdf/LegalPrivacyFrameworkTsunamiAge.pdf
67 https://www.hvl.net/pdf/Privacy%20Gone%20March%202019.pdf
Consent – Different Risk Assurance Levels and Zones of Trust

The paper “Legal Privacy Framework for the Tsunami Age,”\(^{68}\) discusses components of a new legal consent framework. These include:

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

Different Risks Require Different Types of Consent

Consent for a child's data to be used is a much higher risk than other types of consent. Therefore, different consent processes should be used.

For example, Jane Doe’s parents, when agreeing to a wearable contract for Jane, should see screens saying something like:

- Do you agree that Jane Doe’s data can be shared outside the application?
- If so, do you agree the data can be shared with the following enterprises (listing them)?
- As stated by law, if you agree, then we are informing you your child’s data can be used to perform behavioral predicting of the child and then used by other parties to advertise to you, advise you or used to evaluate your child. Do you agree?
- As stated by law, you or the child can change this by requesting data be erased any time in the future

The identity verification and authentication assurance strengths used for the parents/legal guardians, should be higher than for other forms of consent. This ensures it’s them who are providing the consent.

\(^{68}\) [https://www.hvl.net/pdf/LegalPrivacyFrameworkTsunamiAge.pdf](https://www.hvl.net/pdf/LegalPrivacyFrameworkTsunamiAge.pdf)
Zones of Trust

The earlier referenced paper, “Legal Privacy Framework for the Tsunami Age” states the following:

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

The paper “Kids’ Privacy in a Non-Private World – Why Even Super Hero’s Won’t Work,”[^69] discusses creating various degrees of trust for a person walking down the street.

[^69]: [https://www.hvl.net/pdf/Kids%20Privacy%20in%20a%20Non-Private%20World%20April%202019.pdf](https://www.hvl.net/pdf/Kids%20Privacy%20in%20a%20Non-Private%20World%20April%202019.pdf)
Summary
The paper has highlighted the loss of privacy for a child from the fetal stage through to preschool. Parents willingly providing their consent for devices and applications used to monitor the fetus, young children, and preschoolers, without reading the consent agreements, nor understanding the data implications.

As the paper demonstrates, much information about young children is already likely flowing into large commercial databases. Governments too are quickly adopting the same technology and using it to identify not only people, but also predicting their behavior.

The existing patchwork of identity, data and consent laws won’t be able to cope with the incoming tsunami wave of change. Therefore, enforceable new laws for child identity, data, and consent are globally required. Without this, the tsunami wave of change will sweep aside old child data protection abilities.

The first step in addressing the unprecedented change, is recognizing the problems stated in this paper exist. Next, it requires global discussions on how to create new privacy standards and laws.

Meanwhile, parents, nurseries, and preschools should carefully read the fine print in legal consent agreements. They should answer the question in the child data policy section of this document, and carefully decide how to use the new emerging technology for their young children.
About the Author

Guy Huntington, is an old, very experienced identity architect. His past clients include Boeing, Capital One, and the Government of Alberta’s Digital Citizen Identity and Authentication project.

Over the past year, he’s written numerous papers on this, ranging from the bedroom to the boardroom.70

He consults globally on the incoming tsunami wave of change and can be reached at guy@hvl.net.

70 https://www.hvl.net/pdf/Who%20am%20I%20identity%20verification%20papers%20summary%20Mar%202019.pdf