Digital Twins/Virtual Selves, Identity, Security and Death – A Thought Paper

Author: Guy Huntington, President, Huntington Ventures Ltd.
Date: Created February 14, 2020 / Updated Feb 17,2020

Note: Thanks to Milena Martinato for sending me some information which led to writing this thought paper.

TABLE OF CONTENTS

Digital Twins/Virtual Selves, Identity, Security & Death – A Thought Paper

Executive Summary

There's a revolution unfolding on the planet – digital twins and virtual selves. Enabled by massive increases in computing power (quantum computing), machine/deep learning, and increasingly rich data per second (behavioral/biometric data), it's spawning a new age. The concept of using digital twins for manufacturing things, e.g. Industry 4.0, is now moving to create digital versions of ourselves. An example? The emergence of digital twins able to model our physical bodies (medical digital twins).

This thought paper will discuss other potential aspects of use of a digital twin (learning digital twin), virtual selves, and discuss what happens upon our death when our digital twin/virtual selves still exists.

The emergence of digital twins/virtual selves brings new requirements for the new age:

- Legal identity toolkit able to tie the legal physical person to the digital twin/virtual self
- Consent framework with knowledgeable consent tied to an e-consent legal framework
- Identity federation legal tech able to manage the federation contracts between the physical person and those it's granting rights to use the digital twin/virtual self
- Personal identity and access management system able to manage all the above on behalf of the physical person and their digital twin/virtual self
- End to end security framework for the digital twin/virtual self's identity, data and consent
- Legal laws, enforceable around the planet, addressing what happens to the digital twin/virtual self and associated data when the physical person dies

This is a thought paper aimed at industry, political and privacy leaders around the planet, raising identity, legal and ethical questions. It requires a new legal framework to answer them.

Introduction

Technological change as it applies to digital twins has been relatively recent. In 2002, Michael Grieves, first applied the concept of a digital twin in manufacturing. "Grieves proposed the digital twin as the conceptual model underlying product lifecycle management (PLM)".

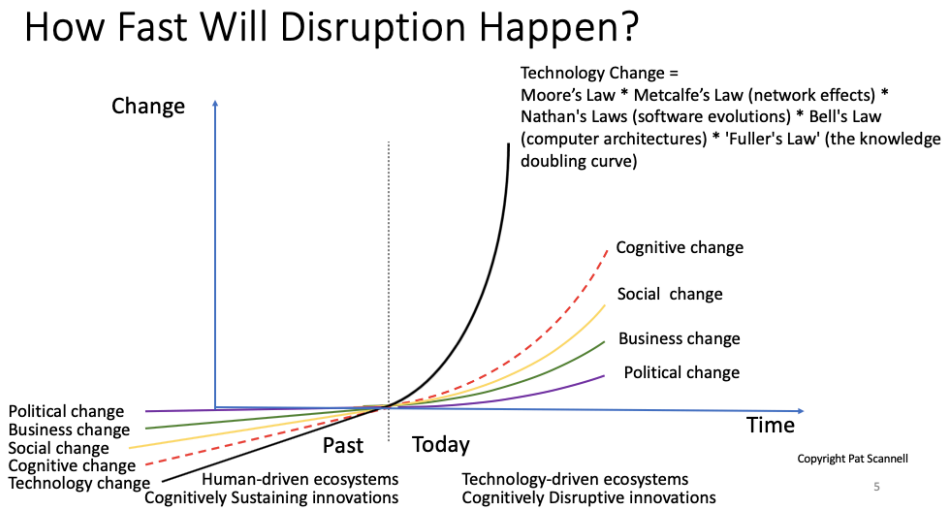
In 2011 at the Hannover Fair, the term Industry 4.0 was introduced. "The characteristics given for the German government's Industry 4.0 strategy are: the strong customization of products under the conditions of highly flexible (mass-) production.[14] The required automation technology is improved by the introduction of methods of self-optimization, self-configuration,[15] self-diagnosis, cognition and intelligent support of workers in their increasingly complex work." As part of this, digital twins began to become central to achieving industry 4.0.

With large scale computing power increasing, along with development of Internet of Things, big data, machine/deep learning, and growing interconnectivity, it enabled rapid development of digital twins. So much so, in February of last year, Gartner stated "75 Percent of Organizations Implementing IoT Already Use Digital Twins or Plan to Within a Year".

Medical digital twins are now just emerging.

Rapid Pace of Technological Change

All of the above are testament to the rapid rate of technological change. Consider the work of technology futurist Pat Scannell:



What Pat's saying is the rate of change is now becoming logarithmic. It exceeds our ability to cognitively keep up with it. I concur.

Artificial Intelligence (AI) Virtual Selves

Consider the rapidly emerging world of artificial intelligence (AI) "virtual selves". In 2018, a US company, Oben, worked with Chinese girl idol group SNH48, to produce the world's first commercially released song, co-starring human singers and their AI 3D avatars.

"To create digital clones of the singers, ObEN used photographs and voice recordings, with each singer required to read 100 to 200 sentences which were used as sample data for the AI algorithm. The result was a digital avatar that could sing like each group member and even speak multiple languages in their own voices, according to Adam Zheng, chief operating officer and co-founder of ObEN."

"To make a more precise digital copy, a 3D body scan would be needed but that was not done in the case of the SHN48 avatars."

So, while the Oben virtual selves aren't true digital twins, using industry definitions, they're a sign other, increasingly sophisticated, digital versions of ourselves are rapidly emerging.

AI/Augmented Reality (AR)

At the recent 2020 CES conference Norm Glasses won the innovation award. Why should you care? It's the rebirth of the what Google Glasses was trying to do. Watch this video. Now imagine a few years down the road where many people are wearing AI/AR glasses, or smart contact lenses. The result?

People will be able to interact with virtual selves/digital twins while walking around. It requires a mind shift from our old ideas about online and offline. Thus, you can be interacting with other people's virtual selves/digital twins or, AI generated ones or, hypothetically, even one or more digital twin/virtual selves' versions of yourself!

Education and Training

In 1993, an innovative paper was produced "Applications of Simulated Students: An Exploration". In it, the authors discussed:

"Teachers can practice the art of tutoring by having them teach a simulated student. Using a simulation instead of a real student allows teachers to see how their actions affect that student's knowledge, to undo their actions, and to try their skills on students with varying prior knowledge and learning strategies. Students can learn in collaboration with a simulated student. Because the simulated student can be simultaneously an expert and a co-learner, it can scaffold and guide the human's learning in subtle ways. Instructional developers can test their instruction on simulated students."

"Our main point is that cognitive simulation has come of age. Although there are still limitations that will take significant basic research to remove, simulation technology can and should be used to solve educational problems now."

Fast forward to today…

It's time to create a digital learning twin. The starting point for doing this is to assess a learner before any instruction or learning occurs. The assessment should include personality assessments, ability to work with others, hearing/visual/motor control abilities, aptitudes, etc. These are the beginnings of the data points for a learning digital twin.

The model should then be constantly updated on qualitative and quantitative assessments. As well, as biometric/behavioral data comes available, this too must be blended into the learning digital twin.

With this, learning/training specialists can then model different learning methods, per student, and determine the recommended approach. Over time, not over night, the learning digital twin should also be able to predict individual and group learning behavior. It will allow us to rethink training as well as what goes on in a classroom.

Note: I've begun reaching out to people around the planet to discuss this. If you're interested, please contact me.

Kids, Virtual Selves and Digital Twins

The Oben example earlier used, was about a teen pop group using virtual selves. Who will be one of the first age groups to adopt the use of virtual selves? Kids. Over the coming years, they'll also be using AI, AR, VR environments, with virtual selves, in classrooms. Couple this with the rise in the pornography industry of using virtual selves for sex. This creates new challenges:

- How is a child's legal age of consent determined?
- How can enterprises protect themselves from offering services to kids using virtual selves which portray them as being much older than they actually are?
- Who owns and controls a child's digital twin or virtual self?
- How can a child use virtual selves anonymously to protect their identity?
- Who owns and controls child data, such as behavioral/ biometrics, being increasingly used in AI, AR, VR environments?
- Most countries don't have a GDPR erasure law, allowing a person to request their data be erased from data systems, with children in mind. Given this, how will a child's data be protected in their later life when it involved digital twins or virtual selves?
- How will parents/legal guardians' consent be obtained electronically allowing enterprises like schools, healthcare services, etc. to then use and/or create digital twins or virtual selves?
- Can virtual selves be created with limited functionality to be used by kids? How will others know this?

Death

Watch this heart wrenching video of a South Korean woman interacting with her dead daughter via a virtual reality (VR) environment. This is a sample of what's coming at us. As the technology curve becomes logarithmic, many different enterprises will leap to use it, offering loved ones left behind, after a death, more advanced services.

It will likely start with companies obtaining, with the loved one's permission, data from videos, social media, etc. This will increasingly make the AI/AR/VR environment experience more and more "lifelike".

One can also see funeral homes et al, offering "packages" before a person dies. They can get people to wear devices producing biometric/behavior data for limited periods of time. The result? When they die, they live behind an increasingly realistic virtual self, able to interact with loved ones.

Yet There's More to Death…

A friend's close friend died 5 years ago. Their Facebook profile and pages still exist. People send message remembering the person on their birthday! This highlights the growing challenge of what happens to our digital footprint we leave behind.

Yet our digital footprint is now becoming much more than "data". It's becoming digital versions of ourselves, increasingly able to think for themselves.

The Thin Edge of the Rapidly Growing Identity Wedge

All of the above are only a few examples of the thin edge of the technological identity wedge appearing in our lives. The old way of looking at data as being online and us, offline, now no longer holds. Over time, not overnight, the intelligence of the digital versions of ourselves, be they virtual selves and/or digital twins, will result in very significant legal, ethical, social, business and political challenges.

Why? They'll be able to increasingly think for themselves. Further, they'll outlive us.

Crime and Digital Twins/Virtual Selves

The world isn't always a pretty place. Thus, malicious people will increasingly see new ways of obtaining control or visual/digital selves, masquerading as others, and making money at the expense of them, either alive or…dead! With the increasing digital footprint of a person, it offers up large pools of data by which malicious people can create false digital identities of people, both living and dead.

Fraud 4.0

I see this as being the beginning of what I call Fraud 4.0:

- **Fraud 1.0** existed a few hundred years ago to this day by obtaining identity pieces of paper and/or fraudulently producing them, using them to masquerade as another
- **Fraud 2.0** came into being when the internet arrived. It allowed others to obtain your username, ID's and pins to masquerade as you.
- **Fraud 3.0** has been developing the last 15 years, with the advent of social media and early AI. It allows bots to masquerade as people online.
- **Fraud 4.0** is in its early days. As increasingly sophisticated digital twins and virtual selves are created, it offers criminals the ability to actually act as the person digitally, looking like them, acting like them, and creating decisions that lend themselves to the criminal bank account.

Human Digital Twins//Virtual Selves Security - It All Begins with Identity

There is scant literature out about human digital twins and identity. In "Digital Twin", by Arup, it mentions identity:

"Identity and Authentication:
Identity is going to be at the heart of security for digital twins. We need to understand who is trying to access what, not just from the user perspective, but also in terms of who is sending us data. Authentication is a core part of identity: how do I know that the right device is sending the right data to inform the digital twin, or vice versa? Devices and users will need to authenticate in a secure way, and the whole concept of identity will therefore be central to digital twins."

My Premise

There must only be one physical human legal identity which is tied to one or more legal human digital identities. Every legal human digital identity must be tied to the singular human physical legal identity.

Human Physical Legal Identity

Ironically, while the planet madly digitizes, the challenge is we're relying upon old technology from the middle ages, paper, to legally create a human legal identity, i.e. a birth certificate. Today's jurisdictional civil registration vital stats systems (CRVS)'s doesn't have any common query protocol to check other CRVS's to see if the identity already exists, NOR are there data standards for CRVS's.

To address this, together with Michael Kleeman, co-founder Sprint and ex-Boston Consulting Group, we've written a proposal to rethink human legal physical identities. We want to rethink CRVS's planet wide as well as existing driver's licenses, both physical and digital, to enable a stronger identity verification.

The proposal would create:

- Self-sovereign legal identity both physically and digitally
- Ability to anonymously prove you're a human and if you're above or below age of consent
- Underlying legal human physical identity to tie human legal digital identities to

The proposal has a separate section devoted to creating a new form of physical and digital legal identity for kids, wards of state and those requiring power of attorney to manage their affairs. We see this as being a new legal building block required to address issues of kids, digital twins and virtual selves earlier raised in this thought paper.

Bots, Digital Twins and Virtual Selves Identities…

There are many new age challenges in creating digital human legal identities:

- There can be one or may digital human legal identities
- They can be created instantly in one jurisdiction, and in the next instant, be operating in another
- These new age digital human identities will be highly attractive to malicious people to obtain the identities, masquerade as the digital human to obtain valuable data or, to create replicas of the human digital identity and masquerade as them

Micheal Kleeman and I wrote a second bot legal identity proposal addressing the above. It calls out for a new civil registration vital stats (CRVS) bot service that's global but locally managed. The proposal would create:

- Common bot identity nomenclature/data standard which enterprises can use to describe bot identities within them and also share between enterprises
- Ability to discern a bot from a human
- A legal registration process for bots

The challenges are large. Yet, even if the proposal is successfully implemented it won't work. Why? The rapid rate of change depicted in the Pat Scannell diagram means today's best human and bot legal identity system might quickly become tomorrow's turd.

Global Human and Bot Legal Identity Test Institute

The bot proposal paper thus recommends creation of an independent human and bot legal identity test institute. Its job is to continuously test the governance, business processes, technological infrastructure and user interfaces for threats. We want the institute to then publish threat assessments using an agreed upon risk measure, with all jurisdictions responding accordingly.

Thus, a very low threat might take months or longer to fix, while a very high threat will be responded to within hours. We're bringing industry best practices to the world of legal human and bot identity. The planet's legal identity system relies upon this.

Rethink Data and Consent for Human Digital Twins/Virtual Selves

Having a new age legal identity framework for humans, bots, digital twins and virtual selves, enables a rethink of data and consent as described in this briefing document. It allows a person, e.g. Jane Doe, to have the ability, if she so chooses, to live privately in a non-private world or, with her consent, to then share her identity and personal data, using zones of consent.

To make this "magic" work requires the following:

- Creation of a personal identity and access management system a person can use as well as their digital twins/virtual selves
- Legal tech to manage the many identity federation contracts a person will likely enter into, since with their new self-sovereign legal identity they are their own identity provider
- Creation of zones of trust able to work planet wide

The document states the likely driver of this will be businesses. They'll want to have a level playing field to operate globally, across jurisdictions, leveraging identity technology for both humans and bots, including digital twins and virtual selves. It also states the place to begin is with large trading partnerships like the EU, NAFTA, Trans-pacific, etc.

Based on Risk, Apply Different Forms of Authentication for Digital Twins/Virtual Selves

In a recent presentation I gave in the Hague, in the appendix, there's an analogy for physical versus digital identities. Part of the way through this, I mention the use of stronger authentication based on risk. With the fast pace of technological change, I can foresee new types of authentication being developed for digital twins/virtual selves.

New Laws and Ethics Discussion Required

Laws

Today, virtual selves already exist. Medical digital twins are just emerging. In this respect, the technological train has already left the station. Thus, new laws are required addressing the following types of questions:

- How is the digital twin or virtual selves legally identified while the physical person is alive?
- What kind of consents should a physical person be required to give for their digital twin/virtual self to be used?
- Who owns and controls the digital twin/virtual self post death?
- What happens post death, to the digital twin and its use when no instruction has been given?
- What are the termination rights for a digital twin/virtual self?
- How should enterprises who are large collectors of private databases on people, with hundreds of thousands of attributes on a person, collected over their lifetime, be managed post death, i.e. erasure law post death similar to GDPR's erasure law?
- Who owns and controls data used to create and manage the digital twins/virtual selves?
- How will these laws be enforced across multiple jurisdictions?
    - As noted on page 44 of this paper, the current rate of successful prosecution of cybercrime is a paltry 5%. Why? Cross-jurisdictions.
    - Thus, while politicians in one jurisdiction may trumpet new laws they create to protect their citizens, it won't likely work across multiple jurisdictions
- How will new legal identity framework laws, notify social media et al, a person has legally died, and to remove the identity from their databases?
- How will legal minor's digital twins/virtual selves be legally handled during their life until adulthood, or post-death when they are a minor?

Ethics:

A rigorous ethics discussion should occur planet wide addressing these types of questions:

- What's appropriate use of a legal digital twin/virtual self
    - Before death?
    - After death?
- How will minors be protected from mis-use of their legal physical and digital twin/virtual selves' identities?
- What kind of counselling needs to be given to people interacting with a loved one digitally post death?

Summary

In a recent Hague presentation, I referenced noted Harvard professor Shoshana Zuboff, author of "The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power", describing how the incoming technological revolution renders us unable to see what's coming, since we're looking backwards to see forwards. She used a personal example of her house being struck by lightning causing a fire.

She rushed around picking up photos, closing doors to rooms to prevent smoke damage. As she exited the house, she watched her entire house burn down. "I was blind to conditions that were unprecedented in my experience".

That's us. Most people are so focused on the actual technology, be it digital twins, virtual selves, bots, etc. that we can't see the incoming wave of very, very significant change. We view this through the lenses of our old laws, our own jurisdictions and our own experiences. Like Shoshanna's fire, it's no longer working for us. It's why I created this thought paper.

I'm not a great seer, who can accurately predict what will happen tomorrow. However, I can see the general shape of the rapidly approaching tidal wave of technological change. With increasing computational computing power, i.e. quantum computing, coupled with machine/deep learning, 5G connectivity, nanotechnology et al, we're in the process of creating digital twins and virtual selves able to increasingly act like us, think like us, and do actions on our behalf.

They're not just "data". Instead, increasingly they're becoming "smarter". The effects of this will ripple through our physical lives. As importantly, they'll continue to exist, long after we're dead.

We need a new legal identity framework to create one physical legal identity per person, and then to legally tie digital twins/virtual selves' identities to it. It's not a trivial problem.

No one jurisdiction can solve this on their own. Jurisdictions won't like this. It requires creating a new global legal architecture, able to work across jurisdictions. However, I can see it being driven into place. Why? Increased costs to politicians, industry and citizens, by virtual selves et al masquerading as others, doing malicious things.

The rapid shape of Pat Scannell's hockey stick shaped technology curve is always in my head. It means that tomorrow is definitely going to be not like today. Therefore, time is of the essence.

Thanks for taking your time in reading this thought paper!

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.

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.