



The Sky Isn't Falling - But Security Models Must Change

Guy Huntington

President, Huntington Ventures Ltd.

March 8, 2022

ISSA Wisconsin

Note: Updated February 28, 2022





Who am I?

- I'm Guy Huntington
- My dear wife would call me an "old fart" always looking ahead
- I've led and rescued several large, global identity projects
- My past clients include Boeing, Capital One and the Gov't of Alberta's Digital Citizen Identity & Authentication project
- I'm on a mission to rethink both human and AI system/bots legal identities around the planet, and leverage this to then rethink learning

What Does This Deck Cover?

- **Change!**
- **The sky isn't falling, but the pace of change means enterprises MUST get their heads into a new risk space**
- So, I'm going to go very quickly through these slides depicting examples of change
- Next, I'm going to briefly discuss a new security model I've created at the 100,000 foot-level
- Then I'm going to briefly discuss small "baby steps" your enterprise can take to get from where we are today towards the "promised land"
- I especially want to have a long, free-wheeling, open discussion with you folks!

Overwhelming Message For Most People...

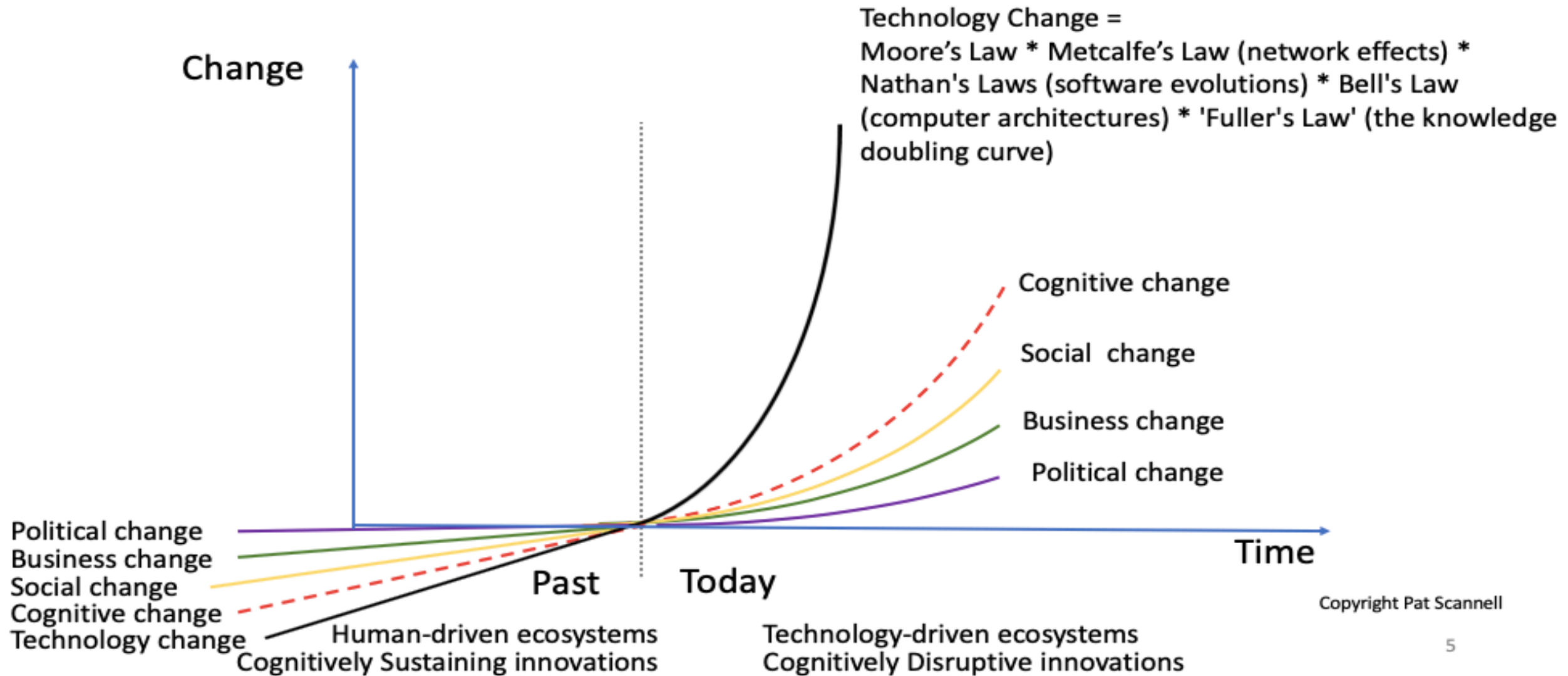
- The change this deck talks about is vast, since it comes at people and enterprises from all sorts of different directions (as you'll soon see)
- Many people I talk to are overwhelmed trying to take it all in
- **Thus, within the deck, I've included LOTS of reference links**
- I've also included a hefty appendix deck containing discussion on things like legal identity for humans/AI systems/bots, identity federation, human cloning, learning, et al, with LOTS of links
- So, you can go back, explore all the links, and digest it all as to what impact it has on your enterprise
- With this said, let's move onto some premises I have...



My Premise?

It starts with this curve....

How Fast Will Disruption Happen?



It Means...

- We can now no longer cognitively keep up with it
- While the curve generates new tools to use in creating new services and products...
- **Hypothetically, EACH HOUR, new attack vectors are being created against not only your enterprise's tech infrastructure, BUT ALSO AGAINST YOUR GOVERNANCE, BUSINESS PROCESSES AND USERS (BE THEY HUMAN OR BOTS)**



YIKES!!!!!!

- Is how in one word I sum it all up
- **A follow-on premise is that current IAM and security vendor solution sets also can't keep up with this pace of change**
- Further, the merging of the physical and virtual worlds is rapidly creating new types of attack vectors for which most enterprises aren't anywhere even remotely prepared
- Like what?



Malicious Molly

She walks into HR to do an assessment for a high-profile analyst type job

She does amazingly well on her assessment and is hired

Molly then gains regular access to the C-suite

So, what's wrong with this picture?



Malicious Molly

Wears AI/AR contact lenses and smart clothes leveraging an increasing plethora of smart IoT devices

The contact lenses transmitted the assessment to an AI system which immediately crafted the answers and displayed it back to Molly using her own writing style

It also read the biometrics and behavioral data from the people interviewing her and predicted their behavior

Malicious Molly

Molly uses the same tech in the C-suite to also record everything she saw in real time

Thus, the enterprise competitors or, well financed global criminal gangs, can leverage this to then design successful attacks against the enterprise

Malicious Molly

- Skim these articles to learn more:
- ["HR and the Technological Tsunami Age"](#)
- ["IT, Security & the Technological Tsunami Age"](#)
- ["Legal Departments, Digital Identities & Tsunami Age"](#)
- ["AI, Cheating & Future of Schools/Work"](#)
- [Skim this](#) to see AI/AR glasses vendors
- **My point? This is just the tip of the proverbial iceberg of change most enterprises won't see coming**



Jane Doe is Negotiating a High Value Contract

The vendors she's negotiating with seem to know her very well, anticipating her responses, with some very good counter points

What Jane doesn't know is they are leveraging AI, plus IoT devices, et al to take in, each second, her biometric and behavioral data, predict her emotions, and also create a running set of counterpoints



Jane Doe is
Negotiating a
High Value
Contract

Jane is effectively negotiating with
one arm tied behind her back

In the not-so-distant future, her neuro
data will also be used against her!

Yikes!!!!

Affectiva et al

- When I rent a car, there's a small dashboard camera pointing at me
- If I take my eyes off the road it flashes up a message to pay attention
- Car rental companies can also use this to prove road rage, et al
- This is but one small example, out of thousands, of behavioral tech quickly migrating into our world
- To learn more about Affectiva [skim this](#)

A Sensitive Manufacturing Process

- Acme Inc. has a sensitive manufacturing process protected by a combination of high physical and digital security
- Evil Inc., their competitor, or a malicious criminal gang, wants to gain access to the process
- They leverage increasingly small flying micro bots to enter the physical area
- These bots contain an increasing array of sensors, cameras, et al
- [Skim this article to learn more](#) about flying micro bots

A Sensitive Manufacturing Process

- Evil inc. also uses increasingly sophisticated digital bots as well physical ones to target sys admins
- They successfully attack Acme Inc's defenses, gaining access to the sensitive manufacturing process
- [Recall Solar Winds](#) where criminals gained access to sys admin accounts, gained access to digital signatures, and hacked into 17,000 enterprises

To Learn More About AI Systems and Bots...

- ["Why AI Regulation Requires Legal Identities of AI Systems and Bots"](#)
- ["Artificial Intelligence & Legal Identification - A Thought Paper"](#)
- ["Mission Control - We Have a Problem"](#)
- ["Lease or Rent a Bot! Rapidly Emerging Contract Law & Legal Identity Challenges"](#)
- ["The Infrastructure Behind Coordinating up to 3,000 bots in One Factory"](#)
- ["Nanobots & Legal Identity"](#)
- ["Micro Flying Bots & Legal Identity"](#)
- ["Microbots Able to Swim Through Your Body & Legal Identity"](#)
- ["Bots, Swarms, Risk & Legal Identity"](#)
- ["Nanobots, Microbots, Manufacturing, Risk, Legal Identity & Contracts"](#)

A Real-Life Example...

- Toyota halts operations at all Japan plants due to cyberattack
- A major parts supplier to Toyota was affected
- “Many of the roughly 400 tier 1 suppliers that Toyota deals with directly are connected to the automaker's kanban just-in-time production control system, which allowed the problems at Kojima Industries to spill over to Toyota”



My point?

- The increasing inter-connectedness of suppliers, manufacturers, distributors and end-users means any weak link can be exploited to disrupt it

AI/AR/VR Environments



These are sweeping into enterprises

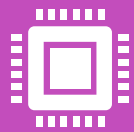


My dumb question to you folks is how can an enterprise and/or their employees/contactors know who's who in these environments, depending on risk, to high degrees of trust?

AI/AR/VR Environments



Answer - they can't



Today on the planet there is no legal identity framework for AI systems and bots, and no legal identity framework for humans, which works both physically and digitally, locally and globally

Metaverse Type Environments

- Skim these to learn more:
- ["Metaverse Bots?"](#)
- ["Lifelike Avatars, Risk & Legal Identity"](#)
- ["Metaverse, Identity, Data, Privacy, Consent & Security"](#)
- ["Challenges With Metaverse Contracts"](#)

Smart Digital Identities of Us

- AI versions of ourselves are rapidly emerging
- These are increasing “smart”
- So, it doesn’t take a brain surgeon to see over the next few years employees, contractors et al will be leveraging this
- **My dumb question to you folks is, depending on risk, how will say Jane Doe’s smart digital identity be legally tied to her underlying legal physical identity and be rapidly confirmed?**

Smart Digital Identities of Us

- Answer - today, on the planet, there isn't this framework
- Skim these articles to learn more:
- "**DIGITAL IDENTITY...**"
- "**Kids & Digital Identities**"
- "**Digital Twins/Virtual Selves, Identity, Security and Death - A Thought Paper**"

Add It All Up...

- Enterprise and personal risk rapidly increases, from moment to moment
- Over time, not over night, our old security models now will no longer work well
- **It requires a bottom up, second by second, risk assessment of many interlocking variables**
- Thus, I've created, at the 100,000-foot level a new security model...

Zones of Trust



It's Dynamic, Assessing Risk/Trust, Second by Second

- In this article, "[Smart Cities - Contracts, Privacy, Data & Legal Identities](#)", I discuss you walking down a street in the not-so-distant future wearing AI/AR glasses/contact lenses and smart clothes with IoT devices embedded within them
- **Thus, you're in the physical and virtual world at the same time**
- This is a mind shift most people haven't yet realized

It's Dynamic, Assessing Risk/Trust, Second by Second

- Around you there'll be:
- LOTS of increasingly smart IoT devices
- People walking towards you wearing the same tech
- **AND LOTS OF BOTS BOTH PHYSICAL AND DIGITAL**
- **This changes the risk game since all of this is what I call in my head, one whopper sized data capture, behavioral predicting environment about you**

It's Dynamic, Assessing Risk/Trust, Second by Second

- [Watch this video](#) and pay attention just after the 1:00 minute mark
- **All those people walking towards you and buildings you cycle by will easily be able to identify you, predict your behavior et al**
- **It throws into the dustbins of time our old ideas of privacy**

Two Premises...

- Each of us needs a new security/privacy model, tools and laws/regs giving us the option, if we choose, to live privately in a very non-private world
- **Enterprises MUST change their risk/trust frameworks to begin getting ready for this**
- **Putting it bluntly - it's damned hard to do today because we lack toolkits of tech, laws/regs and contracts to easily meet the challenges**

To Learn More About the Models...

- Skim these two articles:
- **"New Physical/Cybersecurity Security Model"**
- **"Smart Cities - Contracts, Privacy, Data & Legal Identities"**

Pushing the Vision "Stuff" Aside, What Are Baby Steps Your Enterprise Can Take Today?

POC and pilot the following:

Graph databases to begin replacing or supplementing your existing LDAP infrastructure

TODA to begin rethinking enterprise identity, authorization et al for both humans and AI systems/bots

Age of LDAP Is Ending

- LDAP was an excellent tool in its day to create a centralized hub within enterprises for identities
 - It became the heart of IAM systems which point and reside on top of it, with examples including Active Directory, et al
 - Yet it isn't right for our times – why?
 - It uses a tree structure which worked well when the number of identity relationships was small for a given identity
 - Today? There are fast changing identity relationships between humans, bots, IoT devices et al, with many to one, many to many relationships
 - LDAP isn't good at this
-

Enter Graph Databases

- They're exceeding good at quickly mapping fast changing, complex relationships
 - I have a good friend, Derek Small, CEO of [Nulli](#), who, for the last several years, have been pioneering the use of graph databases with IAM systems and IoT devices
 - They've successfully deployed this with several large companies around the planet
 - **So, my first free consulting advice is to get your enterprise rear end into gear, and begin to phase in graph systems to replace or supplement your existing LDAP architecture**
 - This is one of the key underlying foundational pieces you can then tie your new security models to
 - Let me know if you'd like a personal intro to Derek or, you can contact him yourself
-

Identity, Blockchain and TODA

I don't like Blockchain - why?

It's a shared public ledger AND ISN'T CONFIDENTIAL
WHICH LOTS OF IDENTITY REQUIRES

It deals horribly with the double spend by pooling data
and requiring third parties

It's an energy pig writing to "odds" of servers around the
planet

It's not instantaneous in its updates

**YET THIS IS THE CURRENT RAGE IN DECENTRALIZED
IDENTITY DISCUSSIONS!**



TODA

- I went looking for a better way to do this
- Two years ago, I was introduced to Toufi Saliba, global chair IEEE AI standards
- He and Dann Toliver wrestled with the blockchain problems I just described
- They came up with a much better mousetrap called TODA
- It leverages Merkle math, tries, cycles, et al to offer a much better, secure, confidential and exceedingly fast solution



TODA

Skim this to understand TODA - "**Legal Identity & TODA**"

TODA carries a TODA file which can be anything

When I saw this, I realized I was looking at a tool to rethink not only legal identity around the planet, but also enterprise identity architecture

The TODA file can be an export out of authoritative local government CRVS systems (birth, name/gender change, marriage/divorce, death registries)


It could also contain "capability files" which could become standardized authorization rights allowing an enterprise to effectively delegate portions of authorization



TODA - Enterprises



I realize how long it will take
for local state/provincial
jurisdictions to get a new
legal identity framework
implemented



So, about a year ago, I sat
down and wrote a series of
articles thinking my way
through this from an
enterprise's perspective...

TODA & Enterprises

- **"Part I - New Age Enterprise Identity Architecture"**
- **"Part II - Toda and LLC Incorporation"**
- **"Part III - Employee/Contractor Legal Identities"**
- **"Part IV - Toda Based Decentralized Enterprise Authentication and Authorization"**
- **"Part V - Rethinking Customer Identities Leveraging Toda"**
- **"Part VI - The Need for Quickly Creating AI System and Bots Legal Identities"**
- **"Part VII Rethinking Enterprise Identity- Summary"**

Is All This TODA "Stuff" Ready for Prime Time?

- **Honest answer – sort of**
- While there are many companies leveraging it to deal with transactions et al
- To the best of my knowledge, there are no companies leveraging it the way I outlined in the articles
- Thus, it requires enterprises who can see the opportunity and want to do POC's and pilots, experimenting with it
- Contact me if you're one of them!

Summary

- Skim "[The Times They Are A-Changin'](#)" - to see rapidly changing times
- You'll see the advent of [quantum computing on a chip, 2,300 physical commercial bot swarms, world's smallest commercial camera](#), et al
- My message to you and your C-suite is increasingly fast change is now on your doorstep
- You folks need to begin to change your risk models to address it
- It's also in your best interests to begin lobbying your local state politicians and CIO/CTO's they need to change their legal identity framework



My Favorite Quotes:

We cannot solve our problems with the same thinking we used when we created them” – Albert Einstein

“Change is hard at first, messy in the middle and gorgeous at the end.” – Robin Sharma

“Change is the law of life. And those who look only to the past or present are certain to miss the future” – John F. Kennedy



Thanks For Your Time!

- **Now let's discuss!!!!!!!!!!**

Appendices! (There's Lots Here!)

Note: Clicking on the box takes you to the subject

I - About me

II - An Identity Day in
the Life

III - Laws/Principles
of Identity

IV Biometrics

V- Fraud

VI - Legal Identity
Architecture for
Humans and AI
systems/bots

VII - Identity
Federation

VIII - Digital
Transformation

IX - Governments,
Legal Identity &
Human Cloning

X - Identity Death,
Laws & Processes

XI - Kids, Sex & Legal
Identities

XII - Rethinking
Learning & Schools

XIII- - Behavioral
Marketing

XIV - - Contract Law

XV - Insurers &
Digital Death

XVI - Health

XVII - EMP/HEMP
Proof Legal Identity
Data Centres

XVIII - 100,000 Foot
Level Summary
Human Legal
Identity

XIX - 100,000 Foot
Level Summary
Rethinking Learning

I - About Me!

- I'm an identity problem solver. My past clients include Boeing, Capital One and the Government of Alberta's Digital Citizen Identity & Authentication project
- I've spent the last six year working my way through creating a new legal identity architecture and leveraging this to then rethink learning.
- I've also done a lot in education as a volunteer over my lifetime. This included chairing my school district's technology committee in the 90's - which resulted in wiring most of the schools with optic fiber, behind building a technology leveraged school, and past president of Skills Canada BC and Skills Canada.
- I do short term consulting for Boards, C-suites and Governments, assisting them in readying themselves for LSSI (legal self-sovereign identity).
- I've written LOTS about the change coming. [Skim the over 100 LinkedIn articles I've written, or my webpages](#) with lots of papers.

II - An Identity Day In The Life

- I wanted to convey to people in a short story form about how the world we're entering is so different than the one I grew up in
- So, to see Jane Doe living her life skim this article:
- **"An Identity Day in the Life of Jane Doe"**

III - Laws/Principles of Identity

- Kim Cameron was an identity visionary in the 90's and 2000's, who created "Laws of Identity"
- He recently died
- As homage to him I revised them
- **I STRONGLY ADVISE ALL C-SUITE AND GOV'T POLICY MAKERS TO SKIM THIS:**
- **["Revised Laws of Identity"](#)**
- It should become the legal identity policy making guidelines

IV - Biometrics

- I hate the way we use biometrics today around the planet
- Skim this article to learn more:
- [**"I Hate How We Use Biometrics Today"**](#)
- Yet we love using them all over the planet!
- We need to change
- The legal architecture I'm proposing gives each of us control over our biometrics

V - Fraud

- The identity fraud industry today on the planet is simply staggering i.e., over a hundred billion dollars annually
- The success rate of prosecuting criminals is a paltry 5%
- Why because they operate out of jurisdictions where they can't be easily prosecuted

V - Fraud Reference Links

- ["Digital and Physical Identities - All That Glitters Is Not Gold"](#)
- ["Costs of a Crappy Legal Identity" -](#)
- ["Synthetic Identity Fraud - 1 Million Kids a Year"](#)
- ["AI, Mobile Wallets, Crime & Financial Stability"](#)
- ["Governments, Fraud & LSSI"](#)
- [Argentina's National ID Database Hacked](#)
- [Newfoundland's Health Database Hacked](#)

VI - Legal Identity Architecture for Humans and AI Systems/Bots

- Skim these two architecture docs:
- **Humans:**
 - **“Rethinking Human Legal Identity”** - <https://hvl.net/pdf/RethinkingHumanLegalIdentity.pdf>
- **AI Systems/Bots:**
 - **“Creating AI Systems/Bots Legal Identity Framework”** - <https://hvl.net/pdf/CreatingAISystemsBotsLegalIdentityFramework.pdf>

VI - Legal Identity Architecture for Humans and AI Systems/Bots - Costs

- **“Cost Centres - Rethinking Legal Identity & Learning Vision”** -
<https://hvl.net/pdf/CostCentresRethinkingLegalIdentityLearningVision.pdf>
- **Guesstimate Cost Notes Rethinking Legal Identity & Leveraging This to Rethink Learning (Word Doc)-**
<https://hvl.net/pdf/GuesstimateCostNotesLegalIdentityRethinkingLearning.docx>
- **Guesstimate Costs Rethinking Legal Identity & Leveraging This to Rethink Learning (Excel Spreadsheet) -**
<https://hvl.net/pdf/GuesstimateCostsLegalIdentityRethinkingLearning.xlsx>
- **My guesstimate? Somewhere between \$3.3-6.25 billion**

VII - Identity Federation - A Little History Story

- 20 years ago, at Boeing, the team I led did one of the planet's first deployments of identity federation. Boeing had a visionary architect, Mike Beach, who taught me lots about identity. He walked me into two large rooms in Seattle with about 100 people in each room doing call centre support, 24 hours a day, for Boeing's commercial airline customers.
- Mike explained to me that the vast majority of what they were doing was password resets. Let's say you were a mechanic for Southwest Airlines (the first company we federated with). In the hanger, you'd log on to Southwest Airlines systems and then click on one of the many Boeing links (let's say you fixed 737 planes). You'd be required to enter your Boeing userid and your password. You'd forget them and call one of the 200 people in the rooms Mike took me to.

VII - Identity Federation - A Little History Story

- Mike's vision was to leverage a new protocol developed by a committee he was on called "SAML" (Secure Assertion Markup Language). It established trust between parties. So, here's what would happen when Boeing deployed SAML.
- You'd log on to Southwest Airline's system and then click on the Boeing 737 link. In the blink of an eye, trust would be established between Southwest Airlines (the "identity provider") and Boeing (the "relying party"). A secure assertion would be sent from Southwest Airlines to Boeing, via SAML, containing your identity information, which planes you were authorized to fix etc. Boeing took this, and then mapped your identity to a very complex authorization grid. Up on your screen would show only what you're authorized for.
- Southwest Airlines was happy because you were now no longer sitting around waiting for Boeing to reset your password (i.e., you're more productive). Boeing was happy because they could severely reduce the call centre staff. They used the savings in the millions of dollars to fund all the additional work I created for them to rethink their global identity systems.

VII - Identity Federation - So What's The Problem?

- It took a year to roll out (long after I departed). Why?
- **Identity federation is first and foremost a legal agreement between the identity provider and the relying parties**
- Next, it's a complex set of business processes to deal with all the what ifs associated with identity and exchange of assertions between the parties, getting you off the systems promptly when you change jobs etc.
- Then it's a set of assertions the protocol dictates
- I've led other identity federation projects over the years. **MOST PEOPLE WITHIN ENTERPRISES ARE TOTALLY IGNORANT ABOUT THE LEGAL AND BUSINESS PROCESS "STUFF" ASSUMING THE PROTOCOL WILL SOMEHOW MAGICALLY WORK.**

VII - Identity Federation - Today It's Widely Used

- Since then, the identity federation world has changed.
- Today, billions of people use identify federation protocols each day leveraging their Google, Facebook or whomever accounts to log on to other sites (Google et al is the identity provider and the other sites are the relying parties)
- The protocols have changed to OpenID Connect, Oauth etc.

VII - Identity Federation - Now Come With Me Into The Future

- People want to be in more control of their data et al
- Which is why decentralized identifiers is such a hit topic
- Skim [Decentralized Identifiers \(DIDs\) v1.0](#)

VII - Identity Federation - Now Come With Me Into The Future Re DID's

- In the introduction to DID's (1. Introduction) it states:
- "As individuals and organizations, many of us use globally unique identifiers in a wide variety of contexts. They serve as communications addresses (telephone numbers, email addresses, usernames on social media), ID numbers (for passports, drivers licenses, tax IDs, health insurance), and product identifiers (serial numbers, barcodes, RFIDs). URIs (Uniform Resource Identifiers) are used for resources on the Web and each web page you view in a browser has a globally unique URL (Uniform Resource Locator).
- The vast majority of these globally unique identifiers are not under our control. They are issued by external authorities that decide who or what they refer to and when they can be revoked. They are useful only in certain contexts and recognized only by certain bodies not of our choosing. They might disappear or cease to be valid with the failure of an organization. They might unnecessarily reveal personal information. In many cases, they can be fraudulently replicated and asserted by a malicious third-party, which is more commonly known as "identity theft".

VII - Identity Federation - Now Come With Me Into The Future Re DID's

- The Decentralized Identifiers (DIDs) defined in this specification are a new type of globally unique identifier. They are designed to enable individuals and organizations to generate their own identifiers using systems they trust. These new identifiers enable entities to prove control over them by authenticating using cryptographic proofs such as digital signatures.
- Since the generation and assertion of Decentralized Identifiers is entity-controlled, each entity can have as many DIDs as necessary to maintain their desired separation of identities, personas, and interactions. The use of these identifiers can be scoped appropriately to different contexts. They support interactions with other people, institutions, or systems that require entities to identify themselves, or things they control, while providing control over how much personal or private data should be revealed, all without depending on a central authority to guarantee the continued existence of the identifier."

VII - Identity Federation - Yet Legal Identity Is Different

- It requires authoritative sources to issue the identity and/or your credentials. **This is different than DID's where the controller and verification are "optional"**
- **My goal in creating the architecture was to put each of us in control of this information, mostly outside the control of the initial generating authoritative source i.e., the government**
- So, by creating the SOLICT (Source of Legal Identity & Credential Database) and LSSI Devices (Legal Self-Sovereign Identity), we are now our own identity providers

VII - Identity Federation - Yet Legal Identity Is Different

- To see the ramifications of this, [go to the 1:00 minute mark of this video](#) and watch the next 15 seconds
- The lady is riding her bike down English Bay here in Vancouver where I live, wearing her AI/AR glasses (contact lenses are now just becoming available). As she looks around, she can see places for sale with their prices. What the video doesn't show is people walking towards her will be using the same tech to identify her!
- **Thus, since she's her own identity provider, she's going to have to create consent legal agreements, on the fly, allowing this. She's mostly not going to want to do this.**

VII - Identity Federation - Enter the PIAM

- This is your “Personal Identity Access Management” service
- It’s AI leveraged and you can present it to allow or deny identity federation requests on the fly
- To see how this might work in real life, skim this article:
- **“An Identity Day in the Life of Jane Doe”**

VII – Identity Federation – It Also Requires A SOLICIT

- The Source of Legal Identity & Credential Truth database, is where all your legal consent agreements will be stored leveraging a protocol called **Kantara UMA (User Managed Access)**.
- In the coming metaverse revolution we're entering, you'll likely create several or hundreds of consent legal agreements EACH DAY. Thus, you need a secure, historical record of them
- If you're lucky enough to live in the EU, you can then go back to a person/company/enterprise and ask for your data to be removed leveraging **Article 17 EU GDPR "Right to be forgotten"**

VIII - Digital Transformation

- While governments and companies tout “digital transformation” it’s not going to work well at the planetary level - why?
- The underlying legal identity framework for humans is badly broke and there isn’t a framework for legal identities of AI systems and bots
- Skim this article:
- **“Digital Transformation Requires Change to Our Old Ways of Doing Things”**

IX - Governments, Legal Identity & Human Cloning

- ["State/Provincial CIO/CTO's - A Major Problem Is Heading Your Way"](#)
- ["Governments & Physical/Digital Legal Identity for Humans and AI Systems/Bots"](#)
- ["Cradle to Adolescents & Legal Identity - Child Services, School and Sex"](#)
- ["Identity Delegation - It's Complicated"](#)
- ["Legal Identity & TODA"](#)
- ["Notaries, Digital Identities & New Age"](#)

IX - Governments, Legal Identity & Human Cloning

- **"Voting and Digital Identities"**
- **"What Legal CRVS Systems Should and Shouldn't Do"**
- **"Human Migration, Physical and Digital Legal Identity - A Thought Paper"**
- **"Legal Person: Humans, Clones, Virtual and Physical AI Robotics - New Privacy Principles"**
- **"Part II - Toda and LLC Incorporation"**

IX - Governments, Legal Identity & Human Cloning - A Story/History

- In 2005 I was thinking about how to mitigate the risk of fake birth certificates and a [sheep named Dolly](#), the first mammal cloned in 1996 - I was wondering when human clones came into existence how we'd legally differentiate them
- I contacted by email [Sir Alec Jeffreys](#), the person who invented the use of DNA for forensics
- We both agreed existing CRVS systems were antiquated and required use of biometrics to tie the person to their CRVS entry
- Alec told me that human clones would likely be identical twins and use of DNA wouldn't work differentiating them. He told me other biometrics like fingerprints and iris would likely be able to differentiate human clones
- However, in 2005 it wasn't thought possible to obtain infant fingerprints and iris scans were just coming into existence

IX - Governments, Legal Identity & Human Cloning - A Story/History

- Also in 2005, not all countries signed the [UN Cloning Declaration in 2005](#)
- In early 2006 I wrote my first paper, "[The Challenges With Identity Verification](#)"
- In it, I proposed the use of DNA as the biometric to be used in the CRVS database
- I took criticism from others who didn't like the idea of governments having a national DNA database with which they could profile people
- After reflection, I agreed with the critique and moved on with my business life

IX - Governments, Legal Identity & Human Cloning - A Story/History

- Fast forward to 2015
- In China, the CEO of Boyalife, a large Chinese cloning company working towards cloning 100,000 cows a year (now working towards 1 million), publicly stated they could clone humans but weren't
- At which point I realized the human cloning genie was out of the bottle and would become a reality

IX - Governments, Legal Identity & Human Cloning - Come With Me On A Journey

- If a countries clones humans and they stay within their borders, from a global legal identity perspective it's no big deal
- **HOWEVER, if they cross borders, suddenly it becomes a big deal**
- **IF THEY HAVE DIGITAL IDENTITIES WHICH CAN EASILY OPERATE IN ALL JURISDICTIONS AROUND THE PLANET, THEN IT'S A VERY BIG DEAL**

IX - Governments, Legal Identity & Human Cloning - A Dumb Question

- **So, my dumb question to governments, businesses, enterprises and people around the planet who will interact with human clones, is based on risk, how will they be legally identified?**
- **Good news - the architecture I've proposed addresses this i.e., it leverages fingerprints and biometrics to legally identify people**
- Skim page 53 of "[Cost Centres - Rethinking Legal Identity & Learning Vision](#)" where it proposes doing quick research to confirm that these biometrics do differentiate clones

X - Identity Death, Laws & Processes

- ["Death & Digital Identity"](#)
- ["Kids, Death & Digital Identities"](#)
- ["Digital Death & Metaverses"](#)

XI – Kids, Sex & Legal Identities

- **Here's my main points about kids:**
- From the moment they're born, they should have a legal physical identity
- And also at least one legal digital identity tied to the underlying physical legal identity
- The underlying physical identity **MUST** be biometrically tied to them
- **I.e., from birth on, they have the highest level of identity assurance**

XI – Kids, Sex & Legal Identities

- ["Kids & Digital Identities"](#)
- ["Kids – Rethinking Identity Assurance, i.e. Our Old Model is Dead"](#)
- ["Young Children's Data Privacy Challenges in the Tsunami Age"](#)
- ["Kids, Sex, Metaverses & Privacy"](#)
- ["Sex & Identity"](#)

XII - Rethinking Learning & Schools - Vision

- **"Vision: Learning Journey of Two Young Kids in a Remote Village"**
- **"Sir Ken Robinson - You Nailed It!"**

XII - Rethinking Learning & Schools - Architecture

- **"Learning Vision Flyover"**

XII - Rethinking Learning & Schools - Costs to Deploy

- **“Cost Centres - Rethinking Legal Identity & Learning Vision”**
- **Guesstimate Cost Notes Rethinking Legal Identity & Leveraging This to Rethink Learning (Word Doc)**
- **Guesstimate Costs Rethinking Legal Identity & Leveraging This to Rethink Learning (Excel Spreadsheet)**
- **Guesstimate Costs After Spending the Money to Deploy Human and AI System/Bot Legal Identity - \$2.3-3.6 Billion**

XII - Rethinking Learning & Schools – Schools Et AI

- **In many of the reference articles in this section I used this story:**
- John Doe, son of Jane Doe has learning challenges. When he was very young, his parents bought him a learning assistant bot, "AssistBot". They want him to take this to school
- In school, he takes an AI/AR/VR course taught by Sally Goodteacher, who can be located anywhere on the planet. She's assisted by two teaching assistant bots; PattyBot and BobBot
- John's fellow students might be located anywhere on the planet
- **To make this magic work requires a complete rethink of legal identity, credentials, privacy, consent and contract law**

XII - Rethinking Learning & Schools – Schools Et AI

- ["Bots, Classrooms, Privacy, Legal Identity & Contracts"](#)
- ["We Have An Identity Problem - AI/Bots in School, Home & Work"](#)
- ["Kids, Schools, AI/AR/VR, Legal Identities, Contracts and Privacy"](#)
- ["Kids, Digital Learning Twins, Neural Biometrics, Their Data, Privacy & Liabilities"](#)

XII - Rethinking Learning & Schools – Schools Et AI

- **"The Coming Classroom Revolution - Privacy & Internet of Things In A Classroom"**
- **"EdTech Law - Legal Identity Contracts"**
- **"AI, Cheating & Future of Schools/Work"**
- **"Using AI/Digital Learning Twins in Assessment & Education"**

XII - Rethinking Learning & Schools – Schools Et AI

- ["Bots, Classrooms, Privacy, Legal Identity & Contracts"](#)
- ["We Have An Identity Problem - AI/Bots in School, Home & Work"](#)
- ["Kids, Schools, AI/AR/VR, Legal Identities, Contracts and Privacy"](#)
- ["Kids, Digital Learning Twins, Neural Biometrics, Their Data, Privacy & Liabilities"](#)

XIII - Behavioral Marketing

- **"I Know Who You Are & What You're Feeling - Achieving Privacy in a Non-Private World"**
- **"Privacy Gone - AI, AR, VR, Robotics & Personal Data"**

XIV - Contract Law

- **"A Rapidly Growing Problem - Contract Law & Legal Identities"**
- **"Challenges With Metaverse Contracts"**

XV – Insurers & Digital Death

- **“Insurers Need a New Legal Toolkit”**
- **“Digital Identities, Risk, Insurance & Death”**

XVI - Health

- ["Covid, Health & Legal Identity - Leading from the Heart"](#)
- ["Digital Health Record & Legal Identity"](#)
- ["Health & Bots - A Personal Story"](#)

XVII - EMP/HEMP Proof Legal Identity Data Centres

- **"When Our Digital Legal Identity Trust Goes Poof!"**
- **"US Moves Towards Plan Addressing GMD and HEMP Events"**
- **"The Threat to Digitization"**

XVIII - 100,000 Foot Level Summary Human Legal Identity

- Each person when they're born has their legal identity data plus their forensic biometrics (fingerprints, and later when they can keep their eyes open - their iris) entered into a new age **CRVS system (Civil Registration Vital Statistics - birth, name/gender change, marriage/divorce and death registry)** with data standards
- The CRVS writes to an external database, per single person, the identity data plus their forensic biometrics called a **SOLICT "Source of Legal Identity & Credential Truth)**. The person now controls this
- As well, the CRVS also writes to the SOLICT legal identity relationships e.g. child/parent, cryptographically linking the SOLICTs. So Jane Doe and her son John will have cryptographic digitally signed links showing their parent/child. The same methodology can be used for power of attorney/person, executor of estate/deceased, etc.

XVIII - 100,000 Foot Level Summary Human Legal Identity

- The SOLICT in turn then pushes out the information to four different types of **LSSI Devices "Legal Self-Sovereign Identity"**; physical ID card, digital legal identity app, biometrically tied physical wristband containing identity information or a chip inserted into each person
- The person is now able, with their consent, to release legal identity information about themselves. This ranges from being able to legally, anonymously prove they're a human (and not a bot), above or below age of consent, Covid vaccinated, etc. It also means they can, at their discretion, release portions of their identity like gender, first name, legal name, address, etc.

XVIII - 100,000 Foot Level Summary Human Legal Identity

- **NOTE: All consents granted by the person are stored in their SOLICT**
- Consent management for each person will be managed by their **PIAM "Personal Identity Access Management"** system. This is AI leveraged, allowing the person, at their discretion, to automatically create consent legal agreements on the fly
- It works both locally and globally, physically and digitally anywhere on the planet
- AI systems/bots are also registered, where risk requires it, in the new age CRVS system
- Governance and continual threat assessment, is done by a new, global, independent, non-profit funded by a very small charge per CRVS event to a jurisdiction to a maximum yearly amount.

XIX - 100,000 Foot Level Summary Rethinking Learning

- When the learner is a toddler, with their parents' consent, they'll be assessed by a physical bot for their learning abilities. This will include sight, sound, hearing and smell, as well as hand-eye coordination, how they work or don't work with others, learning abilities, all leveraging biometric and behavioral data
- All consents given on behalf of the learner or, later in the learner's life by the learner themselves, are stored in the learner's **SOLICT "Source of Legal Identity & Credential Truth"**
- This is fed into a **DLT "Digital Learning Twin"**, which is created and legally bound to the learner
- The DLT produces its first **IEP "Individualized Education Plan"**, for the learner

XIX - 100,000 Foot Level Summary Rethinking Learning

- The parents take home with them a learning assistant bot to assist the learner, each day, in learning. The bot updates the DLT, which in turn continually refines the learner's IEP
- All learning data from the learner is stored in **their LDV "Learner Data Vault"**
- When the learner's first day of school comes, the parents prove the learner and their identities and legal relationship with the learner, via their **LSSI devices (Legal Self-Sovereign Identity)**
- With their consent, they approve how the learner's identity information will be used not only within the school, but also in AI/AR/VR learning environments
- As well, the parents give their consent for the learner's DLT, IEP and learning assistant bot to be used, via **their PIAM (Personal Identity Access Management)** and the learner's PIAM

XIX - 100,000 Foot Level Summary Rethinking Learning

- The schools **LMS “Learning Management System”** instantly takes the legal consent agreements, plus the learner’s identity and learning information, and integrates this with the school’s learning systems
- From the first day, each learner is delivered a customized learning program, continually updated by both human and AI system/bot learning specialists, as well as sensors, learning assessments, etc.
- **All learner data collected in the school, is stored in the learner’s LDV**
- If the learner enters any AI/AR/VR type learning environment, consent agreements are created instantly on the fly with the learner, school, school districts, learning specialists, etc.
- These specify how the learner will be identified, learning data use, storage, deletion, etc.

XIX - 100,000 Foot Level Summary Rethinking Learning

- If the learner enters any AI/AR/VR type learning environment, consent agreements are created instantly on the fly with the learner, school, school districts, learning specialists, etc.
- These specify how the learner will be identified, learning data use, storage, deletion, etc.
- When the learner acquires learning credentials, these are digitally signed by the authoritative learning authority, and written to the learner's SOLICT.
- The SOLICT in turn pushes these out to the learner's LSSI devices
- The learner is now in control of their learning credentials

XIX - 100,000 Foot Level Summary Rethinking Learning

- **When the learner graduates, they'll be able, with their consent, to offer use of their DLT, IEP and LDV to employers, post-secondary, etc. This significantly reduces time and costs to train or help the learner learn**
- The learner continually leverages their DLT/IEP/LDV until their die i.e., it's a lifelong learning system
- **IT'S TRANSFORMATIONAL OVER TIME, NOT OVERNIGHT**