"Artificial Intelligence & Legal Identification" – A Thought Paper

Author: Guy Huntington, President, Huntington Ventures Ltd.
Date: Created March 10, 2020

Author Note: Thanks to Michael Kleeman for assisting in editing this paper!

TABLE OF CONTENTS

Executive Summary

"AI is everywhere. It's not that big, scary thing in the future. AI is here with us."
- Fei-Fei Li

The planet requires an operational artificial intelligence (AI) governance system. It starts with legal identification of an AI system or bot. Without having a legal identity for AI, how will the following be handled?

- AI runs a corporation with no human shareholders
- AI does tasks with low, medium or high risk for financial and/or legal civil/criminal liability
- AI creates new ideas/concepts, products, etc.
- AI creates one or more virtual AI bots, each working "independently", having medium to high financial and/or legal civil/criminal liability
- AI creates one or more virtual AI bots, all working together in singularity, having medium to high financial and/or legal civil/criminal liability
- AI models a human person and acts on their behalf with medium to high financial and/or legal civil/criminal liability
- AI models a human person and masquerades as them

At the practical, implementation level, that's what this thought paper addresses. Each of the above use cases is examined, stating legal identification questions requiring answers.

The paper establishes what capabilities a new age AI legal identification framework must have. It describes the framework, referencing proposals for rethinking AI/bot and human legal identities.

Most importantly, the paper states "**However, until politicians want to change, it really doesn't matter what the papers recommend. It all comes down to politics."** Therefore, it analyzes politicians current political pain points:

- Getting elected and managing the discussions
- Business and AI pain points
- Citizen cybercrime and AI
- Immigration/migrants

For each one, it suggests political wins for the politicians both nationally and locally. By using the cover of national security, it suggest politicians can rapidly fund the changes to local jurisdictions, over two years, delivering a win for themselves, business and their voters.

It's our choice as to what we do with artificial intelligence. "It is not in the stars to hold our destiny but in ourselves." - William Shakespeare

Artificial Intelligence (AI)

Growth in 2020

Artificial Intelligence (AI) is rapidly growing. This Forbes' article states the following 10 AI trends for 2020:

1. AI will increasingly be monitoring and refining business processes
2. More and more personalization will take place in real-time
3. AI becomes increasingly useful as data becomes more accurate and available
4. More devices will run AI-powered technology
5. Human and AI cooperation increases
6. AI increasingly at the "edge"
7. AI increasingly used to create films, music, and games
8. AI will become ever more present in cybersecurity
9. More of us will interact with AI, maybe without even knowing it
10. But AI will recognize us, even if we don't recognize it

It Will Be Used to Attack Corporations, Governments and People

The recent paper by Cong Truong Thanh and Ivan Zelinka, "A Survey on Artificial Intelligence in Malware as Next-Generation Threats", discusses evolving AI intelligent evasion techniques, autonomous malware, AI against itself, and applying bio-inspired computation and swarm intelligence. (Note: swarm intelligence is discussed later in this thought paper)

The October 2019 Dark Reading article "Cybercrime: AI's Growing Threat", states:

> "Cybersecurity incidents expected to rise by nearly 70% and cost $5 trillion annually by 2024."
>
> "In one noteworthy recent example of a deepfake that generated headlines in The Wall Street Journal, criminals employed AI-based software to replicate a CEO's voice to command a cash transfer of €220,000 (approximately $243,000). Cybercrime experts called it a rare case of hacking that leveraged artificial intelligence.
>
> "In the cybersecurity world, the bad guys are picking up the pace. As a result, the corporate sector must pay attention to AI's potential as a first line of defense. Doing so is the only way to understand the threats and respond to the consequences of cybercrime."

Yet It's Much More Complicated Than This. Why? There's different levels of AI identification risk.

The World of AI, Risk and Identification

To illustrate the emerging legal identification challenges with AI, consider the following use cases:

- AI runs a corporation with no human shareholders
- AI does tasks with low, medium or high risk for financial and/or legal civil/criminal liability
- AI creates new ideas/concepts, products, etc.
- AI creates one or more virtual AI bots, each working "independently", having medium to high financial and/or legal civil/criminal liability
- AI creates one or more virtual AI bots, all working together in singularity, having medium to high financial and/or legal civil/criminal liability
- AI models a human person and acts on their behalf with medium to high financial and/or legal civil/criminal liability
- AI models a human person and masquerades as them

AI Runs A Corporation with No Human Shareholders

Five years ago, Shawn Bayern, a Florida State Law professor wrote "The Implications of Modern Business Entity Law for the Regulation of Autonomous Systems". In it, he states the following:

> "A quiet revolution is taking place in modern American organizational law. New forms of organizational entities, like limited liability companies (LLCs), resemble familiar business organizations, but they differ radically in largely unrecognized ways. This Article highlights one important implication of certain types of business entities under modern law: their ability to serve as legal "containers" for autonomous systems, such as computer programs or robots. Put simply, LLCs and possibly other modern business forms are flexible enough to permit a phenomenon that most commentators have traditionally considered impossible: effective legal status (or "legal personhood") for nonhuman agents without fundamental legal reform. Because of the unrecognized capabilities of modern entities, anything from a dog to a computer program, or from a 12-year-old child to a robot, can functionally participate in the legal system—buying and selling property, suing and being sued, and so forth."

In 2016, Shawn cowrote, together with law professors from universities in St. Gallen, Cambridge and Marburg, "Company Law and Autonomous Systems: A Blueprint for Lawyers, Entrepreneurs, and Regulators".

The paper states:

> "In particular, this prior work introduces the notion that an operating agreement or private entity constitution (such as a corporation's charter or a partnership's operating agreement) can adopt, as the acts of a legal entity, the state or actions of arbitrary physical systems. We call this the algorithm-agreement equivalence principle. Given this principle and the present capacities existing forms of legal entities, companies of various kinds can serve as a mechanism through which autonomous systems might engage with the legal system.
>
> This paper considers the implications of this possibility from a comparative and international perspective. Our goal is to suggest how, under U.S., German, Swiss and U.K. law, company law might furnish the functional and adaptive legal "housing" for an autonomous system — and, in turn, we aim to inform systems designers, regulators, and others who are interested in, encouraged by, or alarmed at the possibility that an autonomous system may "inhabit" a company and thereby gain some of the incidents of legal personality."

It concludes with:

> "We conclude with a further possibility of interest to both entrepreneurs and regulators: In today's interconnected world, an entity registered in one jurisdiction may qualify to "do business" in another. Thus, for example, a U.S. LLC might operate in Germany. It is unclear the extent to which jurisdictions will tolerate novel uses of existing foreign business forms. Mutual recognition of business forms across national legal systems would seem to assume familiarity with the forms — and with the functional purposes for which the forms are employed. Harnessing company law to house an autonomous system likely would attract challenges in the jurisdictions where it is attempted — and in other jurisdictions where it might have effects."

In summary, it's relatively easy to create an LLC in the US, with an AI autonomous system of some sort running it. Depending on the jurisdictions the LLC operates in, it may or may not be legally well received.

Some AI identification questions requiring answers:

- How will the AI system be legally identified?
- How will an AI autonomous system be restricted from creating yet more LLC's to then interact with?
- How will people, businesses, governments and other enterprises know they're dealing with a corporation where AI runs and controls it?
- How will the potential future issue of AI singularity be addressed, i.e. if one AI system is working in singularity with another AI system across different LLC's?

Financial/Legal Liability Risk Use Cases

I created three use cases to mentally work my way through AI identification requirements:

- AI does tasks with low financial and/or legal liability
- AI does tasks with medium financial and/or legal liability
- AI does tasks with high financial and/or legal liability

Before addressing the use cases, I want to reference an essay, "Legal Personhood for Artificial Intelligences", written in 1992 by law professor Lawrence Solum. In the essay he states:

> "The law currently has a mechanism for assigning liability in the case of a malfunctioning expert system: the manufacturer of the system may be held responsible for product liability. But could the AI itself be held liable? There is a way in which an Al might have the capacity to be liable in damages despite its lack of personal assets. The AI might purchase insurance. In fact, it might turn out that an Al could be insured for less than could a human trustee. If the AI could insure, at a reasonable cost, against the risk that it would be found liable for breaching the duty to exercise reasonable care, then functionally the AI would be able to assume both the duty and the corresponding liability.
>
> Some legal liabilities cannot be met by insurance, however. For example, insurance may not be available for the monetary liability that may be imposed for intentional wrongdoing by a trustee. Moreover, criminal liability can be nonmonetary. How could the Al be held responsible for the theft of trust assets? It cannot be jailed. This leads to a more general observation: although the AI that we are imagining could not be punished, all of the legal persons that are currently allowed to serve as trustees do have the capacity to be punished. Therefore, the lack of this capacity on the part of an AI might be thought to disqualify it from serving as a trustee.
>
> Answering this objection requires us to consider the reasons for which we punish. For example, if the purpose of punishment is deterrence, the objection could be put aside on the ground that the expert system we are imagining is simply incapable of stealing or embezzling. The fact that an AI could not steal or convert trust assets is surely not a reason to say that it is not competent to become a trustee. If anything, it is a reason why AIs should be preferred as trustees."

The essay is an excellent read on the issues of AI and legal personality, which this thought paper doesn't address. However, often when we think of AI, we are using our old school glasses to view it from, including liabilities, punishment and yes, even legal identity registration. What worked in the past, may or may not work in the future (which is the purpose of writing this thought paper).

Thus, in the following three use cases, I'm using financial and legal/criminal liability, as a means of gauging the risk from an AI system and then assessing the legal identity assurance required. How the liability is enforced is beyond the scope of this paper.

Low Risk

The AI system likely won't have to be legally identified. However, it's also likely that it might be identified via some method by its creator, (a corporation, a person or, another AI system). As well, enterprises might want to share information about the AI system within their enterprise or between enterprises.

Medium Risk to High Risk

The AI system will likely have to be legally identified. The AI system may or may not require authentication when interacting with people, enterprises or other AI systems. The level of authentication will likely vary depending on risk. If authentication is used, it must of be sufficient strength to assure the people, enterprises or other AI systems it's interacting with, that it's AI 12345 and not AI abcde.

Some AI identification questions requiring answers:

- What common nomenclature can be created allowing for AI systems to be described and identified within and between enterprises?
- How will AI systems be legally identified?
- What happens to the legal identity registration when an AI system cease to exist and how is the registration system notified?
- Since AI systems are global in nature, how will the AI legal registration system function globally and locally?

AI Creates New Ideas/Concepts/Products, etc.

What was once thought of as science fiction is now here. AI is increasingly able to invent new product/services on its own. Examples include:

- "AI creates new flu vaccine, all on its own"
- "AI can write just like me. Brace for the robot apocalypse"
- "Two AI-led inventions poke at future of patent law"

However, can AI think for itself? Today, the answer is no. In this Forbes article, "Can Artificial Intelligence "Think"?" it states:

> "Returning to the original question about artificial intelligence and thinking, I think we can solidly conclude that these systems don't do thinking at all. If we only have fast and automatic (System 1) artificial intelligence to work with, can we think of an AI model as a gifted employee that thinks differently about the world? Well, no. AI will probably cheat if the training is unmanaged, and so it is a lazy, deceptive employee. It will use the easy way out to get the highest score on every test, even if the approach is silly or wrong.
>
> As we try and build a "System 2" that thinks more like us, we need to remember that thinking is not about passing a test. Instead consider this quote:
>
> The test will last your entire life, and it will be comprised of the millions of decisions that, when taken together, will make your life yours. And everything, everything, will be on it. "

So, given all of the above, its highly likely AI systems developing products or services, will require legal identification.

Some AI identification questions requiring answers:

- What kind of legal identity registration is required for an AI system which is creating new ideas/concepts/products across multiple different jurisdictions?
- What happens when the AI system ceases to exist to their legal identity and how are other systems, like patents, notified?
- How does the AI legal identification for AI system 12345 deal with when the AI system is merged with AI abcde?

AI Creates One or More Virtual AI Bots, Each Working "Independently", Having Medium to High Financial and/or Legal Civil/Criminal Liability

Examples of the above are just emerging. For example, "This Chatbot has Over 660 Million Users—and It Wants to Be Their Best Friend", discusses Microsoft's Xiaoice. In this article "Top 25 successful chatbots of 2020 & Reasons for their success" it states:

> "The average person who added Xiaoice talked to her more than 60 times per month. On average, she even passed the Turing test for 10 minutes, meaning that speakers failed to understand that she is a bot for 10 minutes. This is a significant achievement since the test was one of the first tests designed to measure AI capabilities. It was designed by Alan Turing to see if machines can imitate humans in speech."

It then goes on to review success stories for digital friends, digital assistants, meeting planners, Bot writer/natural language generation, conversion boosters, foreign language tutors, legal bots, medical Q&A/diagnosis bots, therapist bots, travel & hospitality bots, and survey bots.

Are each of these bots, a legally separate bot? Not necessarily. However, depending on their actions, as the legal and criminal risk liability grows for the bots, it becomes more important to know that Jane Doe interacted with Bot12345, on June 15, 2020, which gave her some service which she wants to lay civil or criminal charges for. Bot 12345 may be part of say Acme Enterprise Inc.'s chat bot, or other service, run by a global Acme Inc. AI program.

Some AI identification questions requiring answers:

- What are the legal identification requirements for the overall AI program running many different bots?
- At which point does a bot running under an AI program, like Microsoft's Xiaoice, require its own legal identification?
- How will the legal registration processes be streamlined allowing for rapid registration of new AI bot identities?
- How will the termination of such bots be done within the legal registration system?
- What kind of notification processes are required to people, enterprises and governments when a legal bot ceases to exist?
- If an AI system is merged with another, what happens to the AI systems legal identity? To the legal bots within it?

AI Creates Virtual AI Bots, All Working Together in Singularity, Having Medium to High Financial and/or Legal Civil/Criminal Liability

Today, many bots operate on their own performing specific tasks/services. However, this is beginning to change.

AI swarm intelligence was noted earlier in this thought paper as a potential attack vector. The 2018 article "How Swarm Intelligence Is Making Simple Tech Much Smarter", describes how bots can work closely together in a swarm and learn. The Sept 2019 "The Robotic Future: Where Bots Operate Together and Learn From Each Other", discusses work at MIT in enabling bots to collectively learn together. This YouTube video shows two Boston Dynamics Robots collaboratively working together to open a door.

Given the above, the future is not here yet for AI bots/systems to work together in singularity, learning from each other and then executing physical or virtual "actions", with a medium to high financial and/or legal civil/criminal liability. However, one can see this evolving into place over the coming years.

Some AI identification questions requiring answers:

- How will the AI be legally identified if it's acting in singularity with other AI systems/bots?
- If the AI singularity involved hundreds, thousands, millions or more AI bots/etc., then what effect does this have on our old traditional view of singular identity?
    - Do we need to rethink the concepts of legal identification?
    - If the AI systems are contracting with humans, enterprises, governments or, with other AI systems, and there's singularity involved, how will the contracts specify the partners to the contracts, legally identifying them?
- If AI systems are working together in singularity, what effect does this have on traditional security systems where identification and authentication are built on risk?

AI Models a Human Person and Acts on Their Behalf with Medium to High Financial and/or Legal Civil/Criminal Liability

In my recent thought paper "Digital Twins/Virtual Selves, Identity, Security and Death", I explore digital entities of ourselves. As the paper illustrates, the technology is just now emerging. One can see, in the not so distant future, when virtual selves will be created to be used to work and/or do services on our behalf. These will likely include medium to high risk situations.

The thought paper states the following:

> "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."

Some AI identification questions requiring answers:

- How will digital legal identities be registered?
- How will they tie to the legal physical identity?
- What control does a person have over their digital legal identities?
- How will government agencies issuing human legal digital identities be able to revoke them if they're stolen, etc.?
- What happens when the physical legal identity dies to the legal digital identities?
- What are the terminations laws pertaining to legal digital identities and how does this tie to the legal human digital identity registration system?

AI Models a Human Person and Masquerades as Them

Noted security expert, Bruce Schneier, this past January wrote in the Atlantic Post "Bots Are Destroying Political Discourse As We Know It – They're mouthpieces for foreign actors, domestic political groups, even the candidates themselves. And soon you won't be able to tell they're bots."

The article states:

> "Our future will consist of boisterous political debate, mostly bots arguing with other bots. This is not what we think of when we laud the marketplace of ideas, or any democratic political process. Democracy requires two things to function properly: information and agency. Artificial personas can starve people of both."

The thought paper "Digital Twins/Virtual Selves, Identity, Security and Death" illustrates how what Bruce is talking about will evolve into highly personalized entities. It then discusses new age fraud:

> ***"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."

Some AI identification questions requiring answers:

- How will humans be legally identified as being different than a bot?
- How will digital twins and virtual selves be legally identified?
- What kind of different credential assurance authentication measures can be applied to the digital twin/virtual selves?

AI Identification Solution Framework

Capabilities

The use cases used in this thought paper show that there isn't one answer to create which addresses the AI identification challenges. So, what's does a solution framework require?

It requires the following abilities:

- Provide a common nomenclature for describing AI systems, especially regarding identification
    - This can be used within an enterprise and between enterprises to describe AI systems
- Discern a human from an AI system/bot
- Legally register an AI system/bot globally
    - Since AI bots can be created instantly in one jurisdiction, at insane speeds, and in the next instance be operating in other jurisdictions, it requires a system able to instantly check globally to see if the AI bots exist in any other jurisdiction and, if not, create the AI bot legal identity
- Terminate an AI bot legal registration globally and locally
- Securely register an AI system/bot
    - Design of a secure repository within the AI code which can't be tampered with and/or used to masquerade by another AI code
- Create digital legal identities for digital twins and virtual selves (when required)
    - Link these legal digital identities to the human physical legal identity
        - i.e. Every legal human digital identity must be tied to the singular human physical legal identity
- Have prescribed legal, regulatory and operational rules addressing what happens when AI systems/bots are merged together
- Operationally and legally terminate digital twins and virtual selves' legal identities when the human dies as per the law and regulations
- Have prescribed legal, regulatory and operational rules addressing what happens when AI systems/bots are working together in singularity
- Have the ability for the legal and operational framework to rapidly change as technology changes
    - i.e. Constantly assess legal identify AI governance, administration, business processes, technological infrastructure and user interfaces for potential new attack vectors, rating them with a risk assessment
    - Then have all jurisdictions respond accordingly based on risk

AI System/Bot Identification Proposal

I've coauthored two proposals with Michael Kleeman, a cofounder of many telecom firms across the globe and ex Boston Consulting Group, on rethinking human and AI/Bot legal identities. These proposals have created a new age legal framework, globally and locally, addressing the challenges illustrated in this thought paper, with abilities meeting most, but not all, of the key issues in the area.

100,000 Foot Level Summary

Humans

The legal AI and human identity framework proposal would create:

- A legal, self-sovereign human identity, both physically and digitally, for each person on the planet, that can work at any place on the planet, at any time, at the discretion of the person
    - The legal SSI can be revoked and re-issued when required
- Ability for any legal digital twin/virtual self created to be tied to the legal SSI human physical identity
- Death - ability for the legal registration system to:
    - Notify other agencies and enterprises when the human dies
    - Follow prescribed laws and regulations pertaining to how to terminate the legal registration of a deceased's digital twins/virtual selves
    - Not included in the formal proposals, but laid out in the thought paper "Human Migration, Physical and Legal Identity":
        - Obtaining a baby's fingerprints at birth to attach to the birth registration
        - Obtaining an iris scan during the first year of school to attach to the birth registration
        - The proposal is practical. For example, there are programs including:
            - Designing the underlying databases assuming they're breached and mitigating risk of illegal writes and/or exports
            - Addressing corrupt administrators
            - Obtaining birth registrations in remote places
            - EMP/HMP proofing the datacenters holding the data

AI Systems/Bots

The AI systems/bot proposal would create:

- Flexible, common nomenclature for describing AI systems/bots regarding their identification, then pass this on to a broadly agreed upon standards body to maintain it and promote it to national governments
- Means of identifying Ai/bots from humans
- Global, locally managed, Ai/bot legal identification civil registration vital statistics service:
    - Using some type of AI/bot secure, AI/bot identification code within the AI system
    - Instantly be able to check if the identity exists or not planet wide
        - If not, then instantly register the AI system/bot
    - Have the ability to deal with the merging of two or more AI/bots identities
    - Terminate AI systems/bots as prescribed by laws and regulations

- What the AI system/bot proposal doesn't prescribe:
    - A legal identity solution framework addressing multiple AI systems/bots working together in singularity
    - The proposal acknowledges this, calling out for research on it
        - It's complicated due to the technology, law and business processes involved, many of which doesn't exist yet or, is in early stages of emerging

Both Human and AI Systems/Bots Legal Proposals Would Create

- A global, independent, legal identity test verification institute:
    - Continually do threat assessments of governance, administration, business processes, technological infrastructure and user interfaces used in the legal identification verification processes.
    - Have all jurisdictions respond accordingly, e.g.:
        - A very low risk might take months or longer to address
        - A very high risk will be responded to within hours
    - These would be reported on publicly to both raise awareness and promote good technological hygiene
    - We want to bring industry best practices to the legal identification process

Is All Comes Down to Politics

The paper, "Digital Twins/Virtual Selves, Identity, Security & Death" and "Human Migration, Physical and Digital Legal Identity", lays out many logical reasons why the planet needs to rethink human and AI system/bot legal identities. **However, until politicians want to change, it really doesn't matter what any paper recommends. It all comes down to politics.**

Political decisions revolve around potential pain points, especially how they affect politicians and their political sources of support. So, what are the political pain points?

Getting Elected and Managing the Discussions

As Bruce Schneier's referenced article in this paper notes:

> "Soon, AI-driven personas will be able to write personalized letters to newspapers and elected officials, submit individual comments to public rule-making processes, and intelligently debate political issues on social media. They will be able to comment on social-media posts, news sites, and elsewhere, creating persistent personas that seem real even to someone scrutinizing them. They will be able to pose as individuals on social media and send personalized texts. They will be replicated in the millions and engage on the issues around the clock, sending billions of messages, long and short. Putting all this together, they'll be able to drown out any actual debate on the internet. Not just on social media, but everywhere there's commentary."

The sword that can cut for them, i.e. using AI systems to get their messages out there, can also cut against them. Thus, as AI systems become highly personalized and increasingly harder to detect if it's an AI bot or a real person, politicians will realize they need to rethink human and bot legal identity.

That's why Michael Kleeman and I wrote the incremental human legal identity proposal. Without wading into the political waters in western countries talking about using biometrics for CRVS systems, we simply take what people use today, e.g. paper CRVS, driver's licenses and national ID cards, and begin to rethink it.

The proposed solution will enable politicians to know who really supports them, while minimizing the impact of those using AI bots.

Business & AI Pain Points

Business is paying higher costs due to AI bots, in large part because of:

- Cybersecurity breaches (increasingly using AI as the tool to mastermind the breach) approaching $5 trillion a year by 2024
- False advertising ("Click Deception: Why Marketers Finally Need To Address The Growing Ad Fraud Issue") where up to 1 in 5 ad requests is fraudulent. As the article states:

> "And finally, one more thing to consider is to find a way to identify and verify legitimate human profiles, legitimate businesses and real devices. If you are using popular social media platforms for ads, make sure that the platform participates and uses verified human identities for your ads. Demand in-depth metrics, which include 100% verified identities in results. That way you know for a fact that the like, impression or view was initiated by an actual person."

So, while the politicians address their own concerns about AI/bots being used against them to get elected, they can also give their business community a new set of legal identity tools to:

- Reduce their fraud costs and,
- As this briefing document I wrote notes, the same system can actually be leveraged by business to reduce identity friction costs when the business is interacting with humans and/or AI systems/bots
    - The paper proposes the place to begin in within existing trade agreements such as NAFTA, EU, Trans-Pacific, etc.

Citizen Cybercrime and AI

Citizens, who vote for politicians, are experiencing increasing amounts of identity theft. As Bob Sullivan's November 20, 2019 blog "First-person' ID fraud spikes — sign of coming recession, firm claims" states:

> "Desperation fraud — ID Analytics considers it identity theft and calls it first-party fraud — was up 14 percent in the first quarter of 2019 compared to the year earlier, the firm says. The majority of the increase came in the wireless and online lending industries.
>
> First-party fraudsters knowingly apply for these forms of credit and services with an understanding that their long-term creditworthiness may decline precipitously when they default, but they want the money now and do not worry about the long-term consequences," the firm said."

The best way to combat identity theft, is to rethink legal identity, putting the citizen in control of it via their own legal SSI, both physically and digitally. That's what the incremental human proposal delivers.

Immigration/Migrants

Politicians, planet wide, are increasingly coming under political pressure by their constituents to be perceived as doing something about the rising levels of migrants/immigrants wanting to enter their country. Thus, as the human migration thought paper lays out, the pressure is going to increase over the coming years. However, there are no easy answers.

Thus, for politicians in Western Countries in particular, it makes sense for them to invest in the following:

- Updating their CRVS systems, as per the incremental human proposal paper, to lay the underlying foundations to check CRVS legal identities
    - **This reduces identity fraud within their jurisdictions and also paves the way for implementing a global, CRVS system for AI systems/bots**
- Invest in some pilot sites in Africa, Asia and South America, where resistance to using biometrics isn't high, to implement the proposal laid out in the human migration thought paper
    - Pilot the solutions
    - Design them such that they're rapidly scalable in other jurisdictions
    - Then bring them into the western countries when the time is politically right

Politically Funding the Proposals

One of the challenges with the proposals is it requires rethinking all regional CRVS systems. How can the proposals be rapidly implemented given the number of CRVS jurisdictions involved? Answer: Use national security as the political and funding cover.

The use of AI system/bots can seriously affect a nation's national security. Thus, it makes a good political cover to use this, with national funding to the regional CRVS/driver's license jurisdictions, as the main political driving force to rapidly implement**. It's a win for both national and local jurisdiction politicians.**

If the political will with funding is in place, I can see implementation timelines of approximately 2 years, with pilots occurring at the end of the first year.

Political Summary

Politicians can use the same solution mitigating their election risks due to AI bots, to:

- Reduce identity friction and fraud costs to businesses
- Create a new legal identity infrastructure allowing business to grow
- Reduce citizen cybercrime fraud
- Modernize their citizen identity infrastructure to determine if a person is a citizen or one masquerading as one
- If they're willing, they can invest in a complete rethink of legal human identity in parts of the world where the use of biometrics is acceptable and then bring it back to their jurisdictions when they are ready
- Rapidly show their voters and business they're serious about quickly implementing the initial framework

It's a win for the politicians, a win for business, and a win for citizens.

Summary

What was once thought of as science fiction, i.e. artificial intelligence, is now here and rapidly growing. As this thought paper demonstrates, the lens we use to view it from a legal identification perspective must change. The paper illustrates this via use cases:

- Demonstrating AI can run a corporation with no human shareholders
- AI doing tasks with different levels of financial, civil and criminal liabilities
- AI creating new vaccine products, writing just like the person or inventing new patentable products
- Microsoft's Xiaoice having 660 million chatbot users
- AI bots using swarm intelligence and beginning to work and learn together
- AI creating digital twins and virtual selves of us
- AI bots masquerading as us creating what I call Fraud 4.0

There is no one solution to address the use cases. Instead, the thought paper then lays out capabilities a new solution framework must have. These include being able to legally differentiate humans from AI system/bots, legally registering bots in a global system/locally managed, etc.

A solution framework is then presented, able to meet most of the abilities. It would give people a legal self-sovereign identity, both physically and digitally, identifying them as a human and above or below age of consent. It includes registering bot legal identities globally, tying legal digital and virtual self identities to the physical legal identity. To keep up with the fast pace of technological change, it recommends creation of an independent, global, legal identity test institute for both AI system/bot and human legal identities.

The most important part of this thought paper is the acknowledgment politics is the most important part of the solution framework. Thus, it identifies politicians' pain points:

- Getting elected and managing the discussion
- Business and AI pain points
- Citizen cybercrime and AI
- Immigration/migrants

For each one, it states the benefits to the politicians by adopting the proposed solution framework. It also suggests using national security as a reason to fund the regional CRVS/driver's license jurisdictions. By using it as the main political driving force to rapidly implement, it estimates a two-year implementation window. It's a win for the national and jurisdictional politicians, a win for business, and a win for citizens.

It's our choice as to what we do with artificial intelligence. This thought paper provides a practical AI identification solution framework for the new technology.

"It is not in the stars to hold our destiny but in ourselves." - William Shakespeare

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.