"Artificial Intelligence & Legal Identification" – A Thought Paper

Author: Guy Huntington, President, Huntington Ventures Ltd.
Date: Created March 10, 2020
Updated: October 22, 2021

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

How will legal contracts specify the entities doing the above?

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.

Consider a AI system can create digital bots at thousands or more per second in one jurisdiction, which in the next instance, can be operating in all other jurisdictions around the planet. This throws out the door our old ways of doing legal identity registration in one jurisdiction. It requires a global legal framework, locally managed.

The paper then moves to discussing a high-level architecture for AI systems and bots, as well as referencing a extensive cost centre document.

As Alberta Einstein said, "**We can't solve problems by using the same kind of thinking we used when we created them.**" **Thus, I'm looking for innovative out of the box thinking funders and jurisdictions to work with.**

Artificial Intelligence (AI)

Growth in 2021

Artificial Intelligence (AI) is rapidly growing. This IDC article states AI market growth will be "16.4% year over year in 2021 to $327.5 billion" - https://www.idc.com/getdoc.jsp?containerId=prUS47482321.

It Will Be Used to Attack Corporations, Governments and People

This MIT article, "**Preparing for AI-enabled cyberattacks**" - https://wp.technologyreview.com/wp-content/uploads/2021/04/Preparing-for-AI-enabled-attacks_final.pdf lays it out. The article discusses several different AI attacks including deep fakes stating:

> "In January 2020, the FBI warned that deepfake technology had already reached the point where artificial personas could be created that could pass biometric tests. At the rate that AI neural networks are evolving, an FBI official said at the time, national security could be undermined by high-definition, fake videos created to mimic public figures so that they appear to be saying whatever words the video creators put in their manipulated mouths. "

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

Six 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?

Businesses and Governments Need the Ability to Specify AI System/Bots Legal Identities in Contracts

Contracts are where the legal rubber hits the road. Depending on risk, a contact needs to be able to stand up in a court of law, legally identifying Bot12345 and then specifying what data it can and can't use, who it can share the data with, etc. Today, this isn't possible because we don't have a legal identity framework for AI systems and bots

AI Identification Solution Framework Requirements

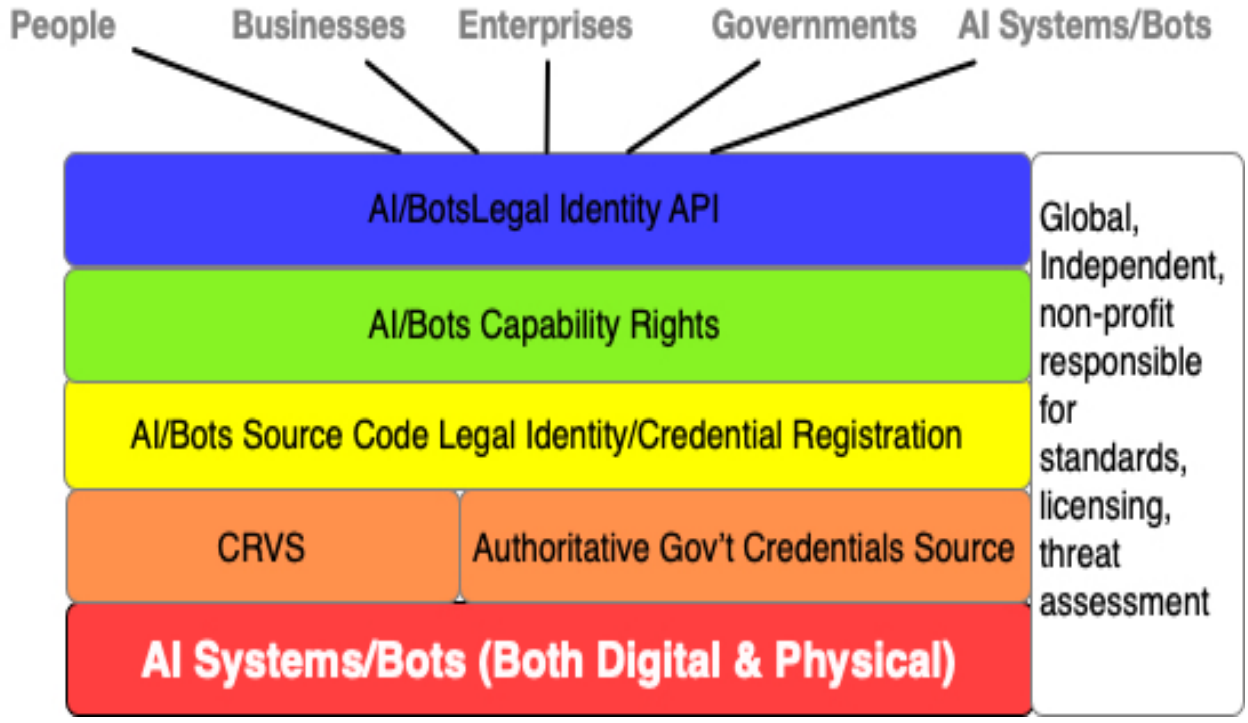
The use cases used in this thought paper show that there isn't one answer to create which addresses the AI identification challenges. So, what's does a solution framework require?

It requires the following abilities:

- 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
- 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 Legal Identity Framework

This recent paper "**Creating AI System/Bots Legal Identity Framework**" - https://hvl.net/pdf/CreatingAISystemsBotsLegalIdentityFramework.pdf , lays out a high-level proposed architecture:



Within the paper it discusses the above, referring to a Cost Centre document which dives into the details. At a high level:

- Where risk warrants it, an AI system/bot is legally registered in a new age global CRVS (Civil Registration Vital Statistics) system, locally managed
- The AI system or bot's legal identity registration is securely written to their source code in a way it's unalterable and can't be easily taken and used in an identity replay attack
- Each AI system/bot has the hypothetical ability to be given authorization rights via TODA file as to what they can and can't do with the data, whom it can be shared with, etc.
    - To learn more about TODA skim this article, "**Legal Identity & TODA**" - https://www.linkedin.com/pulse/legal-identity-toda-guy-huntington?trk=portfolio_article-card_title

- The CRVS, when writing the legal identification to the source code also writes a secure legal identity API
    - This allows other entities to be able to securely query the AI system/bot for their legal identity
- All of this is managed by a new, global independent, non-profit
    - Skim pages 143-155 of "**Cost Centres – Rethinking Legal Identity & Learning Vision**" - https://hvl.net/pdf/CostCentresRethinkingLegalIdentityLearningVision.pdf
    - It does 24x7x365 threat analysis against the AI system/bot legal identity framework, constantly issuing threat assessments
    - Based on the severity level businesses, governments, Ai systems and bots make changes e.g., a very low threat might take months or longer to address, while a very high threat must be responded to within hours
    - This brings current industry best practices to the world of AI system/bots legal identities

To learn more about the cost centres associated with developing the AI system/bot legal identity framework, read pages 74-83 in "**Cost Centres – Rethinking Legal Identity & Learning Vision**" - https://hvl.net/pdf/CostCentresRethinkingLegalIdentityLearningVision.pdf.

Governments MUST Move on This

In In 2017, the EU adopted a resolution with recommendations to the Commission on Civil Law Rules on Robotics. Within the resolution it states:

> "Considers that a comprehensive Union system of registration of advanced robots should be introduced within the Union's internal market where relevant and necessary for specific categories of robots, and calls on the Commission to establish criteria for the classification of robots that would need to be registered; in this context, calls on the Commission to investigate whether it would be desirable for the registration system and the register to be managed by a designated EU Agency for Robotics and Artificial Intelligence."

My point? The issue is far greater than the EU to solve on their own. Why? An Ai system in one jurisdiction on the planet can create thousands or more digital bots per second, which in the next instance can be operating in all other jurisdictions around the planet. Thus, what's required is a global, legal identity registration system, locally managed.

I strongly suggest readers skim this article, "**Why We Need To Legally Register AI Systems and Bots**" - https://www.linkedin.com/pulse/why-we-need-legally-register-ai-systems-bots-guy-huntington?trk=portfolio_article-card_title.

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

The planet is rapidly entering a whopper sized legal identity mess with respect to legal identification of AI systems and bots. Quoting Albert Einstein, **"We can't solve problems by using the same kind of thinking we used when we created them."** **Thus, I'm looking for innovative out of the box thinking funders and innovative jurisdictions to work with.**

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."

For the last six years, he's been thinking, writing, and searching for new pieces with which to rethink both human and AI System/Bot legal identities, as well as also rethinking learning. He now has an architecture and plans addressing this creating:

- SOLICT (source of legal identity & credential truth)
- LSSI (legal self-sovereign identity)
- PIAM (personal identity access management) system
- DLT (digital learning twin) feeding an
- IEP (individualized education plan , with all the above
- Leveraging AI systems and bots as well as
- AI/AR/VR environments

Guy consults on this.