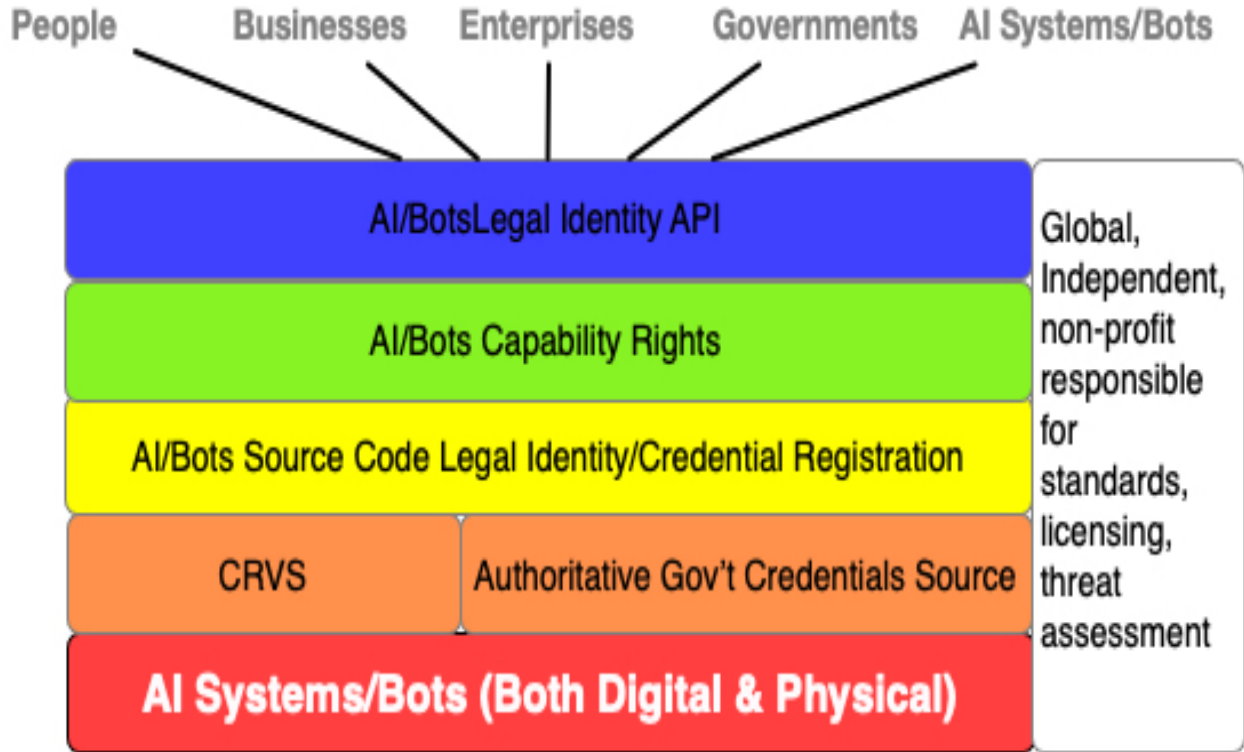


Creating AI Systems/Bots Legal Identity Framework



Author: Guy, Huntington, President, Huntington Ventures Ltd.
October 1, 2021

Table of Contents

CREATING AI SYSTEMS/BOTS LEGAL IDENTITY FRAMEWORK	1
TABLE OF CONTENTS.....	2
EXECUTIVE SUMMARY	3
INTRODUCTION:.....	4
AI SYSTEMS AND BOTS (BOTH DIGITAL & PHYSICAL)	5
<i>Description:</i>	5
<i>AI System/Bots Cost Centre Reference Links:</i>	5
AI SYSTEMS/BOTS CRVS SUB-COMPONENT COST CENTRE	6
<i>Description:</i>	6
<i>AI System/Bots CRVS Cost Centre Reference Links:</i>	6
AUTHORITATIVE AI SYSTEMS BOTS CREDENTIAL SOURCES	7
<i>Description:</i>	7
<i>AI System/Bots Authoritative Credentials Cost Centre Reference Links:</i>	7
AI/BOTS SOURCE CODE LEGAL IDENTITY/CREDENTIAL REGISTRATION	8
<i>Description:</i>	8
<i>AI System/Bots Source Code Legal Identity/Credential Registration Cost Centre Reference Links:</i>	8
AI/BOTS CAPABILITY RIGHTS	9
<i>Description:</i>	9
<i>AI System/Bots Capability Rights Cost Centre Reference Links:</i>	10
AI SYSTEM/BOTS LEGAL IDENTITY API.....	11
<i>Description:</i>	11
<i>AI System/Bots Legal Identity API Cost Centre Reference Links:</i>	11
AI SYSTEM/BOTS, GLOBAL, INDEPENDENT, NON-PROFIT	12
<i>Description:</i>	12
<i>AI System/Bots Global, Independent, Non-Profit Cost Centre Reference Links:</i>	12
SUMMARY	13
<i>High-Level Reference Documents:</i>	13
ABOUT THE AUTHOR:	14

Executive Summary

Typically, we use our old lenses to view change and problems created by the new tech, like AI, coming at us. Quoting from Albert Einstein, “We can’t solve problems by using the same kind of thinking we used when we created them.” This especially applies to AI. Why?

Consider the speed at which an AI system in one jurisdiction can create virtual bots i.e., thousands or millions per second, which in the next instance can be operating in all other jurisdictions around the planet. This effectively throws out the door our old, slow, state/provincially based CRVS (civil registration vital statistics) legal identity registration system. It won’t work.

Then skim pages 6-7 of “Artificial Intelligence & Legal Identification” - <https://hvl.net/pdf/ArtificialIntelligenceLegalIdentificationMarch2020.pdf>, which talks about the fact that today, AI can own LLC’s (limited liability corporations). Read page 10 which discusses patents applied for on behalf of AI systems. Page 11 talks about Microsoft’s Xiaoice chat bot service, used by 660 million people, on average 60 times a month, with the average user taking 10 minutes to figure out they’re talking to a bot and not a human.

There’s one whopper sized technical problem with registering legal identities of AI systems/bots - the legal registration must be written to the underlying source code in such a way it can’t be tampered with by criminals/malicious states. In “**Mission Control – We Have a Problem**” - https://www.linkedin.com/pulse/mission-control-we-have-problem-guy-huntington?trk=portfolio_article-card_title, it lays out the journey I’ve taken to get this far.

Within the article it discusses an idea I had three years ago of creating a identification unit within the source code. Here’s the challenge with doing this:

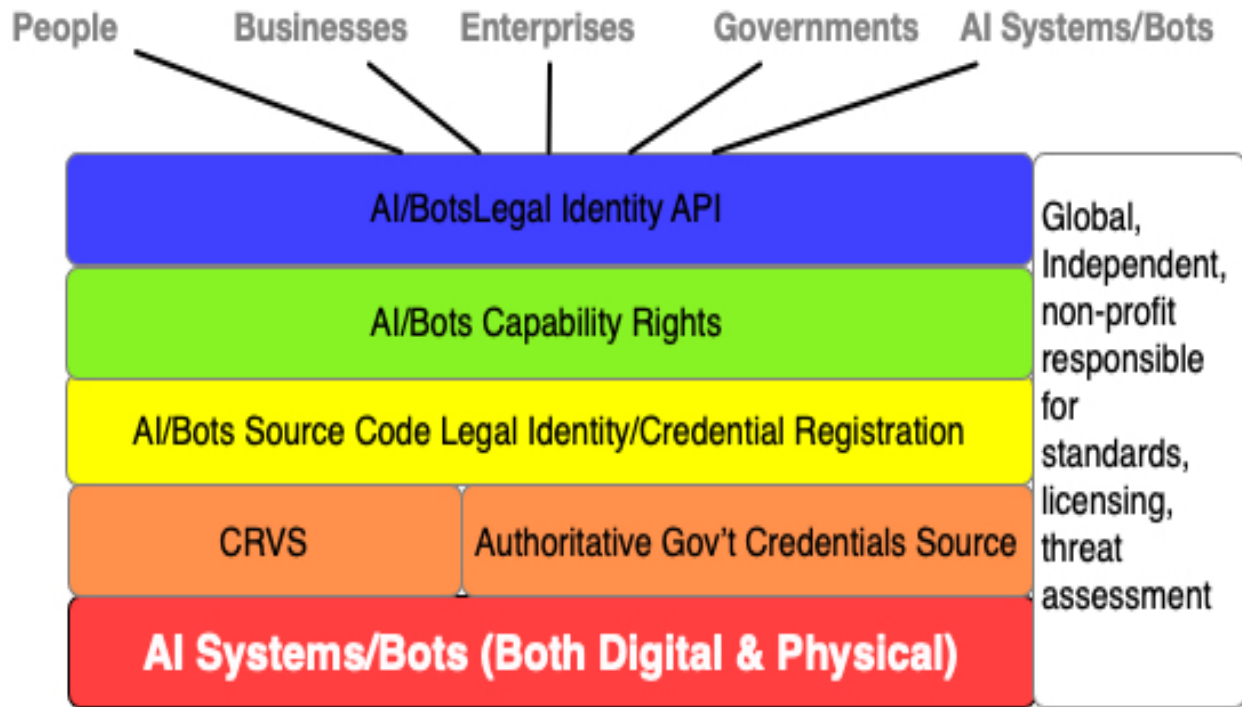
- Can the identification unit code be securely inserted into a Ai system or bot source code such that it can’t be easily manipulated?
- How will the identification unit data be queried by a person, entity or system wanting to know what it’s legal ID is?
- How will any authorization rights assigned to the AI system or bot be attached to the actual legal identity?

I’ve broken out this component on its own, since no existing legal framework exists today which can address this. It requires innovative, out of the box funders, together with jurisdictions, and AI system/bot industry folks, to quickly bear down on this. It’s highly jurisdictional i.e., very political.

Finally, readers should skim “**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/> and “**Why AI Regulation Requires Legal Identities of AI Systems and Bots**” - <https://www.linkedin.com/pulse/why-ai-regulation-requires-legal-identities-systems-bots-huntington/>.

Introduction:

This document is a high-level flyover of the major components to create a legal identity framework for AI systems and bots. It's written for senior decision makers to get a grasp of the components. It uses this diagram to illustrate the high-level components:



Within component section, it contains references to specific cost centre details, which the decision maker will likely want to direct their analysts to.

Here's how the document works:

- Component title
- Short description
- Reference link to more detailed cost centre information

AI Systems and Bots (Both Digital & Physical)

Description:

The strategy is to find funders, and then bear down on only 1-2 industry sectors to focus our efforts on. These sectors must include use of:

- AI systems
- Physical bots
- Virtual bots

I believe the education sector is perfect for this since all the above exists in it. Health is a highly probable sector to also focus on.

Create a core group of:

- AI system/bots experts out of industry and university research groups
- Couple this with legal, legislation and CRVS experts
- Add to this red team experts and business process folks

This then provides the initial team, with practical industry examples, to begin drilling down into the cost centre components.

As background in education, consider these types of bots:

- **QT Robot** - <https://luxai.com/humanoid-social-robot-for-research-and-teaching/>
- **Hanson's Little Sophia** - <https://www.hansonrobotics.com/little-sophia-2/>
- **“Using Chatbots as Smart Teaching Assistants for First-Year Engineering Students”** - <https://peer.asee.org/using-chatbots-as-smart-teaching-assistants-for-first-year-engineering-students.pdf>
- **“A.I. teaching assistants could help fill the gaps created by virtual classrooms”** - <https://www.digitaltrends.com/computing/how-ai-is-changing-education/>

To see a story illustrating the use of bots in schools, skim these two articles:

- **“Kids, Schools, AI/AR/VR, Legal Identities, Contracts and Privacy”** - https://www.linkedin.com/pulse/kids-schools-aiarvr-legal-identities-contracts-guy-huntington?trk=portfolio_article-card_title
- **“Kids, Digital Learning Twins, Neural Biometrics, Their Data, Privacy & Liabilities”** - https://www.linkedin.com/pulse/kids-digital-learning-twins-neural-biometrics-data-guy-huntington?trk=portfolio_article-card_title

AI System/Bots Cost Centre Reference Links:

Read page 74-83 of “Cost Centres – Rethinking Legal Identity & Learning Vision” – <https://hvl.net/pdf/CostCentresRethinkingLegalIdentityLearningVision.pdf>.

AI Systems/Bots CRVS Sub-Component Cost Centre

Description:

Why use the human CRVS system to legally register AI systems and bots? These entities will require legal identities (skim, “**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).

Further over time, as these entities acquire more and more human like abilities, as well as also operating as smart digital identities of us, the lines blur between human and AI systems/bots. Thus, it makes cost effective sense to leverage a rethought CRVS system to also register AI systems and bots’ legal identities. Finally, the CRVS also contains smart digital entities of us i.e., AI powered. Thus, if the CRVS is going to contain these types of entities, it also should contain AI systems and bots entities.

If the decision is made to do so, then it makes sense to expand the teams and budgets used for human and smart digital identities of us within the CRVS systems cost centres.

AI System/Bots CRVS Cost Centre Reference Links:

The CRVS cost centre teams to be expanded are contained within pages 41-73 of **Cost Centres – Rethinking Legal Identity & Learning Vision** – <https://hvl.net/pdf/CostCentresRethinkingLegalIdentityLearningVision.pdf>. Page 76 contains the cost centre link for this section.

Authoritative AI Systems Bots Credential Sources

Description:

The same assumption made above for leveraging the work of the human CRVS team, should also apply here for determining what government authoritative sources are required to certify these entities for different things e.g., teaching credentials, etc. Don't reinvent wheels. Thus, in the Cost Centre: Authoritative Gov't Credentials Source section of the cost centre document, it includes AI system/bots experts as part of the team.

My recommendation is to first focus on only 1-2 industries to focus on e.g., education and health. Learn what works, what doesn't work, and then rapidly scale to other industries.

AI System/Bots Authoritative Credentials Cost Centre Reference Links:

Read pages 89-92 in “Cost Centres – Rethinking Legal Identity & Learning Vision” – <https://hvl.net/pdf/CostCentresRethinkingLegalIdentityLearningVision.pdf>

AI/Bots Source Code Legal Identity/Credential Registration

Description:

As noted in “**Mission Control – We Have a Problem**” -

[https://www.linkedin.com/pulse/mission-control-we-have-problem-guy-](https://www.linkedin.com/pulse/mission-control-we-have-problem-guy-huntington?trk=portfolio_article-card_title)

[huntington?trk=portfolio_article-card_title](https://www.linkedin.com/pulse/mission-control-we-have-problem-guy-huntington?trk=portfolio_article-card_title), determining exactly how a legal identification can be securely inserted into an AI system/bots source code is not trivial. Achieving this is the main deliverable of this cost centre

Note:

1. There are many different university research groups combining AI and law faculties
 - a. It’s likely some of these should be approached to also participate
2. The same team working on this must also work with the following other teams described in the cost centre document:
 - a. CRVS Smart Digital Identity Source Code team
 - b. Cost Centre: Authoritative Gov’t Credentials Source

By solving it for one, it applies to the other. Thus, the costs will be borne between the three different costing groups.

AI System/Bots Source Code Legal Identity/Credential Registration Cost Centre Reference Links:

Read pages 79 in “**Cost Centres – Rethinking Legal Identity & Learning Vision**” –

<https://hvl.net/pdf/CostCentresRethinkingLegalIdentityLearningVision.pdf>.

AI/Bots Capability Rights

Description:

Skim these two articles on AI/AR/VR environments in a global classroom:

- “Kids, Schools, AI/AR/VR, Legal Identities, Contracts and Privacy” - https://www.linkedin.com/pulse/kids-schools-aiarvr-legal-identities-contracts-guy-huntington?trk=portfolio_article-card_title
- “Kids, Digital Learning Twins, Neural Biometrics, Their Data, Privacy & Liabilities” - https://www.linkedin.com/pulse/kids-digital-learning-twins-neural-biometrics-data-guy-huntington?trk=portfolio_article-card_title

It has a student, John Doe, who has his learning assistant bot “AssistBot”, with a human teacher, Sally Goodteacher, and two teaching assistant bots, BobBot and PattyBot. Further, contracts need to be created on the fly between not only John’s parent Jane Doe, for him and his AssistBot, his school district, other school districts, Sally Goodteacher, BobBot and PattyBot, that specifies what data can be used by whom, how it’s used, stored, shared, archived, and terminated.

So, an AI system, physical and/or digital bots will require authorization rights, which depending on risk, must be spelled out in contracts. My dumb question is how will this be done in a secure, scalable manner? Where will the contracts pertaining to a specific legal identity AI systems or bots be stored? **Yes, it’s complicated. That’s the world we’re entering.**

Which led me to a protocol called TODA, to rethink how not only contracts are sent from one party to another, but also to begin to create authorization rights standards, leveraging TODA capability files. Skim this article to learn more about TODA – “**Legal Identity & TODA**” - https://www.linkedin.com/pulse/legal-identity-toda-guy-huntington?trk=portfolio_article-card_title.

In the human cost centre of the cost centre document, I have architected for the storage of consents to occur in each person’s SOLICT. Can this be applied to AI systems and bots? I don’t think so. Why?

The sheer number of them can easily be in the trillions or more. Thus, creating a separate database per AI system and bots doesn’t make sense. Which is why in the diagram used for AI systems/bots legal identities, I don’t have a SOLICT component.

I don't have a magic wand to wave that solves all AI systems and bots authorization rights and contracts. However, I can see the need to come together to agree on preliminary authorization rights, protecting a human and AI system/bots privacy. Which is why I've included capability files in my first guesstimate at an architecture. I honestly don't know how this will evolve.

My suggestion is to first focus on one industry e.g., education. Try to evolve some standards for AI systems and bots authorization rights, assigning it to a specific legal entity, leveraging Kantara User Managed Access (UMA)

(<https://kantarainitiative.org/confluence/display/uma/Home>) to store it in a common, secure, location for each entity. As a last thought, perhaps the Groningen Foundation or, a similar body, might be interested in developing common education contract standards.

AI System/Bots Capability Rights Cost Centre Reference Links:

Read pages 80-81 in “**Cost Centres – Rethinking Legal Identity & Learning Vision**” – <https://hvl.net/pdf/CostCentresRethinkingLegalIdentityLearningVision.pdf>.

AI System/Bots Legal Identity API

Description:

Beyond the challenges associated with writing legal identification information to the source code, there's another challenge i.e., how to uniformly access the legal identification within an AI system or bot? I have an idea on how to solve this...

Create a standard AI system/bot legal identity API which can also be inserted into the AI system/bot source code. Hypothetically, it can be designed to be very secure. IF IT'S POSSIBLE, AND IT MAY OR MAY NOT BE, it addresses the problems of how to query trillions of AI systems and bots for their legal identities and/or for them to present it to a third party. So, I've included this in the architecture to get discussion and debate going on how this will be addressed.

AI System/Bots Legal Identity API Cost Centre Reference Links:

Read page 82 in “Cost Centres – Rethinking Legal Identity & Learning Vision” – <https://hvl.net/pdf/CostCentresRethinkingLegalIdentityLearningVision.pdf>.

AI System/Bots, Global, Independent, Non-Profit

Description:

This curve - <https://hvl.net/pdf/PatScannellHockeyStickShapedCurve.pdf>, hypothetically means each hour new potential attack vectors are being created against the legal identity framework for AI systems and bots i.e., governance, business processes, tech used and AI system/bot entities. My premise is most governments and enterprises around the planet don't have the expertise, resources or budgets to continually address this.

That's why myself and Michael Kleeman created the concept of a global, independent non-profit. It's job is to not only set standards for AI system/bot legal identification, but also do 24x7x365 threat analysis. The non-profit also does the same for human legal identification.

Our idea on how to continually fund the non-profit is to license out the new CRVS system, on a per CRVS event, to a maximum yearly amount. The actual fee per event must be low to encourage all jurisdictions to participate.

AI System/Bots Global, Independent, Non-Profit Cost Centre Reference

Links:

Read page 143-155 in “Cost Centres – Rethinking Legal Identity & Learning Vision” – <https://hvl.net/pdf/CostCentresRethinkingLegalIdentityLearningVision.pdf>

Summary

The reason I've broken out AI systems/bots legal identification as a separate document is to draw attention to the urgent need to address this. Today, there isn't a legal identity framework on the planet for it. Ironically, we're creating millions of these types of entities, without a legal ability to specify each entity in contracts, in a manner which works around the planet.

The lack of a legal identity framework for AI systems and bots is creating very high risk as criminals and malicious states take advantage of it. In my head, it's like opening the vault to a rich bank, telling criminals to come on in:



To close the vault door, requires out of the box, innovative funders, along with 1-3 willing jurisdictions.

High-Level Reference Documents:

- “Rethinking Human Legal Identity” - <https://hvl.net/pdf/RethinkingHumanLegalIdentity.pdf>
- “Cost Centres – Rethinking Legal Identity & Learning Vision” – <https://hvl.net/pdf/CostCentresRethinkingLegalIdentityLearningVision.pdf>
- “Transformational Learning Vision” – <https://hvl.net/pdf/TransformationalLearningVision.pdf>
- “Learning Vision Flyover” – <https://hvl.net/pdf/LearningVisionFlyover.pdf>
- “Learning Journey of Two Young Kids In A Remote Village” - <https://hvl.net/pdf/LearningJourneyofTwoYoungKidsInARemoteVillage.pdf>
- “Sir Ken Robinson – You Nailed It!” - https://www.linkedin.com/pulse/sir-ken-robinson-you-nailed-guy-huntington?trk=portfolio_article-card_title

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.

