Artificial Intelligence Governance - Identification

G. Huntington, President, Huntington Ventures Ltd.

March 13, 2020

Putting What Follows Into Context…

- I’ve been working the last 4 years on rethinking human and bot legal identification
- While it’s important, it pales into insignificance against global warming
- Each day, when I get up and look out over the Pacific ocean, where I live, I think to myself, “We have to change”, as the waters warm, the icecaps melt and lots of planetary life is lost
- I’ll return to this at the end of the presentation…

What's Covered in this Presentation?

- Premise
- Who am I?
- Co-writing two proposals on rethinking human and AI system/bot legal identities
- AI Governance and Identity
- It all comes down to politics
- Questions!!!!
  - This is the part I'm most looking forward to!

My Premise for this Presentation

- 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
- Which leads me to my premise:

  "Regarding AI, what worked in the past for identity laws and operationalization, won't likely work in the future. It requires a global rethink, not just a regional jurisdictional one"
- Which is the point of this presentation and the proposals discussed herein

Who am I?

- I’ve led, as well as rescued, many large, complicated identity projects including Boeing, Capital One and the Government of Alberta’s Digital Citizen Identity & Authentication project
- You can check me out via LinkedIn
  - https://ca.linkedin.com/in/ghuntington

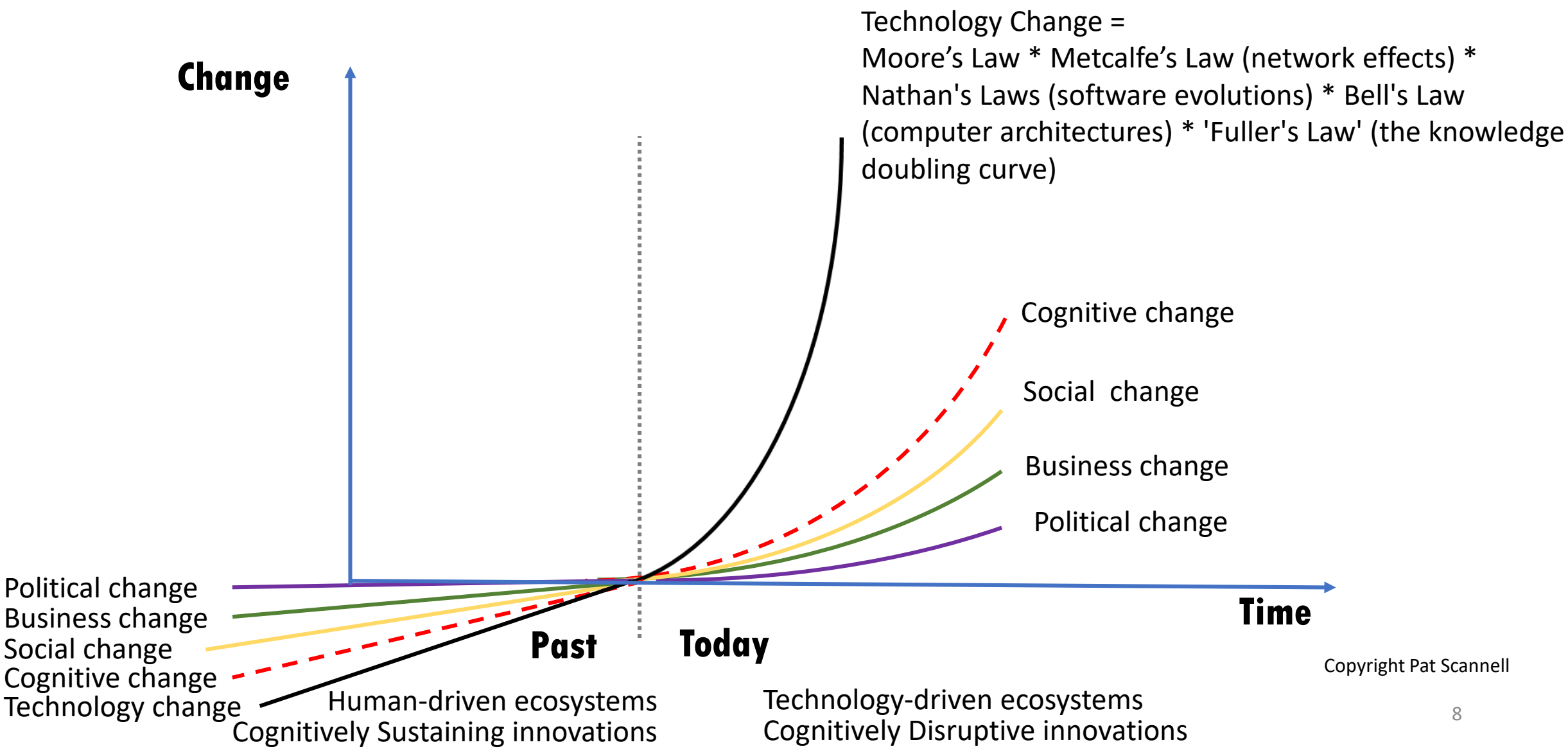
Technological Tsunami Papers

- This past year and a bit, I've written 29 papers about the incoming technological tsunami wave composed of AI, AR, VR, bots, genetic engineering, wireless and nanotechnology
- My premise? We're rapidly entering what I call a "non-private world", requiring new laws for identity, data and consent AND, they must be enforceable around the world

Meeting Pat Scannell

- Along the way of writing all the papers, Vint Cerf really liked the bot ones, and invited me to join his “People Centered Internet” (PCI) group he’d cofounded with Mei Lin Fung
- There, I met technology visionary Pat Scannell, and he’s been in my head ever since! Why?
- As part of his research he produced the following graph…

How Fast Will Disruption Happen?



What This Means…

- “Think about it: The pace of change has never been this fast, yet it will never be this slow again” - Justin Trudeau, Davos, 2019
- It also means that the best human or AI system/bot legal identification solution created, can quickly become tomorrow’s turd due to technology affecting the underlying governance, administration, business processes, technology infrastructure and user interfaces
- That’s why Pat is in my head

Meeting Michael Kleeman

- This past Sept I attended ID2020 in New York where I met Michael Kleeman, a cofounder of many telecom firms across the globe, and ex Boston Consulting Group. We immediately hit it off because we are both visionaries, and practical implementors
- As an aside, I talked to him about a device I had spec'd out at the 100,000 foot level to capture CRVS (civil registration vital statistics) registration remotely in the paper "Where Shit Happens" (go to page 25)
- He told me it was all do-able

Private Keys

- In my papers, you'll see I was recommending the use of Blockchain/Sovrin
- However, I wasn't comfortable with this because of the issuance of virtual private keys. The cryptocurrency market is full of horror stories where a malicious person gains access to your personal e-wallet, obtains the key and then milks the account
- I went looking for a better solution and came across Ngrave, where they use an offline device to publish the private key to, also sending a QR code which then sync's with their digital app
- I called Michael up asking him how we could take the same type of strategy and inexpensively use it with CRVS systems?
- He suggested using Near Field Communication (NFC)

The Birth of Our Human Legal Proposal

- At that moment, the lightbulbs went off in both our heads
- We could see how we could rejig what people already use today, e.g. driver's licenses and/or national ID cards by converting them to NFC cards
- Have the CRVS be able to write a private key to the card along with a QR type code containing their legal identity information
- Then sync the QR type information with the legal digital app
- We also could see how the CRVS could also write a private key legally, anonymously indicating you're a human and above or below age of consent
- The physical card can be revoked and reissued
- Thus was born our human legal self-sovereign identity (SSI) proposal

Diane Strahan Liked the Proposal

- She's ex COO of the Motion Picture Association and ex SVP at Nuestar, who I also met at PCI (thanks Vint and Mei Lin!)
- She helped edit the proposal, telling me how advertisers are currently being significantly frauded by bots mimicking humans
- She liked the idea of a person being able to legally prove they're a human
- **Keep this in mind for the last AI use case coming up!**

To Make the Human Proposal Magic Work…

- Global data and common query protocol standards for CRVS systems
- Global common standards for digital driver's licenses and national ID cards
- Conversion of driver's licenses and national ID cards to NFC devices
- Creation of CRVS as certificate authorities
- Allowing CRVS to write to driver's licenses/national ID cards
- Changing laws enabling all the above to happen

Artificial Intelligence Governance Operationalization

- Identification of AI is one of the major components
- However, it's not straight forward
- I've just finished a thought paper "Artificial Intelligence and Legal Identification" in which I lay out my thoughts about this
- It all begins with risk…

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 Running a LLC

- The thought paper refers to two legal papers written in 2015/16 by Shawn Bayern, Florida State University and some other professors from Cambridge and EU
  - The Implications of Modern Business Entity Law for the Regulation of Autonomous Systems
  - Company Law and Autonomous Systems: A Blueprint for Lawyers, Entrepreneurs, and Regulators

- It states that it's relatively easy to set up a LLC (limited liability corporation) and have AI run the company with no human shareholders, especially in the US
- It affects entities like GLEIF (Global Legal Entity Identifiers Foundation), producing unique identifiers for corporations planet wide

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?

AI Does Tasks with Low, Medium or High Risk for Financial and/or Legal Civil/Criminal Liability

- 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 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?
- What determines when a low risk becomes a medium/high risk?

AI Creates New Ideas/Concepts, Products, etc.

- 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"
- What was once thought of as science fiction is now here, in its early days

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 to their legal identity, and how are other systems, like patents notified, when the AI system ceases to exist?
- 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

- 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."

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

- 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
- Singularity is not here yet…but one can see it evolving

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 involves 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 and law?
  - 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 this, 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?
- I don't have any good answers for the above

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
- The thought paper states the following:

  "Every legal human digital identity must be tied to the singular human physical legal identity"

- **So, you can see where the use of the human legal physical SSI comes into play!**

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 to the legal digital identities when the physical legal identity dies?
- 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."
- In my thought paper "Digital Twins/Virtual Selves, Identity, Security and Death", it illustrates how what Bruce is talking about will evolve into highly personalized entities, and discusses what I call new age 4.0 fraud:

"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 Legal Identification Framework – 100,000 foot level

- For low risk legal identification – create a flexible, common nomenclature for describing AI systems/bots regarding their identification, then pass this on to broadly agreed upon standards body to maintain it, and promote it to national governments
- Means of identifying AI/bots from humans
  - How this will happen needs to be determined
- Global, locally managed, AI/bot legal identification civil registration vital statistics (CRVS) service:
  - Using some type of 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 AI/bots merging with one another
- Terminate AI systems/bots as prescribed by laws and regulations
- All of the above is very challenging to achieve

Global, Independent, Legal Human and AI/Bot Identity Test Verification Institute

- Continually do threat assessments of all 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
- We want to bring industry best practices to the legal identification process
- **This addresses the challenges Pat's diagram illustrates**

It All Comes Down to Politics…

- Regardless of what I and others write and say, it doesn't matter until politicians want to change
- Political decisions revolve around potential pain points, especially how they affect politicians, and their political sources of support
- So, what are their political pain points?

Getting Elected and Managing Messages

- **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

- Cybersecurity breaches (increasingly using AI as the tool to mastermind the breach) costing $5 trillion 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
- **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 document proposes the place to begin is within existing trade agreements such as NAFTA, EU, Trans-Pacific, etc.

Citizen Cybercrime and AI

- 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
- So, by using the same solution to solve politicians' problems, they can use it to give their voting base a win

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
- By updating their CRVS systems, as per the incremental human proposal paper, it lays 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-ish 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 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. Then bring it back to their jurisdictions when they're 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**

Montreal Protocol 1987

- In 1987 countries around the planet agreed to reduce CFC's to mitigate the risk of a deteriorating ozone layer, called the "Montreal Protocol"
- For what it's worth, in my gut, I feel a similar situation exists today regarding AI governance, i.e. Pat Scannell's technology curve shows its already moving faster than our old laws in each jurisdiction
- I feel, if the collective "we" can line up the EU, US and China on agreeing to implement the proposals, many other countries will also fall into line
- I also feel that if we can get this accomplished, and yes it's a whopper hill to climb, it sets the stage for subsequent environmental agreements, as global warming increases, and planetary conditions deteriorate

Some Last Wise Words From the Bard…

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

Thanks for Listening to Me!

- The thought and proposals paper referred to in this presentation are all available off my website at https://hvl.net/papers.htm
- My email is guy@hvl.net, cell is 780-289-2776
- I live in West Vancouver, BC, Canada
- **Thoughts, comments, criticisms, suggestions or questions?!!!!!!**