"Technological Tsunami & Future of IAM"

Author: Guy Huntington, President, Huntington Ventures Ltd.
Date: Created May 2019/ Updated July 2019

TABLE OF CONTENTS

Target Audience

This paper's aimed for the following:

- C-suite
  - CIO
  - COO
  - CTO
  - CSO
  - CRO
  - CEO
  - CLO
  - CHRO
- General Counsel
- Security folks
- IAM specialists
- Anyone interested in a deeper dive into the world of identity and what the future looks like as a result of the incoming technological tsunami wave

As the Executive Summary says, it's not a quick read. That's because the incoming tsunami wave is complex. To understand the wave impacts from the bedroom to the boardroom on identity and access management, read on.

Note to Reader:

I have been writing about rethinking civil registration systems since 2006

- "The Challenges with Identity Verification"

Over the last year, I have written 26 papers on the impacts from the technological tsunami. Here's a listing of them, by subject area, with links to each one:

- 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.

Executive Summary:

I selected the picture at the beginning of this paper for a reason. It's a person, holding an umbrella, standing in a growing puddle of water, watching a large tsunami wave approaching them from in front and their sides. The analogy is it's us, holding up our old school IAM systems as our umbrella. Meanwhile, all around us, the technological tsunami wave is rapidly approaching.

This paper takes a very different approach than the other 22 I've written. In those, I state a premise the incoming technological tsunami of AI, AR, VR, robotics, genetic engineering, nanotechnology, and wireless, requires new laws for identity, data, and consent. This paper assumes it's not going to happen anytime soon. Thus, I take a pragmatic approach to IAM, measuring what can be done to survive this coming tsunami.

The paper covers the following:

- Age of LDAP is ending
- Old ways of identification/authentication are becoming less relevant
- IAM and behavioral/biometric technology
- Strategies addressing biometric ERR rates and reader spoofing
- IAM, AI & IoT- reducing the attack vectors
- Robotics is here
- Cloning/biorobotics is coming
- Tsunami wave cybersecurity center
- Global digitization is at risk

It’s not a quick read because the coming tsunami wave is complex.

To illustrate this, I use practical use cases from the bedroom to the boardroom, explaining how behavioral/biometrics will change IAM. I propose each of us will have our IAM system.

The paper reviews IoT and its many different attack vectors showing how IAM should assist. It discusses robotic identity registration and authentication, using practical use cases, showing challenges the IAM industry needs to face. Next, it examines the growing impact of cloning and biorobotics.

It then states my belief most enterprises can't keep up with the tsunami wave. They'll increasingly outsource a growing portion of their cybersecurity, both internally and externally. It ends with a discussion of a 1 in 8 chance THIS DECADE we could all go back to the dark ages.

This paper is a summation of my many years of experience leading complex identity projects. I believe the tsunami wave will make these past projects look like child's play.

"Technological Tsunami & Future of IAM"

Introduction

I have an underlying premise. There is a technological tsunami approaching our planetary shores composed of the following:

- Artificial Intelligence (AI)
- Augmented Reality (AR)
- Virtual Reality (VR)
- Robotics (both virtual and physical)
- Genetic Engineering
- Nanotechnology
- Wireless

They're converging, creating what I call a "non-private" world, rendering increasingly useless our old ideas of identity, data, and consent.

Pat Scannell, noted technology industry veteran and thought leader, showed me some of his work regarding technology change. It shows a hockey stick shaped curve indicating change vs time. He told me that while most people believe technology is growing at something like the speed of Moore's Law, he believes the rate of change is much steeper:

- Instead of proceeding at the exponential pace of Moore's Law, technology is exploding logarithmically at the rate of Moore's Law * Metcalfe's Law (network effects) * Nathan's Laws (software evolutions) * Bell's Law (computer architectures) * 'Fuller's Law' (the knowledge doubling curve)
- All of these manifests in different industries and domains, which is in itself another feedback loop, adding additional acceleration
- It is accelerating much faster than anyone realizes

I concur.

This past year, I wrote 22 papers about this. In "The Identity Lifecycle of Jane Doe," I describe the effects on Jane Doe the child, the teenager below age of consent, the adult, and through to her death.

This incoming tsunami wave affects all of us, regardless of where we live on the planet. It affects children playing in a playground, us in our bedrooms, or walking down a street. In the papers, I propose a rethink of our laws about identity, data, and consent, globally.

This paper takes a different tack than the others. It assumes the creation of new laws won't be happening any time soon. Instead, it focusses on the impacts of the technological tsunami wave on identity and access management (IAM) making practical recommendation. Throughout the paper, I make numerous suggestions as to what's required to channel the incoming tsunami wave.

It will cover the following:

- Age of LDAP is ending
- Old ways of identification/authentication are becoming less relevant
- IAM and behavioral/biometric technology
- Strategies addressing biometric ERR rates and reader spoofing
- IAM, AI & IoT- reducing the attack vectors
- Robotics is here
- Cloning/biorobotics is coming
- Tsunami wave cybersecurity center
- Global digitization is at risk

This paper is a summation of my many years of experience leading complex identity projects. I believe the tsunami wave will make these past projects look like child's play.

Age of LDAP is Ending

The Light Weight Directory Access Protocol (LDAP) has been a foundational cornerstone for the IAM industry since the industry began. It offered a tool, allowing enterprises to centrally link identities to authoritative sources, with a swift lookup.

This age is ending. Why?

- IoT
  - The sheer number of different IoT devices, with who can use them, share the data, etc. creates many relationships. LDAP and traditional databases aren't traditionally designed to handle this.
- Robotics
  - As other sections of this paper state, robotics is here
  - In the not so distant future, we'll soon be creating millions and then billions of them
  - As with IoT, there will be many different relationships with a robot; it's owner, users, etc.
- Fast-Changing Relationships
  - The speed of change I was referring to earlier in the paper affects each of us at the relationship level
  - As the planet digitizes, we can assume many different relationships with each other, IoT and robots
  - These can and will change frequently

Summing all this up, LDAP isn't suitable for fast changing multiple relationship models.

The Rise of Graphing Databases and IAM

Graphing databases allow for creating many to one and one to many relationships and quickly changing them. My friends at Nulli - Identity Management, have been integrating graph databases with IAM since 2013. They bring a true Identity Relationship Management (IRM) solution to their IAM clients.

Graphs are the foundations of social networking successes like Facebook, Twitter, and others as well are the "recommendation engines" underlying digital commerce. Nulli works with clients to deploy these graph features that provide IAM flexibility, better governance in support of compliance as well as deepening connections to customers. The use of graphs, like Neo4j is a crucial enabler for securing access to the IoT world as well as current and future IAM standards.

Graphing databases are the future. As each year progresses, with the total number of "identities" going into the trillions, having what I call "oodles" of changing different relationships, the age of LDAP will diminish.

Old Ways of Identification/Authentication are Becoming Less Relevant

The IAM industry began with the concept of a global unique identifier (GUID) or, universally unique identifier (UUID), which enterprises adopted to centralize a common identity within their multiple databases.

The GUID/UUID was and is still used today to rapidly provision, change, and deprovision an identity of access to systems, applications, and things. It's also used as the cornerstone to grant a user one or many different authentication mechanisms.

Over the last 20 years, identity assurance came into being. Different levels of trust were created, assigning different types of documents and identity proofing processes. Various legal jurisdictions and enterprises use different identity assurance schemes.

With the rise of digitization, the concept of a "digital ID" began to emerge. Over the last several years, there has been increasing debate about what the digital ID should be, who owns it and who controls it. The rise of Sovrin/Blockchain is but one example of this.

Here's my premise…GUID/UUID will be increasingly become less meaningful with the incoming technological tsunami wave. Why?

As the papers "I Know Who You Are & What You're Feeling – Achieving Privacy in a Non-Private World" and "Privacy Gone – AI, AR, VR, Robotics and Personal Data" lay out, a person can be identified by their face, gait, eye blinks/second, mannerisms and increasingly on more personal biometric data like skin temp, ECG, EEG, etc.

At the state level, in China, today, this is already beginning to occur. Watch this video by Michelle Yan of Business Insider to see what's rapidly coming at us. Businesses too will want to adopt this technology to intimately know their customers. Thus, a person walking down a street can be "identified" by people walking towards them, by storefronts, etc.

The revolution extends into emotions. As one example, go to Affectiva's website. There you'll see how, via face muscles, feelings are detected. This type of technology is being deployed into HR departments for recruitment interviews, cars for determining road rage, etc.

If one stands back and contemplates all of this, one can see:

- Accumulation of data from a person, at the rate of gigabits/second, combined with
- Analysis of it, in real time and compared to other times will result in
- The instant ability to not only recognize who you are and authenticate you BUT
- Do predictive behavior modeling
- If it's combined with other external databases, there is no privacy for the person UNLESS
- They are in control of their own identity, data, and consent

The idea if a UUID/GUID will slowly become less critical as data behavioral/biometric profiles grow to identify a person.

With each passing week, month, and year, it increasingly puts under the technological tsunami bus our old ideas of identity verification, authentication, data, and privacy. So, what's required to address this?

New Laws About Identity, Data, and Consent

The 22 papers spell out the requirement for new laws allowing Jane Doe to live privately in a non-private world:

- Identity
  - Biometrically tied identity to the civil registration at birth
  - Full legal digital identity issued at birth
  - Anonymous digital legal identity at birth indicating it's a human and under age of consent
  - At the age of consent, being given control of their digital legal identity
  - Also, being given the ability to sign documents digitally legally
  - At death, using biometrics, if available to confirm the identity
  - The ability for parents, legal guardians or people with power of attorney to delegate identity of their children, custody person, etc. with their consent
- Data
  - Citizens own and control data about them
  - Create globally agreed upon zones of trust
  - All data shared must be with the citizen's consent
- Consent
  - Different assurance levels for varying levels of trust re consent
  - Laws protecting consent and central consent managed services
  - Informed consent depending on the risk
- Enforcement of the laws
  - Citizens assured their identity, data and consent can be protected regardless of the jurisdiction they're in and others who are in other jurisdictions

Isn't This a Daydream?

Today, the current success rate of cybercrime prosecution in 5%. There's no likely end in sight to nation states creating their own laws and administering them. Given this, isn't the above a daydream? No, and yes.

I am both a visionary as well as an implementor. The paper "Harnessing Technological Tsunami Wave of Change" outlines some practical steps to get countries collaborating.

However, I agree the chances of this occurring anytime soon are remote. Therefore, what practical steps enterprises using IAM can take to address this? Let's begin by looking at several different types of use cases extending from the bedroom to the boardroom.

IAM and Behavioral/Biometric Technology Use Cases

Jane Doe's IAM System

I have a premise, in the not so distant future, due to the technological tsunami wave, each of us will have our own IAM system:

- It may be created ourselves (via things like opensource foundations/companies) or, perhaps offered by telco suppliers, Google, Facebook, Amazon, Microsoft, etc
- We will use it to approve and create who we'll send our identity and data to
- It will also react dynamically with other IAM systems as we come into contact with them virtually or physically
- It also applies to kids.
    - Kids require their parents/legal guardians' permission to provide identity information. Additionally, they must also approve the use of the kids/other's IAM system with fine-grained control
- The result? Effectively, we'll be federating our identity/data with other enterprises
    - I suspect OpenID Connect or, some modified version of it, will be used to federate Jane Doe's IAM system with others
    - There's another option i.e., a "federation hub"
        - It could act on Jane's behalf, with other enterprises
- Given the sheer number of IAM systems Jane will be interacting with, legal automation software will be used
    - It will establish initial contracts between Jane Doe and the enterprises or other people's IAM systems she will be interacting with
- Consent will become a significant issue for Jane to manage due to the sheer number of them.
    - In the paper "Consent Principles in the New Age – Including Sex" I lay out requirements for new age consent laws
    - Given these laws don't currently exist, the use cases below suggest what the IAM systems should do
    - All of them recommend leveraging Kantara User-Managed Access and User-Managed Access Federation
- I foresee a growing interest in enterprises wanting to act as Jane's IAM system on her behalf.
- The personal IAM is also applicable to robots

In the use cases following, I, therefore layout options, including Jane Doe having her personal IAM system.

Bedroom

Jane Doe has virtual sex with one or many partners using behavioral/biometric technology. Her virtual partners potentially live in one or more different jurisdictions and/or are AI generated virtual selves.

Note: The paper "Virtual Sex, Identity, Data & Consent" states what the optimal end-user state should be. However, given this doesn't exist today, here are the challenges the IAM systems need to address:

- Jane Doe's IAM System:
  - The VR environment may or may not offer Jane the option of sharing her behavioral/biometric data beyond the equipment Jane is using
  - If it does, Jane's IAM system should have the ability to:
    - Pass to the VR IAM system her identity information proving she's of legal age according to the jurisdiction in which she lives
    - Authorize the behavioral/biometric data she'll be passing
  - Provide security for the data transferred according to the contract established between Jane's and the VR's IAM systems
  - Coordinate authentication amongst the likely multiple devices Jane will be using for VR, smell, touch, etc.
    - The Virtual Sex paper referred to above, calls out for manufacturers of the hardware/software to leverage behavioral/biometric data to authenticate the person using them
  - Authorize
    - Jane should have the ability to authorize what type of sex is permissible and what type isn't
- VR's IAM System:
  - Use identity assurance to determine:
    - Jane Doe is of legal age of consent AND
    - Her age is sufficient to have sex with other jurisdiction's laws where her partners reside in (i.e., different jurisdictions have different age of consent laws)
    - Record the age of consent proof presentation to the degree required by jurisdiction laws Jane and her partners are in
  - Obtain Jane Doe's informed consent
    - Record and archive the consent as required by jurisdiction laws

- Authenticate Jane
  - When Jane enters the VR sex environment, the technology she's using should leverage biometric/behavioral technology to authenticate her
  - Note: Jane, who is of the age of consent, might want to pass the equipment to her friend Alice, who's not of the age of consent. The hardware/software used should detect it's Alice who's now using it and stop her from using the VR sex environment
  - The authentication should be recorded and archived according to the jurisdictions' laws Jane and her partners are in
- Authorize Jane
  - The VR IAM should offer Jane the ability to select the type of sex she wants as opposed to the kind of sex she doesn't want
    - The AI generated selves should be able to deliver this experience to Jane
  - The AI software should also monitor the sex environment between Jane and her human virtual sex partners to determine and stop when they do something Jane doesn't approve of
- Determining who's who in the VR sex environment
  - Jane should have the option of displaying her name and/or acting anonymously, as do her other partners
  - The VR sex environment should illustrate which partners are virtual selves of humans and which are AI generated
- Replayability
  - The consent Jane agrees to should include:
    - How the session is recorded
    - Where it's recorded/stored
    - Length of storage
    - The ability for Jane, her partners and any others to access this

Home

Jane Doe and her family use behavioral/biometric technology in their home, allowing each of them to determine the others' emotions.

The IAM systems of the not so distant future in the home must meet the following challenges:

- Individual IAM Systems:
  - Identification:
    - Each person living in the home should approve their identities to register with the Home IAM system
  - Authentication:
    - If the person has their IAM system, it should automatically pass their authentication to the Home IAM system
  - Authorization:
    - Authorization data for the use of the Home IAM system should automatically be sent to it
- Home IAM Systems:
  - Identity registration
    - Should be able to register identities dynamically, with their consent, who either live in the home or, enter the house, e.g., kids' friends, visitors, etc.
  - Consent:
    - The Home IAM system should meet local jurisdiction legal requirements
    - Children below the age of consent should require their parents/legal guardians authorization permission for accessing goods/services via the home network
    - There should be some informed consent policy agreed to by adults living in the home and/or parents/legal guardians for children, addressing:
      - What behavioral/biometric data will be allowed to be used in the home
      - How the data will be stored and shared
    - Stronger identity and credential assurance for higher risk consent should be used when required
  - Authentication
    - Should be able to leverage behavioral/biometric technology to authenticate identities
    - The strength of the authentication should vary according to risk
      - For example, the risk associated with someone trying to order food is lower than someone using the home network to enter VR sex environments or access personal sensitive data

- Authorization
  - It may be more complicated than it seems. Why?
  - The behavioral/biometric data can effectively read a person's emotions and do predictive modeling
    - Let's say a person has been sleeping with others without the knowledge of their partners, parents, etc.
    - It's hypothetically possible for the behavioral/biometric system to detect a person is covering something like this up or not answering a question honestly
- **I see the world of "relationships" changing between people as a result of the technology becoming easily accessible and used**
  - There might be times when the home IAM system behavioral/biometric components are turned off

K-12 School

The teacher, their virtual/physical robotic assistant, and the class use behavioral/biometric technology to provide enhanced learning environments.

In the paper ""Kids' Privacy in a Non-Private World" – Why Even Super Hero's Won't Work," lays out how kid's identities, authorization, and consent can apply to schools leveraging new identity, data and consent laws.

Since these don't exist, here are the challenges IAM systems should address:

- Student IAM System:
  - If the student has their personal IAM system, it should address:
    - Identity registration
      - Identity registration likely won't apply to student identity information from their personal IAM system
      - The student's parents or legal guardians should be the ones supplying the school with the child's legal identity documentation
    - Authentication
      - Depending on the quality of the authentication used, the school may or may not accept the authentication from the student's IAM system
    - Authorization
      - Any attributes for which the student is authoritative AND for which the school's IAM system allows, are passed from the student's IAM system to the school's IAM system
- K-12 IAM System:
  - Student identity registration
    - The IAM system should protect the child's identity as they enter AR/VR environments with students and/or teachers in other parts of the planet
      - Any presentation of the child's identity must be with the consent of the parents/legal guardians
  - Teacher identity registration
    - Teachers' identities should be identity proofed against the authoritative government teacher certification source
    - Virtual teaching assistants will need to be legally registered in some fashion within the school and hopefully by an external registration agency
  - Parents/legal guardian identity registration
    - Parents/legal guardian identities should be identity proofed according to whatever local jurisdiction requirements

- Authentication
  - Students/teachers/administrators
    - Should be able to leverage behavioral/biometric technology to authenticate identities
    - The strength of the authentication should vary according to risk
      - For example, the risk from someone regularly entering a classroom is different than a student sitting final Grade 12 exams
  - Parents/legal guardians
    - Should be able to leverage behavioral/biometric technology to authenticate identities
- Authorization
  - Parents/legal guardians MUST provide their authorization permission for:
    - Accessing AR/VR environments
    - Use of behavioral/biometric data within the classroom and/or school
  - The permissions should state:
    - The ability for the session or data to be stored
    - How it's stored
    - How long it's stored
    - Who can view and/or use the data
    - Replayability using the data
- As technology becomes adopted by students coming into the school, school policies will need to be created determining:
  - If a student can use behavioral/biometric data to determine emotions/predictive behavior of their teachers, classmates, administrators, etc. when in the school's environments either physically or virtually
  - The ability of a teacher/administrator to enforce the non-use of these technologies during prescribed times
    - For example, in the future, it's highly likely a student can use technologies like a smart contact lens to transmit exam information automatically and receive answers
  - These policies will need to be enforced by the IAM and school cybersecurity system

Shopping

Jane Doe is walking down a street towards Acme Retail Inc. Acme can tell her emotions via their 360-degree cameras. They can call up any other time Jane has walked by the storefront, if she came in, her feelings at the time, what advertising worked, what she bought, etc. Based on this, Acme can display a customized ad to Jane. An Acme Retail virtual assistant, using predictive behavior modeling, greets Jane at the entrance knowing what to tell her.

Note: This use case is only for one party Jane Doe might interact with as she walks down a street. As the technology deploys, the reality is she'll likely interact with many and then hundreds of different enterprises. Keep this in mind while reading below.

In the paper "I Know Who You Are & What You're Feeling – Achieving Privacy in a Non-Private World," Jane Doe is walking down a street with her friends. As they pass by Acme Retail Inc., it illustrates using different zones of consent, leveraging new identity, data, and consent laws.

Since these tools don't exist today, here are the challenges IAM systems will need to address:

- Jane Doe's IAM System:
  - She will have to configure her IAM system if she wants to broadcast out her identity
    - What the identity is, i.e., a digital identity, will have to be determined by Jane and/or other parties
  - She may or may not have a relationship with Acme Retail Inc.
    - Assuming she does, her IAM system will agree to pass along Jane's consent to Acme Retail Inc's IAM system
    - The type of authentication performed will likely use her behavioral/biometric data
    - Requires initial informed consent from Jane to Acme Retail Inc. (and/or the federation hub if used)

- Acme Retail Inc's IAM system
  - As soon as Acme Retail "sees Jane" walking towards them, they need to be able to identify her
    - Likely use historic behavioral/biometric data
  - Next, the IAM system needs to see if the identity has provided their consent to use their data
  - If not, the IAM system would pass the known identity information to the marketing system which would create a customized ad for the identity as they walk by the store
    - A virtual assistant, leveraging any prior data, would be at the door in case Jane walks in, greeting her anonymously
  - If it does find a consent agreement, the IAM system now formally knows its Jane Doe
    - Jane Doe would have given prior authorization consent for the use of her past behavioral/biometric data and past shopping/buying experiences
    - The IAM system would pass this along to the marketing system to create a tailored Jane Doe advertisement
      - As Jane walks into the store, a virtual assistant would be at the door greeting Jane by name, adapting what it says according to Jane's history and feelings
    - The consent agreement with Jane Doe would also approve the ability to use replay data from prior shopping engagements at Acme Retail Inc.
      - Thus, during this shopping experience, the virtual assistant could potentially "call up" anyone or portions of past replay and use this to display to Jane, leveraging this to increase the chance of a sale
    - Thus, any consent agreement with Jane should specify the following approvals:
      - Length and storage of past shopping experiences including all of Jane Doe's behavioral/biometric data
      - Allowing Acme Retail to share this data with one or many suppliers, advertisers, marketing agencies, etc.
        - Depending on the consent agreement, Jane Doe's identity and behavioral/biometric data can be shared with one or many partners

Healthcare

Jane Doe and her physician agree to use behavioral/biometric technology to monitor her emotions and body functions for the next month. When specific parameters are exceeded, her physician and/or their virtual assistant immediately communicate with Jane, offering corrective advice

The technological tsunami will significantly affect healthcare over the next several years in diagnostics, monitoring, AI virtual physician assistants, healing, etc..

Regardless, here are some of the challenges the healthcare IAM system should address:

- Jane Doe's IAM System:
  - The requirements are the same as used above for retail except Jane Doe's system must interact with the healthcare services IAM system
  - Jane Doe's informed consent
    - The risk of providing consent for Jane Doe's healthcare information is higher than of Acme Retail Inc.
    - In the paper "Consent Principles in the New Age – Including Sex", it states new consent laws are required. Different levels of consent require corresponding increased levels of identity and credential assurance
    - Higher levels of identity and credential assurance should be used until these laws are created
  - Authentication:
    - As the year's progress, it's highly likely Jane Doe's authentication will be increasingly done using behavioral/biometric data
  - Authorization
    - Jane's IAM system will authorize transmission of the agreed upon data to the healthcare provider
    - Jane will agree to accept notifications from the healthcare provider, her physician and/or their virtual assistant

- Healthcare Provider's IAM System;
  - Identity assurance:
    - Use the assurance levels specified by each jurisdiction
    - Legally identify the healthcare virtual assistant
  - Credential assurance:
    - As mentioned above will increasingly use behavioral/biometric data
  - Informed consent:
    - As mentioned above, will use best practices to ensure it's Jane who's providing her consent
    - The consent should include:
      - Specifying the type of data used
      - Security of the data en route from Jane to the healthcare provider's systems
      - Storage standards for the data within the healthcare provider's system
      - Archival policies for Jane's data within the healthcare provider's system
      - The replayability of the healthcare provider using the data
      - Who the healthcare provider is allowed to share the data with
  - Authorization:
    - When certain parameters are exceeded, the healthcare provider will send Jane notifications
      - Within the IAM system, it must allow for automated AI virtual assistant(s) to interact with Jane as well as her physician in real time
    - The healthcare provider's IAM system must enforce the data as per the consent policies agreed to with Jane

Insurance

Jane's health insurance company offers her an attractive lower rate. The requirement is she continuously sends them behavioral/biometric data showing she is psychologically and physically healthy. If she begins to exceed specific parameters, their virtual assistants instantly communicate with Jane offering advice and/or increasing the rates.

Here's what the insurance IAM systems should address:

- Jane Doe's IAM System:
  - The requirements are the same as used above for healthcare except Jane Doe's system must interact with the insurance provider's IAM system
- Insurance Provider's IAM system:
  - The requirements are the same as used above for the healthcare provider's IAM system
- In real time, the insurance provider's virtual assistant(s) and/or their physicians can interact with Jane, sending notifications, advice, etc.
- As per the informed consent agreement, the insurance provider can increase rates in real time if Jane ignores the advice or, has shown over time, she is ignoring the advice
- Jane needs to be careful in entering into these types of agreements on how her data can be shared
- Note:
  - The insurer has a risk Jane Doe might give her monitoring technology to another, who's much healthier, to wear and masquerade as Jane
  - Thus, the technology used must authenticate Jane Doe and detect if another is trying to masquerade as her
    - It's similar to the VR sex example earlier used

Recruiting

Jane Doe's interview with Acme Inc. uses behavioral/biometric technology to determine if Jane is the best fit. The technology also enables Acme to see how Jane reacts under certain conditions.

The use case is for Jane Doe wanting to be hired by Acme Inc. However, in the not do distant future, Acme Inc. might contract with Jane Doe to use her one of her virtual assistants. I touch on this towards the end of the thought paper "Rapidly Scaling Robot Identification?".

Regardless, here are the recruiting challenges for the IAM systems:

- Jane Doe's IAM System:
  - It depends on how Acme Inc. wants to use behavioral/biometric data
    - If they have their own external sensors, there may be no requirement on Jane's IAM system to provide her data
    - Jane's authorization consent is required for her IAM system to pass behavioral/biometric data
  - If Jane's hired
    - Acme Inc. should inform Jane if she is required to provide any of her own biometric/behavioral data will working for Acme
- Acme Inc.'s IAM System:
  - Identity assurance:
    - Acme Inc. will use whatever identity assurance they choose and/or are required by law in the jurisdiction they're hiring Jane
    - If Jane's hired, they will likely increasingly use behavioral//biometrics to identify her
  - Obtain Jane's consent including:
    - Agreement from Jane for Acme Inc. to use behavioral/biometric data as part of the recruiting process
      - Acme Inc. should inform Jane the data used can assist Acme Inc. in determining if she's lying, etc.
    - Storage requirements for Jane's behavioral/biometric data
    - Archival policy for the data
    - Specify who the data can be shared with
    - internally within Acme or, with other partners, etc.

- If Jane's hired:
  - Credential assurance:
    - They'll likely use behavioral/biometrics to authenticate
- Use of behavioral/biometric data within Acme Inc.
  - I can see this growing to become a challenging problem for both Jane and Acme Inc. Why?
  - As the deployment of miniature 360-degree cameras and behavioral/biometric technology increases, Acme Inc. will be become more compelled to leverage this to improve its security based on risk
  - Thus, depending on where Jane physically or virtually goes within Acme Inc., her data might become increasingly used
  - Further, as predictive behavioral/biometric technology improves Acme will likely be compelled to use this for fine-grained access control, calling people into HR for a "chat", etc.
  - How this information is used, shared with, etc. will likely become a growing legal area of interest for both Acme Inc. and Jane
- As the use of this technology increases within Acme Inc., Jane's employment contract and consent should be updated

Boardroom

Jane Doe is negotiating a large contract on behalf of Acme with a supplier's representative. She uses behavioral/biometric technology to understand the reactions of the people with whom she's negotiating.

Beyond the boardroom, behavioral/biometric data can be used at all levels within an enterprise as well as customer interactions with Acme Inc.

In the early days, I suspect many enterprises will use this technology silently when negotiating contracts. However, over time, as the technology becomes widely deployed, I suspect both parties will be using it openly. That's the scenario used for this use case.

Here are the challenges the negotiating supplier's person Jane's negotiating the contract with the IAM system and Acme's enterprise IAM system and should address:

Negotiating the Supplier's Person IAM System and the Acme's IAM System:

- Consent:
  - There should be informed consent given by both parties as to how behavioral/biometric technology and data will be used including:
    - Authorizing data to be sent between each party
    - Specifying external behavioral/biometric monitoring by each party
- Authentication
  - Depending on the consent agreement, both parties might authenticate each other via their enterprise or personal IAM systems
- Authorization
  - Depending on the consent agreement, both parties will authorize for the data to be exchanged in real time
- Storage/archive
  - Depending on the consent agreement both parties may, or may not store the data
  - Storage security, length of time ad authorization rights to view it should be derived from the consent agreement
- Replay ability
  - Depending on the consent agreement both parties may, or may not have the ability to replay the session

Evolution of Today's Use of Biometrics

In today's identification and authentication world, there is a growing reliance upon biometrics to identify and/or authenticate a person, with the belief it's accurate and secure. However, there are problems with biometric accuracy and also biometric readers being able to be spoofed.

Today, there is little independent testing done by external agencies on:

- Equal error rate (ERR) for the biometric as deployed by the vendor
- How easy is it to fraud the biometric reader at the time of sale on each authentication platform?
- After the sale, as time passes and new technology develops, how easy is it to fraud the biometric reader?

Thus, vendors state their claims. Enterprises, trusting it all works as advertised, purchase and deploy the technology,

Does this mean I am against the use of biometrics? No. What I keep in my mind is the hockey stick shaped curve, Pat Scannell, showed me (referenced in the introduction).

The pace of change means today's golden biometric solution might quickly become tomorrow's turd.

Enterprises should mitigate their risk by:

- Leveraging AI to monitor not only authentications, IP address, etc. but also what the person does
    - This will reduce risk from criminals masquerading as the person using spoofed biometrics
- Ask biometric vendors for independent verification of the ERR and reader spoofing
- Conduct semi-annual risk assessments on the technology used, looking for weaknesses due to the rapidly changing technology
- Change out authentication platforms based on the risk assessment

Without this, an enterprise IAM infrastructure might become unknowingly weaker until it's too late.

I see an evolution from the use of biometrics today, to behavioral/biometric patterns. These will likely be more accurate than today's biometrics used on their own. However, as with all technology, there is a cat and mouse game with criminals.

As the use of behavioral/biometrics comes into play, criminals will want to find ways to masquerade as another using the technology. Therefore, as pointed out above for biometrics, independent testing agencies should be created which:

- Provide ERR for the behavioral/biometrics used
- Determine how easy it is to fraud existing hardware/software used
- Continually test old hardware/software to see if new technology makes the old one prone to being able to be spoofed

Caveat emptor when it comes to believing what the technology sales reps tell you.

IAM, AI & IoT- Reducing the Attack Vectors

The rapid rise in the number of IoT (internet of things) devices also increases the amount of attack vectors into and within an enterprise. In the SCADA world (supervisory control and data acquisition) the last several years have seen the rise of IoT gateways to mitigate these risks (e.g., Cisco, etc.). Outside these gateway systems, the challenge is there are billions of other IoT devices, many of which are insecure. These can connect to supplier/partner networks and hence act as a gateway into secure enterprise systems.

From the 100,000-foot level, here are the challenges IAM/AI should address:

- Identity registration
    - An enterprise connecting an IoT external device to its network should insist the IoT device have a digital certificate with which to register the device
    - The device's owner should agree to informed consent as part of the registration process covering things like security and data standards, terms of use, etc.
        - I see this process becoming automated using legal automation software
        - Data standards are essential to mitigate the risk of malicious malware inserted into the data
    - One of the problems with IoT devices is weak security within the device
        - Depending on the risk level from the IoT device, enterprises should determine if the device security meets a minimum standard
        - This requires, as part of the registration workflow, obtaining acceptance from the IoT's owner to test it rapidly
    - IoT firmware updates
        - Many IoT devices have weak firmware updates
        - Depending on the risk from the IoT device/data to the enterprise this may or may not be a risk
        - If so, the enterprise should:
        - Record the IoT firmware device information
        - Monitor any changes to the firmware by the manufacturer, taking steps, if warranted, to either test or deregister the device
    - Outdated IoT components
        - As time passes, IoT device components may become insecure (including the deprecation of software, etc.)
        - Depending on risk from the IoT device/data, the enterprise may want to:
        - Monitor device usability
        - De-provision the IoT device as and when required
    - Weak physical hardening for the IoT device
        - Many IoT devices have inadequate physical hardening
        - Depending on the risk level, if it's known to be insecure, an enterprise might not register a device

    - Weak IoT device management capabilities
        - Many IoT devices have weak device management capabilities including but not limited to systems monitoring and response capabilities
        - Depending on the risk level, an enterprise might not register a device, if it's known to have weak device management capabilities
    - IoT device's identity should register it in an enterprise's identity graphing database
        - The data should include all relationships for the device, its owner and the enterprise
    - One of the challenges with IoT registration is deprovisioning the device
        - How will the enterprise determine the device is no longer working, been sold to another party, etc.?
- TLS layer
    - The enterprise should mandate:
        - Version(s) of TLS supported
        - Within each version, which algorithms are supported
        - Security standards used
- IoT authentication:
    - What authentication measures will be supported?
    - AI should be used to monitor this, looking for any discrepancies
        - It should be looking for things like IP location, time of day, frequency of usage, etc.
- Archiving IoT device registration, authentication, authorization and data
    - There will likely be different levels of risk for various IoT devices
    - Depending on the level of risk, different archival policies should be implemented for the IoT device

- IoT authorization:
  - The enterprise should address the following:
    - The IoT data should initially flow into a self-contained DMZ part of the network. AI should analyze:
      - The data, looking for malware and/or false data to mislead the enterprise's systems
      - The DMZ endpoints should be secure, resistant to denial of service attacks, and continually well tested
    - In real time, once the AI's finished with analysis, the data should be securely sent within the enterprise to be used and recorded
      - All points the data flows through the network should be encrypted with attention paid to endpoints within the enterprise where possible attacks can take place
    - The enterprise's IAM system should authorize the
      - Use of IoT data for applications and/or people
        - AI should be monitoring the apps and people's use of the data looking for any irregularities in data usage
- **The sword cutting for you can also cut against you**
  - IoT devices can also be used against the enterprise
  - Thus, management and the cybersecurity teams should continuously be reappraising their IoT security architecture components

Robotics Are Here

The paper "I'm Not a Robot!" discusses the emerging robotic revolution. It gives examples of physical robots as well as virtual ones, like Oben. Last Fall, I began to ponder how we'd identify them?

I wrote a paper "Legally Identifying Robots (Robot Identification)," suggesting the use of a new age civil registration system. Vint Cerf, the inventor of the internet (TCP/IP) liked it and asked me how we'd identify robots at "insane" speeds? This lead to a thought paper, "Rapidly Scaling Robot Identification?"

It proposes:

- Automating much of the process
- Requiring all jurisdiction's new age civil registration systems to instantly be searched to verify the robotic identity didn't already exist.

A month ago, I created an OWASP (Open Web Application Security Project) Robot Security Project to begin addressing this.

This paper assumes nothing exists today to identify robots legally. Therefore, here are some sample use cases to consider:

- A robot is moving down a street. A person walks into it, falls and claims the robot is to blame, wanting to sue the robot owner
- A robot is serving food in a restaurant and spills some hot soup over a person. The person wants to lay civil charges against the restaurant
- A robot in a pharmacy fills out a medication order for a person. The person becomes ill after taking the medication and sues the pharmacy claiming the robot made a mistake in the prescription
- A patient in a nursing home claims a robot injured her.
- A virtual robot, acting on Jane Doe's behalf withdraws money on behalf of its owner. The robot disappears. It was masquerading as another robot. The bank claims it authenticated the robot and isn't liable for the robot masquerading as another. The person sues the bank.
- Jane Doe has virtual sex with two partners in a VR environment. One is representing a human in another jurisdiction, and the other is AI generated. Jane claims she was mentally and/or physically abused and wants to press criminal and/or civil charges.

The first four either exist or, are coming into existence at this time. VR sex and banking examples don't exist yet.

Here are some IAM challenges the use cases illustrate:

- Robotic identification
  - How does an enterprise identify physical and virtual robots it either owns, interacts with, or serves its customers?
  - Is it unique, and can it stand up in a court of law?
  - How does the robotic registration tie to who owns the robot?
- Robotic authentication
  - How are robots authenticated?
  - For virtual robots, one solution for this is "Project PAI."
    - It leverages blockchain
    - However, it relies on a private/public key pair
    - The recent financial history of using this suggests the security is only as strong as how the secret key is stored
- Robotic authorization
  - How is the robot authorized to act on a person's behalf?
- Robotic movements
  - How can an enterprise or robotic owner claim where their robots are at each point in time?

In the not too distant future, robots, both virtual and physical, will likely be leased to others, or do contract work on our behalf. **Imagine a world where there are tens of millions of physical robots and hundreds of millions or more of virtual ones. They'll create challenges a whole new aspect of IAM and law should address**.

Recently, The Chinese University of Hong Kong "Machine Lawyering" recently published a blog on one of my papers illustrating this. In "The Identity Lifecycle of Jane Doe," I have a young Jane acquiring both virtual and physical robots before she's of legal age. She changes her gender. In his old age, she requires others to act legally on his behalf, and he dies.

Throughout the paper, I show how robots are identified and managed. In the end, I pose several challenging questions:

- The lifespan of virtual and physical robots will likely be much longer than the lifespan of John
- Can John's virtual robots exist perpetually?
- If repairs are made to robots, allowing them to live perpetually, how does this affect the identities of John's robots?
- When do John's robots cease being his robots?
- What if John's robots create copies of themselves either virtually or physically?
- What if John's robots create new robots, virtual or physical, without John?

Finally, there's robotic singularity. In 1989 in Star Trek, the TV/movie series, there was a computing race called the "Borg" who operated in singularity. As singularity develops over the next decade, how will it be managed by IAM, laws, and contracts?

Cloning/Biorobotics is Coming

Cloning

In 1996 Dolly the sheep was the first cloned mammal. Fast forward to today in China, where Boyalife currently clones 100,000 cows a year working towards 1 million. In 2015, their CEO publicly stated they could clone humans but weren't. In 2017, the Economist published a spoof article imagining how the world would learn of the first human clone. Thus, the age of human cloning in now almost upon us.

In 2006, I published my first paper, "The Challenges with Identity Verification," in which I suggested DNA be used at birth as part of a birth registration enabling differentiation of clones. I took criticism from this from others who didn't like the idea of governments using a biometric able to profile people, e.g., DNA. After reflection, I agreed.

Our existing civil registration system, the source of legal truth for a person's identity, is now outdated. It uses technology from the 1800s, i.e., paper, to tie an identity to the person.

Due to low-cost technology, e.g., printers, it's relatively easy to fraud a birth certificate. That's why, in security circles, birth certificates are called "breeder documents." With a birth certificate, one can obtain other identity documents higher up the identity chain, e.g., driver's license, passports, etc.

Rethinking the Civil Registration Systems Globally

This past year I wrote, "Why The New Age Requires Rethinking Civil Registration Systems." It states, as part of the birth registration process, fingerprints should be obtained at birth and iris during the child's first year of school. All of this is subject to research confirming the ability to differentiate clones, as well as research confirming the usage of fingerprints from babies.

I also wrote "What New Age Civil Registration Systems Won't Do" outlining how the system should be built to ensure a citizen's privacy.

The papers propose:

- Biometrically tied identity to the civil registration at birth
- Full legal digital identity issued at birth
- Anonymous digital legal identity at birth indicating it's a human and under age of consent
- At the age of consent, being given control of their digital legal identity
- Also, being given the ability to sign documents digitally legally
- At death, using biometrics, if available to confirm the identity
- The ability for parents, legal guardians or people with power of attorney to delegate identity of their children, custody person, etc. with their consent.

Then there are biorobotics…

Biorobotics

"Biorobotics may make robots that emulate or simulate living biological organisms mechanically or even chemically, or make biological organisms as manipulatable and functional as robots, or use biological organisms as components of robots." - Wikipedia.

It's a relatively young part of science. It ranges from medical applications, illustrated by this article "More Than Meets the Eye: The Future of Bio-Robotics" to applications like "cyborg insects'(read the section 'Cyborg Insects' in the paper "Privacy Gone – AI, AR, VR, Robotics and Personal Data").

As medical applications unfold, the robotics used will also need to have their identities registered, authenticated and authorized.

As insects become used by enterprises to do things like surveillance, etc., their identities need to be registered, authenticated, and authorized! The sheer number of these, having potentially different relationships, will likely require the use of an IAM graphing database. With insects short lifespan, it also means ways have to be found determining when they are no longer alive. This should result in changing their status within the IAM system.

Then there's the science fiction future…

Is it Still Science Fiction?

For the last few years, I've been wondering when science will be able to create the following:

- Grafting/creating onto an existing human, biometrics from other humans?
- Grafting/creating onto a robot, biometrics from other humans?

There is a significant financial, military reward from this type of technology. It will render useless our existing reliance upon biometrics as identification and/or authentication mechanism. People who can do this can likely successfully masquerade as another.

Enterprises should thus keep a close eye on research literature looking for early signs of the ability to graft/create biometric on either humans or robots.

Tsunami Wave Cybersecurity Centre

The 22 other papers I've written illustrates how the incoming technological tsunami wave creates many new opportunities for enterprises to offer goods and/or services. It also shows how it's not just one technology to focus on, BUT the result of the convergence of AI, AR, VR, robotics, genetic engineering, nanotechnology, and wireless. As they crash together against the enterprises IAM shores, it also offers criminals many new attack vectors.

Therefore, the challenge to an enterprise is how to:

- Mitigate risk from the attack vectors based on risk assessment
- Daily, continually update the attack vector risk assessment

I like the statement Justin Trudeau made at this year's Davos meeting. "Think about it: The pace of change has never been this fast, yet it will never be this slow again." It captures the dilemma of trying to keep up with the hockey stick shaped curve Pat Scannell showed me (referenced in the introduction of this paper).

It leads to a premise about cybersecurity centers. It isn't feasible for most enterprises to run them on their own. Why? The attack vector surface is too large, the expertise required is limited, significant resource requirements and the pace of change increasingly fast.

Given the above, here's what I think will evolve over the next few years regarding cybersecurity centers:

- Medium to large enterprises will deploy and/or enhance their cybersecurity centers
    - They'll include all components of the technological tsunami hitting their virtual and physical perimeters
    - When they don't have the resources or expertise to do continual research, testing, etc., they'll outsource this to other specialists
        - An example might include behavioral/biometric
            - The service would not only test the efficacy of the technologies but also look for ways to fraud it
- **Small to mid-sized enterprises, will increasingly outsource their cybersecurity defense**
    - They don't have large budgets, people, expertise, and knowledge to in effect "staff the barricades."

IAM is at the heart of the cybersecurity center. Determining, on a second by second basis, who is trying to do what, with what approvals, is critical. Learning if an attack is being coordinated by using AI, robots, masquerading as someone else, etc. is key to an enterprise's security and their future.

Global Identity Digitization is at Risk

In many of my past engagements, I have been the instigator to deploy high availability. Why? Identity was the first project requiring it.

Therefore, a year ago, while writing papers suggesting the use of Sovrin/Blockchain as part of the identity solution, I asked myself a dumb question. "What would stop the blockchain solution from working?" Answer – a sun geomagnetic disturbance (GMD) causing an electromagnetic pulse (EMP).

In 1859, a sun GMD EMP event occurred called the "Carrington event". It brought down many telegraph systems in both hemispheres of the planet. **What are the chances of this occurring again? 1 in 8 THIS DECADE.**

There is another type of EMP event called a High Altitude EMP or "HEMP," caused by a high-altitude nuclear explosion. Studied in the 1960s by the US and Russian military, it damages/destroys electronic grids. It contains an additional energy component than the GMD generated one which can destroy data within a data center.

The US Government has studied the effects of an EMP or HEMP event occurring today. Their estimate? Loss of life, post-event up to 90%! Why?

Either one would burn out transformers in the electrical grid. There is a limited number of transformer manufacturers AND, it takes time to make each one. Thus, given the digitization requiring electricity, we would likely be in the literal 'dark ages" for many years. Most things would stop working, resulting in people starving, etc.

Good news – the technology exists to address this. So, you're likely thinking, "Surely there's a plan addressing this? Answer – No. Why not? It costs LOTS of money and requires governments to lead and spend the money.

In the US, there's a group "Secure the Grid Coalition," which has been very actively lobbying the US government to act. Recently in March, the Whitehouse issued an "Executive Order on Coordinating National Resilience to Electromagnetic Pulses." It's early days of at least beginning to create a plan.

The rest of the planet? There is little action. There isn't any "Secure the Grid Coalitions" in most other jurisdictions. So, while we as a planet madly digitize, including IAM systems, we are putting ourselves in potentially mortal danger.

I wrote a paper "When Our Legal Identity Trust Goes "Poof!" in which at the end, I recommend some common sense steps for enterprises to take. **At a minimum, GMD EMP/HEMP should now be on the enterprise risk register.**

The end of the paper makes several practical recommendations. One of them is enterprises asking their data center suppliers to prove their data centers can withstand GMD EMP or HEMP events. While cloud suppliers are working away at creating EMP proof data centers, today, many data centers aren't EMP/HEMP proofed.

All the components of the technological tsunami striking our planetary shores require a secure, stable electrical grid. As someone who's been the instigator of highly available systems, a 1 in 8 chance this decade, is a relatively high number. Enterprises should be lobbying their respective governments to at least get a plan together addressing this.

Summary

I selected the picture at the beginning of this paper for a reason. It's a person, holding an umbrella, standing in a growing puddle of water, watching a large tsunami wave approaching them from in front and their sides. The analogy is it's us, holding up our old school IAM systems as our umbrella. Meanwhile, all around us, the technological tsunami wave is rapidly approaching.

This paper illustrates why the IAM umbrella we're using to protect ourselves no longer works with the incoming tsunami wave.

I'm not belittling the existing IAM industry. However, the toolset we use today isn't going to work well tomorrow. We need new laws providing us with new age legal tools for identity, privacy, and consent, enabling us to live privately in a non-private world.

This paper, unlike the other 22, assumes new laws not coming any time soon. Therefore, it focusses on the challenges, offering advice on how to meet the new age requirements.

The hockey stick shaped curve of change Pat Scannell showed me, requires a comprehensive, multi-faceted approach with the ability to rapidly change. It should include:

- Graphing databases
- Behavioral/biometric identification and authentication
- Strategies addressing biometric ERR rates and reader spoofing
- Rethinking IOT using IAM and AI
- Having a virtual and physical IAM robotic strategy
- Getting ready for cloning and biorobotics
- Expanding scope for cybersecurity centers and/or outsourcing portions of them
- Adding GMD EMP/HEMP to risk registers and ensuring existing data centers are EMP proof

As stated in the introduction, this paper is a summation of my many years of experience leading complex identity projects. I believe the tsunami wave will make these past projects look like child's play.

The waves are now almost upon us. We need to build new IAM dikes to channel the incoming waters safely and securely.

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.