

When Our Legal Identity Trust Goes “Poof!”



Copyright: 123RF Stock Photo

Author: Guy Huntington, President, Huntington Ventures Ltd.

Date: Updated November 2018

TABLE OF CONTENTS

NOTE TO READER:	3
When Our Legal Identity Trust Goes “Poof!”	4
Electromagnetic Pulse Event (EMP)	4
It’s All a Matter of Risk	4
A BIG RED FLAG	4
Planning, Laws and EMP Proof Data Centres	5
It’s Not A Question of If, It’s a Question of When	6
About the Author	7

Note to Reader:

I have been writing about rethinking civil registration systems since 2006

- [“The Challenges with Identity Verification”](#)

Over the last several months, I have written 11 papers about:

- New laws required to do this
 - [“Why We Need to Rethink Our Vital Stats Laws”](#),
 - [“Why Your Digital Consent Matters – Including Sex”](#)
 - [“Why We Need New Biometric Laws Protecting Our Privacy”](#)
- What the new age civil registration/vital stats service does and doesn't do
 - [“New Age Vital Statistics/Civil Registration Services: What They Do and Don't Do”](#)
- 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”](#)
- Protecting the civil registration/vital stats infrastructure
 - [“When Our Legal Identity System Goes “Poof!”](#)
- Separating vital stats services/databases from other identity authentication services
 - [“Architecture Summary”](#)
 - [“Creating Estonia Version 2.0 – Adjusting for Changes From 1999 to 2018”](#)
- Rethinking identity assurance using new age vital stats
 - [“New Age Identity Assurance – Turning it on its Head”](#)
- Rethinking Civil Registrations in Remote Locations
 - [“Where Shit Happens - Rethinking Civil Registrations in Remote Locations”](#)
- New Age Civil Registration/Vital Stats Design, Implementation & Maintenance Vision
 - [“Guy's New Age Civil Registration/Vital Stats Design, Implementation & Maintenance Vision”](#)

This paper deals with EMP proofing data centres for legal identity data.

All papers are available at my website <http://hvl.net/papers.htm>.

When Our Legal Identity Trust Goes “Poof!”

We are quickly constructing a world where we are digitizing our legal identification of identity, i.e. birth, name/gender change, marriage and death registries and biometrics to verify and authenticate an identity. If the underlying data was destroyed, it would result in a collapse of our legal identity system. **What are the chances of this system going “poof”? Actually, they’re quite high.**

Electromagnetic Pulse Event (EMP)

In the mid 1800’s there was a major electromagnetic pulse event from the sun. Called the “[Carrington Event](#)”, it caused widespread electrical damage. If this event was to occur today, it would likely wipe out most of the earth’s electrical grid. It may or may not wipe out data centre data. A smaller event, “[The Railroad Storm](#)” in 1921 occurred affecting telegraph equipment. We narrowly avoided a similar storm in 2012. Thus, the risk is high that we will experience a similar event within our lifetime. **NASA estimates it’s about 12% this decade!**

Then there’s the risk of a high altitude EMP nuclear attack. This type of attack emits some additional energy waves that will wipe out data in datacentres unless they are EMP proofed.

Readers should view this video, by Frank Gaffney, in 2017, for a US perspective on these types of attacks (<https://securethegrid.com/a-must-see-briefing/>).

It’s All a Matter of Risk

Enterprise executives analyze the chances of an event occurring against the expected outcome and then weigh it against what they could instead spend their money and time on and the expected outcomes from this. Decisions are made based on the risk.

In today’s world, digitization decisions are made to reduce costs and offer new and/or faster electronic services to citizens. New technologies such as Blockchain and Sovrin offer citizens the ability to control most of their identity (refer to “[A Modern Identity Solution](#)”). These solutions rely upon the use of many thousands of servers around the planet.

Yet the risk of a business executive making decisions is different than that of a government leader whose government is responsible for documenting, storing and attesting that an identity document is true and legal. Without these documents, the underlying system of identity trust which makes the world operate won’t work. Thus, the underlying legal trust risk is extremely high from an EMP event.

A BIG RED FLAG

An EMP event is a big red flag. It will happen again. After an EMP event, those who survive, will need to rebuild their legal and economic systems, using the underlying identity verification data. Governments bear a responsibility to their citizens to ensure the data will survive and remain intact. So, what can be done to prepare for this big red flag event?

Planning, Laws and EMP Proof Data Centres

Governments and third parties like banks, telcos and insurance companies, need to pause in their digitization efforts to see what the effects would be today, if an EMP event occurred. They should determine the following:

- Survey:
 - What electronic data exists within EMP proof data centres and which resides in data centres that aren't EMP proof
 - They should assume that the non-EMP proof data centre data is lost
 - For the non-EMP proof data, they should then determine:
 - If any paper-based records exist
 - Time, effort and cost required to reconstruct new electronic records from the paper-based ones
 - Temporarily halt plans for digitization of identity data until it can be determined that the data will be stored in an EMP proof data centre
- Publish:
 - Governments should publish the result of their findings such that citizens now know the potential effects of an EMP event upon their identity data
- Plan:
 - Governments should plan for EMP proof data centres to occur as soon as possible to hold identity verification data
 - The plans and costs should be made public
- Legislate:
 - Governments should legislate that any core identity verification data must be stored in EMP proof data centres
 - [This should include vital stats/civil registration data such as certificates for birth, name/gender change, marriage and death](#)
 - Governments should review legislation regarding financial, telcos and insurance companies and determine the requirements to store sensitive identity data to be stored in EMP proof data centres
 - It might be useful for legislation to require these entities to publish if identity data of their customers is stored in EMP proof data centres
- Implement:
 - Governments should prioritize spending such that EMP proof data centres are implemented as soon as possible
 - This might mean revamping existing data centres and/or building new ones
 - Third parties, such as banks, telcos and insurance companies should be “encouraged” to rapidly move to EMP proof data centres

It's Not A Question of If, It's a Question of When

An EMP event will occur again. It's only a question of when it will occur. In the mid 1800's, when the last major EMP event occurred, it disrupted telegraph systems. Yet, because society then wasn't as reliant upon electronic transmission and storage, it didn't stop most life from occurring. Consider today...

We rely upon our electrical grid and millions of different electronic components to store and move our data. Our cars, planes, trains et al rely upon electronics. Our movement of goods and services rely upon electricity as well as systems that produce and send traditional energy like gasoline. Our water and sewage are all dependent on electricity.

This type of event will severely disrupt us, causing loss of life and taking likely years to recover. We, as a society, need to prepare for these events.

There's some good news. This risk can be mitigated by governments and industry investing in similar technology that militaries have been using to harden systems for the last couple of decades.

One of the first places to begin is with our underlying legal identity trust systems. This can be done relatively quickly in comparison to upgrading the entire electrical grid. It's time to quickly survey, publish, plan, legislate and implement for this.

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."

