PNWER Working Group Session Report

Working Group: Innovation
Meeting Date/Time: Tuesday, July 24, 2018 - 9:15am

Co-chairs:
- Senator Mia Costello; Alaska Legislature
- Nirav Desai; Senior Partner, Moonbeam
- MLA Rick Glumac; Parliamentary Secretary for Technology, BC

The agenda, speaker bios, and presentations from this meeting can be found on the PNWER website under ‘Past Events’ http://www.pnwer.org/past-events.html or at http://sched.co/DYMy

Summary of Meeting:
Welcome and Introductions
- Opening remarks by Sen. Mia Costello on the importance of innovation in Alaska
- MLA Rick Glumac on embracing and growing the tech sector in BC
  - Innovate BC provides support to startups
  - BC’s Supercluster

Targeting emerging technologies to achieve more efficient delivery of gov’t systems
Drummond Reed; Chief Trust Officer, Evernym
- Self-Sovereign Identity (SSI)
- Why are we (potentially) finally able to solve the issue of online identity and anonymity? [this is a 20+ year old problem]
  1. Siloed (Centralized) Identity
     - You do not exist on the internet until you make an account on a network
     - There is no real way to prove you exist as a real person
  2. Third-Party IDP (Federated) Identity
     - You have one account with an identity provider, and they verify that you are a person
     - Inside one system, you are verified
     - This system is not portable though
       - If you’re using Facebook to log into other services or apps, and you delete your Facebook, then you cannot access the other things you used that account to access
  3. Self-Sovereign Identity (SSI)
• Taking control of your identity, being empowered on the internet, owning and controlling your identity for life
• You connect directly with the parties (person, organization, thing) you interact with
• There is a verifying party that will essentially certify that you are supposed to access what you need to
  • Driver’s license → have the DMV issue a license that ends up on your phone/device, so TSA can easily know that you are who you say you are because your license was issued by an accredited authority
  • Only certified authorities can issue verifiable certificates
  • Blockchain solves the issue of digital signatures (Public Key Infrastructure) → Decentralized Identifiers
  • No more usernames or passwords
• Emerging open standards for SSI
  • There is work going on with this
• How long until we see this in the public sector?
  • Hopefully within the next few years. Early 2019 is when the first few things will be rolled out
  • Organizations like sovrin.org and others are focused on maximizing control of personal data by the individual who the data belongs to

Pamela Dingle; Director of Identity Standards, Microsoft
• The data about you is on different apps, and is not owned by you. You don’t know where it is, what it’s being used for, etc.
• This is a problem that Microsoft is seeking to address

Carol Prest; Registrar and Executive Director & John Jordan; Executive Director, Ministry of Citizens’ Services, Government of British Columbia
• The government of BC is working on ways to implement these kinds of blockchain-backed certification and verification structures
  • Currently working with using this technology to streamline the business licensing and verification process, but plan to eventually expand it to address other citizens’ services
• A ‘bootstrapping technique’ is needed here
  • Public community holder, [TheOrgBook] which will allow registration etc. which will communicate digitally signed and sealed verified claims
• Selective disclosure will allow verifiers to see only the information will need to be seen

Questions:
• How might you be using this application for border security and I-9 requirements?
  • Reed:
    • Part of the R&D standards has been sponsored by the Department of Homeland Security because cross-border issues are hugely important. All of the benefits that apply to what we talked about earlier apply to border crossings. The benefit of using digital credentials is the ability to revoke them in real time, which is hugely beneficial to the border crossing process
      • Allows for verifiable supply chains at border crossings
  • Glenn Cosby: I want to know about how identity theft came about in the current cyber realm we live in? How is this new technology going to be better than the current regime we live under?
    • Jordan:
      • With current technology, you can’t fake the public keys. We can technically know for sure if something (a certification, for example) gets transferred from A to B
and isn’t revoked. Organizations that are accredited, will stay accredited, but the accreditation will transfer over to being online, creating webs of trust

- Prest:
  - Right now, there are challenges with businesses knowing if other companies are in good standings. There is no way to verify if other businesses are reliable, and this technology hopes to help address this issue

- Reed:
  - Identity theft exists today because the thieves can access your data; data about you can be used to verify that you are you. This will change because only you will be in control of the cryptographic signature, which will not be accessible to anyone else
  - Something I’m surprised no one has asked: What happens if I lose my phone?
    - The information can be backed up and encrypted, and there is also Social recovery (ppl or institutions you trust to help you backup and recreate your profile if something happens to your device)

- Dingle:
  - There will be fraud, but it will be easier to see how fraud is happening because there is more of a record

- There are industries where chain of possession is important, including transferring people from one place to another. Is there work going on in this field? How far along are they?
  - Reed:
    - Yes, DHS and customs border control are interested in this, especially with food supply chains.
  - Jordan:
    - 1. We haven’t started it yet, but chains of evidence in the justice department is something that we’re thinking about.
    - 2. We are not going to be bound to limited time on things like driver’s licenses because they will be reverified every time you use it
  - Prest:
    - What we’re doing is printing to another site, but allowing the corporate registry to keep control of the data, allowing people to maintain the integrity of the data through the registry

- Glumac: are there other places/agencies in the US or Canada where there is room for collaboration with this?
  - Jordan:
    - Yes, we are working to create ‘software products’ that others can use, and we want to make sure that everyone maintains their issuance authority, and make it as easy to have them join the network. We are open to collaboration
  - Reed:
    - There are many collaboration opportunities, but the largest push for SSI is from Europe (Finland, Estonia, Sweden, Austria) in addition to several US states (Illinois, Arizona and Maryland are leaders). However, BC is the most innovative and the fastest at developing tech/software to address these issues

Panel Concludes

Dealing with privacy concerns: How does government and business ensure privacy while delivering gov’t services

Anand Vadapalli; Chief Executive Officer & President, Alaska Communications
• There are a variety of threats that face citizens in the cyber sphere, and the government must respond as a regulator, a policy maker (on the state and federal level) and as a provider of services
• In the past, and even today, we have given away our privacy for “free” services
  • This business model will have to change, and we as consumers have to be more aware that this is what we are doing

Mark Masongsong: CEO and Co-Founder, UrbanLogiq
• We as data companies are asking you, the legislators, to regulate us
• Companies can track the signatures of different cars, which is alarming, but can also provide some benefits, especially in rural communities that don’t have smart road sensors
  • We can still predict traffic patterns and infrastructure issues
• We need to bridge the gap between companies discovering patterns through this data, but ultimately, should they have access to it?
  • There are currently no rules, but UrbanLogiq is really concerned about this, and has integrated blockchain into their platform while implementing GDPR-style laws
  • However, GDPR and Blockchain are diametrically opposed
  • Specifically the GDPR’s ‘right to be forgotten’ versus blockchain’s ‘immutability’ or the ability to never be forgotten. So how do we bridge this gap?

Bill Tam; Co-Chair, Canada’s Digital Technology Supercluster
• The global economy is undergoing a fundamental shift. Data is the new ‘big thing’. Industries are being created and disrupted by data, data mining, etc.

Michael Farber; Founder, Ratio Innovation Management
• How do we navigate the balance between citizen consumers and government commerce? Between law, policy & regulation, and technology
  • Perhaps by looking into how citizens should be aware, control their risk, and make better choices with their data while the government must be clear about intent, have oversight, and good ethics.
• Presentation can be found here: https://schd.ws/hosted_files/2018pacificnorthwesteconomicregi/9b/Michael%20Farber%2C%20Ratio%20Innovation%20Management%20-%20Presentation.pdf

Questions:
• George Caan, Washington PUD association: Given what you’ve talked about, all the data and the spectrum of ethics present there, are we going to have to change our definition of what we expect for privacy?
  • Masongsong:
    • We have to accept past change. We might have to move our ideology from talking about who controls data, to how we can punish those who misuse data. The data is already out there, so it’s a lost cause. How can we as a society identify ways to punish misuse of data and identity? That is the real question
  • Farber:
    • Yes. Privacy means something different today than it did 20 years ago. There’s just so much more data than there was before, and anonymizing data is a way to perhaps enforce segregation and discrimination, so we have to keep that in mind, but it’s not the best solution
• Maralyn Chase: So suppose we were to adopt the EU’s rules on privacy, would any of you still be in business?
  • Vadapalli:
Yes, we would still be in business. Philosophically, I’m a big believer in personal choice, and we will have to answer questions about what data we’re willing to trade for the services we are given. As long as you are given control over your data, you have that choice. Right now, you don’t have much choice, so security data and verifying who you are will enable you to take back that choice over how others use your data.

Masongsong:
- Yes, we are GDPR compliant, especially because our investors realized that the things we’re doing might be illegal in 7 years. However, GDPR is in some ways already out of date. By the time they come up with GDPR, technology had already moved on.

Derek Morrison: Voting on issues and issue-based governance is hugely important to millennials, and being able to act on issues in real time is very critical. So do you think we can address the needs of the people in real time, interact with government, and empower digital democracy with these kinds of systems? What’s happening in that space?

Farber:
- There is a lot going on right now in the US to try to connect the people to their government through these kinds of things and exchanges. Not quite at the digital vote level (as far as I know)

Vadapalli:
- Not enough is being done, but that is why it is important that we’re in panels like this that involves government officials

Panel Concludes

Action item:
- Mechanisms that can be employed for feedback so that companies don’t have to regulate themselves on their own, and won’t be held accountable by an organization that doesn’t actually understand the tech
  - Tam:
    - innovating on the trust model. All of the questions around feedback center around verification → we don’t have a good idea of what a trust model really looks like on a larger scale
    - It’s hard to manifest itself bc we don’t have a baseline yet
  - Masongsong:
    - if you try and regulate the way tech works, you will lose the battle. The only way we can regulate, is to regulate the behavior that should be banned → keep anonymized data anonymized, b/c if you’re not careful, and you’re layering data, you can do really invasive things even if you didn’t intend to. We do not provide our analytics to the private sector, only to the government. GDPR is a good first step, but we should look to regulating behavior instead of the technology itself
  - Farber:
    - the notion of government and commercial should fall under high degrees of scrutiny. Data can be exploited by both sides if people are not super careful with the data

Notes taken by Elizabeth Mayer
## Action Items and Findings:

<table>
<thead>
<tr>
<th>Number</th>
<th>Action Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Conduct a study/Share information across states/provinces on how each handles data privacy and associated legislation (GDPR). Assemble a common body of knowledge on this topics</td>
</tr>
<tr>
<td>2</td>
<td>Promote the US Navy Hack the machine event in Seattle on September 21-22 Coordinate a call with AK, WA and OR on potential Navy Future Command in the PNW with PNWER maritime cyber task force</td>
</tr>
<tr>
<td>3</td>
<td>Investigate development of a White Paper on state verified identities leveraging block chain tech - Lessons learned and best practices from BC and Others</td>
</tr>
<tr>
<td>4</td>
<td>Update PNWER's Innovation assets Map of the PNW</td>
</tr>
<tr>
<td>5</td>
<td>Plan a session to Investigate mechanisms for ethical use of technology for Big Data (deep learning and AI) and coordinate with our universities in PNWER jurisdictions</td>
</tr>
</tbody>
</table>

### Findings

1. BC Government is leading on government utilization of Blockchain Technology