STATE · 2025

TRANSCRIPTS

State Endorsed Digital Identity Summit 2025

A complete transcript of every recorded talk from the State Endorsed Digital Identity Summit.

Contents

Full transcripts of all 22 recorded sessions, in the order they appear in the archive.

01	**afternoon-00-10-05--00-16-06-Alan-Fuller**	*afternoon-00-10-05--00-16-06-Alan-Fuller*	05:52
02	**afternoon-00-16-06--00-26-12-Scott-Perry**	*afternoon-00-16-06--00-26-12-Scott-Perry*	10:05
03	**afternoon-00-26-28--00-44-25-Timothy-Ruff**	*afternoon-00-26-28--00-44-25-Timothy-Ruff*	17:57
04	**afternoon-00-45-26--01-02-47-Thomas-Mayfield**	*afternoon-00-45-26--01-02-47-Thomas-Mayfield*	17:19
05	**afternoon-01-06-53--01-10-02-Utah-Life**	*afternoon-01-06-53--01-10-02-Utah-Life*	03:12
06	**afternoon-01-11-15--01-21-17-Steve-McCown**	*afternoon-01-11-15--01-21-17-Steve-McCown*	10:01
07	**afternoon-01-22-14--01-31-45-Simon-Wood**	*afternoon-01-22-14--01-31-45-Simon-Wood*	09:27
08	**afternoon-01-32-08--02-32-06-Chris-Bramwell**	*afternoon-01-32-08--02-32-06-Chris-Bramwell*	1:00:00
09	**lunch-00-20-51--00-32-51-Jay-Stanley**	*lunch-00-20-51--00-32-51-Jay-Stanley*	11:55
10	**lunch-00-33-30--00-41-34-Jason-Chipman**	*lunch-00-33-30--00-41-34-Jason-Chipman*	08:04

11	**lunch-00-41-41--00-48-06-Jeremy-Grant**	*lunch-00-41-41--00-48-06-Jeremy-Grant*	06:25
12	**lunch-00-48-12--00-52-35-Christian-Reza**	*lunch-00-48-12--00-52-35-Christian-Reza*	04:24
13	**lunch-00-52-44--00-58-51-Scott-Stornetta**	*lunch-00-52-44--00-58-51-Scott-Stornetta*	06:10
14	**morning-00-03-34--00-18-20-Chris-Bramwell**	*morning-00-03-34--00-18-20-Chris-Bramwell*	14:48
15	**morning-00-19-05--00-29-15-Ryan-Hurst**	*morning-00-19-05--00-29-15-Ryan-Hurst*	10:09
16	**morning-00-31-20--00-55-41-Cindy-George**	*morning-00-31-20--00-55-41-Cindy-George*	24:17
17	**morning-00-59-44--01-29-30-Legislative-Panel**	*morning-00-59-44--01-29-30-Legislative-Panel*	29:43
18	**morning-01-30-34--01-41-59-Daniel-Hardman**	*morning-01-30-34--01-41-59-Daniel-Hardman*	11:29
19	**morning-01-43-00--01-50-14-Phil-Windley**	*morning-01-43-00--01-50-14-Phil-Windley*	07:13
20	**morning-01-50-35--01-58-24-Joe-Jackson**	*morning-01-50-35--01-58-24-Joe-Jackson*	07:48
21	**morning-01-58-29--02-20-59-Wayne-Chang**	*morning-01-58-29--02-20-59-Wayne-Chang*	22:34
22	**morning-02-21-20--02-32-35-Paul-Cutler**	*morning-02-21-20--02-32-35-Paul-Cutler*	11:15

TALK I



afternoon-00-10-05--00-16-06-Alan-Fuller

STATE ENDORSED DIGITAL IDENTITY SUMMIT · TALKS · 05:52

really great conversations here. And I'm so glad that you're all able to come. Let me just quickly make one big point. And I want to talk about digital identity as critical infrastructure. So as Phil Windley talked about earlier, the purpose of a digital identity is to create a trusted relationship online. And we used to talk about with trust credentials that was going to be like with identity and access management systems, that you needed something you know and something you have.

But that is becoming not sufficient. And what we need is something you can prove. And something you can prove is a credential with cryptographic codes that can verify both the holder and the issuer of the credential. And I just want to point out that this is actually new territory for states to be leaning in to this area where we are adding a state endorsement to a relationship where it hasn't really existed before. Yes, the state has issued driver's licenses and other credentials, lots of them, but the online age changes the nature of these things. Okay, so in the digital age where so much of our lives have moved online from social media, social banking, commerce, application for government services, where so much of our relationships have moved online, this identity, digital identity becomes absolutely critical infrastructure.

There's so many public sector areas that rely on this and we've seen in our country since COVID hundreds of billions of dollars in fraud and a lot of that fraud is tied directly to not having good identity verification. So, you know, for at the state level, public social services systems like food stamps or unemployment insurance or housing assistance or Medicaid or child health insurance. Many of these rely on being able to identify someone successfully. We have a lot of discussion in our state about voter registration and signature gathering and petitions for citizen initiatives. Can we do those digitally without having a true digital identity? In the last legislative session, one of our leading senators asked me, what will it take to be able to do online elections and will this help us do it? And I told them, I know for darn sure you can't do an online election without a digital credential that is reliable and trustworthy for identity. Professional licenses and education credential and also our corrections and public safety interactions. Across the private sector, we have a plethora of use cases as well that that rely on secure online infrastructure, whether it's verifying proof of age online or in person, whether it's accessing our health records and benefits and also our financial transactions. We have the know your customer requirements in that area and then we have many different online commercial and travel related needs. But we have a big problem. And so as part of my organization, we have the state cyber security center. And what we see is we're constantly under attack. Our state systems in Utah have about a billion and a half scans per day of our system. And we have numerous efforts by malicious actors trying to create fraud, trying to create ransomware attacks. And so what we see is our infrastructure, especially our digital infrastructure of all kinds, will be under attack. And the point of attack, the attack vector most often used, is identity. And so because digital identity is critical infrastructure, incomplete and half measures with regard to the security of these systems are not acceptable. We have to have reciprocity between states, but that also means that all states need to have strong security around their digital identity systems. We have to build SEDI with the highest level of security that is available. And we know that nothing is perfect. So we need an ability if compromise occurs, or I should say when compromise occurs, we must have a way to recover. So when we think about SEDI and we think about keys, cryptographic keys that are the backing that credential. What I'm talking about for the technical person and the technical people in the room is we need a way to rotate those keys. One of the concerns I have about the current MDL technology is that we don't have a great ability to recover if those are compromised, you know, short of canceling and reissuing credentials. So the ability to revoke is important. The ability to recover if it's compromised is essential.

Thank you so much. Glad you're here. We could do this quickly like a pit stop, right? All righty. They said wait 30 seconds. something

TALK II



afternoon-00-16-06--00-26-12-Scott-Perry

STATE ENDORSED DIGITAL IDENTITY SUMMIT · TALKS · 10:05

There we go. Yay. All right. So my name is Scott Perry. I'm here to talk about open standards and open protocols. And so when you're looking at a SEDI project, okay, we're just getting started, but there's been effort to deal with decentralized identity for the last 20 years, starting with Phil Windley co-chairing the Internet Identity Workshop 20 years ago. And then for me, it's been 10 years after I got a call from Timothy Ruff saying, I need help around trying to deal with internet trust.

And I realized as an auditor that was auditing certification authorities, I realized that the traditional model wasn't going to work to add internet, to add the kind of trust that we're trying to do with the SEDI project. So just a quick little bit about me. I'm the auditor in the room. I was auditing for my career. Last 20 years, I've been auditing cryptography as a profession. Auditing small group folks that audit certification authorities. I was the auditor for a certification authority based in Utah. It's great to be back here. I was working with DigiSearch for quite a long time. And I've also been leading some open source and open standards projects. projects that are listed here, but I want to focus on the acronym suit that I'm going to talk about because it's important for folks to understand there has been a lot of work. There was a question around, is it going to work today? I'd say two years ago, things hadn't been completely baked in, but I think we're ready. The open source community is absolutely ready for SEDI and I'm excited for them to demonstrate their value in all of the work that that they've been doing for over 10 years. And so when we start about that, I'm going to give you just a summary of some of the organizations that I've been touched with that have been developing some unique products that can be leveraged into the SEDI project. And it starts with the Linux Foundation. So I don't know if you know, but the Linux Foundation is the largest repository of open source code in the world. They operate 100% of all the supercomputers and 62.7 of servers run the Linux kernel. And so they decided to get involved in decentralized trust. There was a number of projects that was driving some of this type of thinking. And so they established a subset of their organization last year and they invited and consolidated a couple of open source and open standards projects. One that is called the Trust over IP and I'd invite all of you to spend time going to the Trust over IP. I am the co-chair of the steering committee. We have a couple of steering committee members here in the audience and they've been doing enormous work to get ready for the SEDI project. We've created a stack, a technology and a governance stack. Everyone's talking about governance. Trust over IP is the leading organization driving governance standards and methodologies and toolkits. And I hope that the organization here, the SEDI projects uses it because it's been successful in the C2PA, in GLEIF, in the government of Bhutan and such. It also is housing KERI. You've heard some stories about KERI. It's a blueprint of how to decentralize identity and make security more autonomous and user controlled. It's exactly one of the main principles within the SEDI project. We have a trust spanning protocol which acts underneath the internet protocol to the ability to authenticate senders and payloads of transactions because we need that level of trust in our transaction protocols and also it is leading around trust registries which are public repositories of those that have passed certain governance frameworks. The Open Wallet Foundation was founded in August 2023. It hosts components that can be used to create secure, flexible, and portable wallets.

Where are we going to keep the SEDI credentials? We need a secure place because they have private cryptographic keys. Also, we've talked about the W3C started in 1994, produces two key standards that we can leverage within the SEDI project. The decentralized identifiers, the DIDS projects, as well as defining the components of verifiable credentials which we expect to use. In the decentralized identity foundation started in 2017, we have a number of projects that are working that can add value. They are the leading place to deal with all of the decentralized identity methods that are out in the marketplace

and they are working to consolidate that. They're creating standards around the communication using DIDCOM as well as the presentation exchange of credentials as well as hosting an organization called the Creators Assertion Working Group which I co-chair which deals with individual and organizational attribution to any digital object based on the content credential created by the C2PA. So I would look that up as well. Also the OpenID which has been around since 2007 and has modified their standards to deal with verifiable credentials with OpenID Connect and OpenID verifiable credentials. ISO as we have mentioned here has been instrumental in creating foundational security standards both with quality and ISO 27001 for for foundational security management systems as well as they have identity management standard ISO 24760 and finally also the mobile driver's license the ISO 18018013.

We talked a little bit about what the role of the federal government would be. Well, NIST is providing a lot of value there associated with dealing with post-quantum cryptography. They're also dealing with the certification of hardware security modules which protect your private key and are the leading standard for digital identity guidelines both for proofing of identity, authentication, and federation.

So what's the case for open standards? How do you use it? Okay. At the end of the day, it enhances interoperability and compatibility. accessibility. Okay? It prevents the vendor lock-in so that all the tech vendors are using open standards and they can use it so you're not locked into an individual technology company and can't get out of them. It creates the innovation and collaboration. You're not limited to an individual's company, R&D. You're leveraging world R&D. And that's what the state of the organizations that I work for, they are creating that research and development that we could leverage. It increases flexibility and Joe Jackson to mention about future proofing. They're baking in advances of these standards to deal with new technologies as they come along and they're free. State loves free, right? And the best way to leverage it is steal. this technology and steal these standards because it's there for the taking and they work. So I'm going to just walk through I'm not going to go into details of some of the products that we've created in the open standards world but these are the some of the ones as a governance you know professional have leveraged on and you know we've realized there was a trust you know triangle with the issuer holder and verifier trust over IP added a governance model and we have found that that's the missing, that's the secret sauce into making it long-lasting and workable. This, I'm not going to go into the detail, but this is the trust over IP trust stack. And you can see that there's been a lot of work that's gone into it. And Chris Ramel said to me, if you do one thing, let people know how complicated it is. And we've done a lot of the baked in work. So governance framework, it's already built. the framework's work. You don't have to worry about it. You just have to put in your requirements into the governance framework and then you could leverage the time and energy to get this to market. So I'm going to quickly go through the reasons why you should adopt open standards.

It's all there and I think we're ready to go and I think you could take advantage of a lot of the work that's been done to make this happen. If you want to have an idea of a white paper that's free to use on how to use governance and use trust registries. I put it out there. It'll be in the videotape so that you could access this at your leisure. Thank you very much for your time.

TALK III



afternoon-00-26-28--00-44-25-Timothy-Ruff

STATE ENDORSED DIGITAL IDENTITY SUMMIT · TALKS · 17:57

I would like to recognize two individuals if they are here. Scott Stornetta, are you here? Been walking around. Is he in the room? Samuel Smith. He took off. I was hoping to, I want to acknowledge two people whom I think are fathers of modern digital trust. And I'll just say that Scott Stornetta was cited by Satoshi Nakamoto's Bitcoin paper. He's the original conceiver of blockchain, which is a really important innovation in digital trust. We wouldn't have cryptocurrency without that innovation. And literally the creator of blockchain quoted Scott Stornetta, who's been here today. He's out in the hall or somewhere. And then Sam had to leave. Sam is the creator of the KERI protocol key event receipt infrastructure that has inspired the SEDI identity model including the very exciting thing I get to talk about which is guardianship and delegation. A really big breakthrough in digital trust to solve a very thorny problem. Now I'm going to break from how I usually present things and I am going to I'm going to really almost read the slides which I hate to do that but I know this is being videoed And I know these presentations are going to be asked for.

And I want anyone who gets this presentation at a later time to be able to understand every single point. And so you're going to see me, you know, basically reading some of this, but we're going to go quickly. Really important concept. First of all, a couple of definitions. Guardianship gives someone legal authority and responsibility to make decisions for another, like a child or a disabled person. So real key concepts underlying there legal authority and responsibility. Two different really important concepts that make up guardianship. Delegation, I want to wait for my example to come up. There's a little bit of a lag here. Temporarily transfers specific duties or powers but not full legal responsibility. Key concepts are temporarily and specific duties or powers and not full legal responsibility. That's the difference between guardianship and delegation. So let's give an example. If a parent delegates school pickup to a neighbor, the parent still holds the ultimate responsibility for the child's welfare. Okay, that's just a task that has been delegated, but not ultimate responsibility or legal authority. Guardianship legally transfers that responsibility. The guardian and not the parent is now the one accountable for decisions and care. So those are the two conceptual differences.

Now I'm going to share with you 10 tools that we use in combination to make guardianship and delegation work as well as all of the rest of the SEDI protocol. I chose Lego here instead of a toolbox. The difference is when you put Legos together, you might make a pirate ship. You might make a pirate, you might make spaceship, you might make a dinosaur. You put them together in different combinations to do the thing you're trying to do. A toolbox, you get out of the toolbox and you do something to use the tools and then you're done. So with SEDI, it's very much the Legos, even though they are tools. The first tool is verifiable containers. Now, for those of you familiar with verifiable credentials, we're talking about the same concept, but a verifiable credential is misnamed. It is a container that holds data and makes it portable. It might or might not be a credential. It can have anything inside the container. It's the container that's verifiable technically.

So it makes data portable and verifiable. The next tool is secure attribution to verify who digitally signed a thing. So if you get a container that has some data in it, who put that container together? Who did it? And being able to secure part is really important. Verify who did it. The third tool, non-reputability. You can't later say that you didn't. once it's been signed, it is non-reputable. You can't later say someone else did that. So when you have encryption with TLS or HTTPS, you see the encryption that happens on the internet. There is repudiability. You don't know who is on the other side of it. It's not bound to a human person or an individual. It's just there's a weak form of authentication that goes with encryption,

but it's not like a digital signature that you can actually bind to an individual and say who did the thing. Chain signatures which give you verifiable provenance so you can actually see a chain of authority rather than just a single level. So if someone signs something like a manager, well, who was their boss?

Where'd they get their authority from? Who was their boss? Who did they work for? And is that really the company? How do we know that was really the company? And on you can see a full chain and it's unlimited. A full chain of provenance on there is another really important tool. And then weighted multisig critical for business and on a whole lot of other cases we're going to talk about here in a moment. But weighted multisig means that you can have one of two signatures. You can have one of one, just one person signs it and they have the full weight. You could have one of two, two of three, five of seven, 11 of 92, whatever you make up. Okay. So it's weighted because you can have one signature have more weight than another.

and in a situation with divorced parents and things like that and where the court might be intervening, really important in guardianship to have weighted multisig. We'll talk a little bit about that. Consent. The ability to use your identity to make a non-reputable agreement and say, I agree to a thing. Delegation of authority, which we're going to talk about in a little greater detail. Revocability of that delegation. And critically, a really important breakthrough with SEDI, privacy respecting delegation. I was just talking to a representative from another state who said that the reason that they were adopting a very popular technology for identity is because their technical people thought that there was no way to get around a phone home for revocation. That is not true. There is a way to get around a phone home and have privacy respecting revocation. Really important breakthrough in digital trust in one of the tools in SEDI. Graduated disclosure which can be selective contractual. Basically you can disclose as little as you want to disclose when you're doing something and there's actually a way to only disclose that thing once terms for disclosure have been agreed to and consented to and that can happen behind the scenes with agentic AI and these agreements can be made and you actually don't disclose a thing until the terms have been agreed and it's mutual. It's like a real-time NDA. done digitally.

Really exciting capability and detection and recovery from compromise. As a matter of fact, SEDI brings a four-step concept I'm very excited about from a security standpoint. SEDI expects compromise, then it can detect compromise, then it can contain compromise and recover. These are mind-bendingly awesome in digital trust.

Expect, detect, contain, recover. Secure attribution, really important in Utah law, an electronic signature can be as legally valid as handwritten with some assumptions. There's got to be an intent to sign. There's got to be attribution, which is where SEDI comes in and really helps consent to electronic transaction, which interestingly, there's going to be a dilemma, a legal one. Can you use digital means to agree to use digital means?

That's going to be a fun one. And then no legal exclusion. Sometimes there's a legal exclusion that says you cannot use digital. You must have paper. SEDI can use its own tools to prove each of these. Doesn't mean that we legally want it to.

There's going to be some policy debates, but it does mean that SEDI can use the tools to do these things. So guardianship, examples of guardianship, parent of a child, the natural guardian, guardian of a disabled adult, guardian for an orphan, orphan, which is court appointed or temporary guardianship like when parents are traveling. Guardianship is the missing piece of government digital identity. You don't

see it anywhere. You don't see it talked about. I think it is the cherry on the Sunday when you're doing a digital identity system if you're government. If you're not government, you don't care as much. But when you are government, you absolutely are the dog wagged by the tail of dependent populations. So these are the children children, infants, elderly, disabled, homeless, right? There's advocates for all of those and they're loud and they're powerful and they should be. And so to be able to have guardianship and digital guardianship that actually brings those dependent populations into the digital realm, really important stuff.

And if there's one takeaway from any representatives of other states that are looking at SEDI, there's some privacy and autonomy reasons for looking at SEDI. There's some security reasons for looking at SEDI. But I think the number one reason why a state would look at SEDI is because of digital guardianship. Because it includes everybody. All the different dependent populations you want to include.

No government system has figured this out. Few of them are even talking about it. Only 25% of US 16 year olds get a driver's license. Only 50% of 20 year olds have driver's licenses. But yet 100% of 15teen -year-olds need identity.

SEDI solves a big technical challenge, decentralized digital guardianship that's peer-to-peer with no phone home and no dependence on any vendor network or blockchain. That's a really important thing. You know what's easy to do technically? To prove a guardian relationship, if you phone home to a server and the server says, oh yeah, that's the parent of the child, we're good. And you're phoning home to the server. That's easy technically to do. You know it's extremely hard that requires the breakthroughs enabled by Sam Smith, who I mentioned earlier, is to be able to verify that guardian relationship in a decentralized manner where you're not phoning home. Offline, using Bluetooth peer-to-peer, major breakthrough in digital trust. Now, you know, I gave these guys some kudos at the beginning. SEDI can mimic any form of guardianship. A guardian can prove that the guardian award can prove who their guardian is and verifiers can follow guardian requirements for award authorization. So what I mean by that is Johnny requests to spend 35 bucks on Fortnite and his mother is prompted for approval. It's a simple example of how a verifier can follow guardian requirements for award authorization. Guardianship however gets very tricky. A single guardian is very simple. It's one-to-one. A single parent actually is the simplest use case. A single parent just they're the only one who makes the decision, right? It gets trickier when there's two parents. When they're married, it's still trickier than a single single because you can say the parents either one of them can say Johnny can do it. You can say both of them have to approve before Johnny can do it.

You can say up to a certain dollar amount either parent can do it, but if it exceeds another dollar amount, then both parents need to be able to do it. and that's what I call graduated. So you can have conditions in there and things like that for that approval. It gets even trickier with divorced parents where you have a two -to-one relationship with Johnny, potentially a three-to-one relationship if the court is involved, which they might be for some things that Johnny might want to do. And there's waiting. So you can give more weight to the court. You can give more weight to one parent. You can give weight to a grandparent. You can do whatever you want. It's called weighted M of N multi-sig and so you can divide that authority however you choose. And adults show children of a disabled parent. So I've got a mother who's 89 and she's starting to forget some things and she's got a lot of living adult children. And there's some of these adult children who should probably not have a say in what happens with mom. It's an opinion, but at some point that might have to be adjudicated. And someone might have to say, well,

when push comes to sub, the kids are not agreeing. How is that adjudicated? And however that is, if the conclusion is that a certain subset of children have authority and maybe one has more than the others, that can be modeled with MFN weighted multisig, which is part of KERI, part of SEDI. How about homeless people unable to carry credentials? Well, what are you doing there to bring that homeless person in the digital realm if they're unable to carry credentials? How does work in real life. We try to mimic what happens in real life and that is there's a government agency that actually holds some credentials or has the ability to do something on behalf of that homeless person. Very tricky situations. And I'm going a little bit slower than I want so I'm going to go a lot faster. Delegation.

A parent signs a permission slip that authorizes another adult child to pick up their child or a manager delegates a task or an individual delegates to an AI agent. We talk about AI and agentic AI. That is a form of delegation. Delegation is absolutely everywhere. A legislature can delegate to committees and agencies who then delegate to departments and outside companies who delegate multiple levels of employees who provide a service to a citizen. So delegation is absolutely everywhere. All organizations, private or public or are hierarchies of delegation.

SEDI enables an individual to directly delegate authority to another without involving anyone else. else. The individual, the authority can go directly to the delegate and give them that authority. With SEDI anyone anywhere can verify the claimed authority without phoning home. We talked about that earlier decentralization. SEDI can mimic any form of delegation. A delegator can prove what and to whom they've delegated. A delegate can prove what's delegated and from whom.

And by the way, the word delegate a little bit awkward because in some cases a noun, in some cases a verb. Okay, so I'm I'm using the form delegate here in number two. A delegate noun can prove what's delegated verb and from home. Delegation can expire or be revoked. A delegate can delegate again with proof of authority to do so. Delegations are non-reputable which means they can't be denied later.

Delegations can form hierarchies or chains. They're auditable, traceable. They cannot be forged. They're resilient to key rotation. And rules and restrictions can be made verifiable, machine readable, and enforceable. Sounds like a dream list. It is. Now you know why we're excited. Agentic future, by the way, I have to laugh at this picture of grandma being helped by a robot. And no, that wasn't made by AI. And no, I didn't take that photo. But Microsoft CEO said this and I'm paraphrasing because this quote is too long, but the the paraphrase of the Microsoft CEO, AI agents will replace all software as a service, SaaS. class. CEO of Microsoft. And the reason he says that is because of frankly what I think is illustrated by grandma. It's a user experience. Most agentic tasks are simple and don't require delegation, but some important ones do. And they require some delegation, some authority on behalf of the agent. And I think one of the greatest use cases, I keep it in the wrong button and gets rid of them. I think one of the greatest use cases for agentic AI is user experience for elderly people. I know my mom could talk to an agent and ask her to do something. She struggles to open her phone and start an app to play Scrabble with her daughter in Pennsylvania. But I know she could talk to an agent and say, please open the Scrabble game or please do something. I think the future of AI for elderly people is really, really bright.

And I want that agent's authority to do something on behalf of my mom, carefully constrained. SEDI is ideal for delegating to agentic AI. So in conclusion, SEDI brings guardianship and delegation into verifiable digital form, harmonizing law and technology. SEDI includes everyone through digital guardianship. Parents, caregivers, and courts can securely represent those who cannot self-manage their identity.

Through SEDI, delegation individuals can safely empower others or AI agents with limited revocable authority. SEDI actualizes both human and legal rights and principles and is designed for the coming agentic AI era.

Thank you.

TALK IV



afternoon-00-45-26--01-02-47-Thomas-Mayfield

STATE ENDORSED DIGITAL IDENTITY SUMMIT · TALKS · 17:19

My name is Thomas Mayfield. I am joined here today by my colleagues Fergal O'Connor on stage and Jeremy Furster in the audience. We are here representing the Cardano Foundation, a Swiss-based non-for -profit, and we've traveled from quite far and wide. Jeremy has traveled from Taiwan, Fergal has traveled from Ireland, and myself has traveled from the United Kingdom. And we have done so because what is happening here in the state of Utah is a paradigm shift in digital identity. And what we would like to demonstrate for you today is the art of the possible, the potential for what some of these things we have heard of today, such as guardianship, could look like for your citizens and how the state could leverage these technologies. Before we start the demo, I would just like to say a few words. We live in a world where our trust in government technology and our fellow citizens is eroding every day. I would testify that every person in this room and those watching online believe the protection of children is our most important societal responsibility. It is evident that the internet is a powerful but dangerous place. A place where we do not know unequivocally who we are interacting with online. Is it an adult or a child? Is it a human? Or a machine. It is a genuine person or a predator. There are numerous statistics available and I would like to highlight a few given the time constraints we have today. In 2024, ChildLight, the Global Child Safety Institute, reported more than 300 million children fall victim to online sexual exploitation and abuse each and every year. Similar to the tragic story we heard this morning, there are more than 1300 reports made involving violent online groups that encourage children to harm themselves and others. Online games have become hunting grounds for predators. Some of the largest being Roblox, Minecraft, and Fortnite. Roblox self-reported cases of suspected child sexual exploitation to the National Center for Missing and Exploited Children increased dramatically between 2019 and 2024 from 675 to 24,000 cases. In the first six months of this year alone, Roblox has reported more than it reported all of last year. In 2019, a study of more than 2,000 child Minecraft players found that nearly 10% had been asked by another player to meet in real life. That's almost 200 children and that was six years ago. This number has grown exponentially. There have been numerous attempts to remedy these risks to children. However, they do not address the core problems, how we access the internet, digital content, and the interactions children are exposed to. Today, you will witness for the first time in the world two technologies, key event receipt infrastructure, commonly referred to as KERI, and authentic chained data containers, ACDCs, being leveraged in a manner that no other technology can achieve today. Providing open source, state-endorsed, digital identity wallet and supporting services designed to return control back in the hands of parents and guardians, empowering them to ensure a safe and and verifiable digital future for their children and their children's children. What we'd like to do now is walk you through a demonstration leveraging these technologies.

What Fergal is going to be demonstrating on the left-hand side is a representation of the state of Utah vital records platform. What he will be doing here is issuing a birth certificate. Now, this may be a manual process conducted by an administrator. It could be a checkbox in an existing system that's integrated. It could be fully automated. But the point here is that there are certain aspects of SEDI that must be introduced by the government and others that fall into the power of the parents. Fergal is forming a peer-to-peer channel with the government, leveraging the mobile wallet of the child Oliver in today's demonstration. The parent, Mary, also has established a peer -to-peer communication. and she will be requesting the government issue a birth certificate to her child as well as a guardianship credential. These are all ACDC technology.

So what has happened now is a guardianship credential has been issued to the parent and a birth certificate has been issued to Oliver. What you can see online here is the credential contains any amount of information, including a direct link potentially to a file system or server. It can be fully customized based on policy.

And that is the most important aspect. This is not tech providers dictating what the state can use. This is technology that is built based on policy and law. Now that the birth certificate has been issued and the guardianship credential has now been issued to Mary, the mother. And this could be a multi-signature relationship for both parents, for example, all capable with KERI and ACDC technology. Now, Mary will leverage the family portal. This is all open source software you are seeing here today. This could be running in your home system like a home media center, or it could be provided by a third party. The key difference here is these are not like the centralized systems. The keys controlling the data reside in the SEDI wallet in the hand of the parent. They never leave that platform. They never go into this system you are seeing. Everything must be signed and approved at the edge or from the wallet. So now Mary has logged into this system. You'll notice there were no usernames, no passwords. This is known as passwordless authentication. And now Mary is presenting her SEDI credentials to the family portal.

This will allow the portal to determine what features should be available to her. In there, you will see a number of things appearing in the family tree. This is this chaining characteristic that was just mentioned behind ACDC credentials. In the SEDI wallet is not only a credential dictating the guardian relationship for Oliver, but also the guardian relationship to Liam, Liam's father. So this would be a power of attorney issued by a court, for example. The idea is to demonstrate that all of this information can be contained within a chain of credentials that are cryptographically built upon one another, similar to that scenario with the Lego blocks just presented on screen. So now the parents are empowered to issue credentials to delegate authority to their children, completely removed from the state. The state has provided the credential to prove guardianship, but now the parent has control. Now, Mary will issue a credential to Oliver and you'll see there are three scenarios we've explored here. Social media, streaming platforms, and gaming consoles. We will demonstrate a social media credential and the ability to customize the attributes. What you can see here initially is a conversational age rating. This is the ability for the parent to decide the age in which they want their children to interact with. Second, you will see a time constraint. They can set parameters around when these credentials can be used, when these platforms can be accessed. And finally, there is a content rating that can be set by the parent. You'll see a checkbox at the bottom that says enable safe interactions. What this is telling the system wherever this credential is presented, that this user can only interact with other SEDI-endorsed users.

What we're going to do now is issue this credential. But before I do so, this is just an example. The policy will dictate the parameters of this credential, not the tech providers. So when that is established, exactly what will go into this credential, what are those options, then that will be implemented. They are fully flexible. What you will see now is Mary will receive a request because although it looks like this system is creating and issuing the credential, it isn't. It is merely a Lego block to build, but Mary must sign with the keys that are stored in her SEDI wallet, her identity which is contained within, in order to execute this action. And now what you will see is the child will receive a prompt in their phone saying their mother would like to issue them a credential and they must also approve this credential in order to hold it and receive it. So what you see here is not only holding and issuing, but also the ability to do decentralized verification, which is the next step. So now that Oliver has received a social media access credential, he can now register for a new paradigm shift in social media that we are calling Socialbook today. You'll

notice again there is no usernames and passwords. Oliver will log in online with his delegated authority from his mother in an ACDC credential into the Socialbook platform. Oliver will scan this QR code you see on screen to establish a peer-to -peer connection with SocialBook. He will input his email, but you'll notice Oliver will not be telling the system how old he is. The state-endorsed digital identity, which empowered the mother to create a social media access credential, will inform the platform cryptographically how old Oliver is. Oliver will now register for the platform and will then then log into the platform using no usernames and passwords.

Once Oliver has logged into the platform, we will now start to explore how those criteria and restrictions that were set by his parent can be visualized in a system. What we have done here is we have tagged the data in this post with a metadata label indicating the content level of which this image was. And because the parent has set that restriction to teen, he can no longer view that image. If he wanted to view it, he could request it. But let's move on now to the chat to demonstrate how chat now is leveraging that age restriction. What you will see on screen here is existing conversations that are already underway. And you will notice below there are a number of SEDI tokens that indicate that these are users that that have leveraged a SEDI-based credential to access and register for the system. And you will see other users that have red tags there. These fall outside of the constraints of the age that was set by the mother. In a scenario where Oliver would like to talk to Justin, he must receive approval from his parents. In this scenario, Mary, in order to do so. This is creating a shield online that parents can control for their children children cryptographically. What we will now do is we will move on to another example of how social media can be leveraged. We've had a couple of conversations with social media platforms as well as game development houses. And we were trying to establish a proof of concept leveraging decentralized identity. And the very common feedback we received was decentralizedidentity is too complex to integrate into gaming. Games must have centralized servers. The identity systems must be centralized in the platform to ensure the game and user experience is maintained. So although the concept and the idea behind a centralized identity is powerful and they understood the value it could bring, their statement was you simply cannot integrate this comprehensive technology. So I set this task upon my team to do exactly that. So, what we have done is we have cloned roadblocks. We are calling it KERI blocks. We did this in less than two weeks. Just to give you an understanding of the timeframe here, we are not game developers by any means. And what you will see is Oliver is now going to register and log into this platform in the exact same way, leveraging a credential that was issued to him by his mother in order to play this game online. And all of those constraints and restrictions that are embedded inside the credential will also pertain to his usage of this game platform. So, Oliver will join the system and he will begin gameplay. And there are a number of elements here I would like to touch upon.

The level of predatory engagement that is happening in in-game chat is a significant concern. What you have now demonstrated today on screen is the ability to have age verification built into a game This is a complete KERI and ACDC based chat integration into KERI blocks. All of these communications are digitally signed and the age of the individuals that can communicate with Oliver must fall within those constraints that were set in the credential. Another huge element to in -game concerns is purchases. Many times parents will input their credit card information to purchase something that time. And what has happened is children have racked up credit card bills because that information is in the game. The children can click on things and purchase them and mom and dad only find out once the bill arrives. In the exact same way that Oliver had to request permission to speak to someone who was outside of the age constraints, mom and dad also have to approve the purchase. Again, this is a completely new par-

adigm shift in in-game purchases and parental controls for individuals leveraging online systems. The next one to two minutes of what you're about to see is the potential future for the users that are leveraging Roblox. There are 20 to 40 million users a day leveraging this system. There is a huge opportunity here from a commercial perspective, but there is a huge risk that can be solved with this technology. Go ahead. Let's see if the sound works.

Okay. Sound's not working, but that's okay. Go ahead. Do it one more time. Okay. Secure, portable, and self-sovereign. Using this identity, you can create your own rules and trusted circles with cryptographic proof. Set age limits for your private space. Define your play hours or grant access only to friends you have personally approved. In KERI blocks, you don't just build worlds. You build the rules that govern them, creating a provably safe and personalized gaming experience. Developed by Veridian and integrated with NotBlocks.online project, KERI Blocks redefines how we play in a connected world. So I leave you here with a thought. To the parents and the guardians in the audience and viewing online today. If you could choose from this safe, secure, friendly gaming experience for your children, or you can take a gamble and leverage the systems that are available today, what choice would you make? Thank you very much for your time.

TALK V



afternoon-01-06-53--01-10-02-Utah-Life

STATE ENDORSED DIGITAL IDENTITY SUMMIT · TALKS · 03:12

Where a grandparent can have a grandchild call them and say, hey, I made a mistake and I've run into somebody and I need some money. And then an attorney gets on and says, we're actually going to need you to send us over here. It's a $10 billion industry a year in fraud, which is in addition to what we saw earlier, which that happened 10 years ago. It's like what's happened since this Cindy's son had actually taken her life. These are some of the things that actually can can do it in real time. And so when a grandparent actually imagine a future where a grandparent doesn't need to use username and passwords. They just grab their phone, push on an apps, log in, and they can actually see all of their assets, all of their ability to pay things, all of the things that they own, all the contacts.

And it's actually managed by someone that's given guardianship rights from an organization like a state to be able to help manage that grandparent. Maybe it's accounts. Maybe it's paying bills. Maybe it's paying different vendors. Maybe it's different assets and how to pass them from one generation to another. Maybe it's currencies. Maybe it's the ability to actually manage context, not just for your child, but also for grandparents. There's a lot of confusion when people get into that environment. And then the ability to actually take these types of things and actually drop from one environment to another to actually make it easy for them to pay. So if you wanted to pay a utility bill or you wanted to pay a grandchild, it's all integrated and simple. So that's a good example of a grandparent type guardianship reality with a simple app that you can pull down, log in today and actually start using these types of things. It also works with children. So the ability for children to be able to be managed from what apps are they using to what sites are they going to. There's a lot of functionality and opportunities there. So I just want to say thank you for those specifically Sam Smith, Phil Windley. These are people that have dedicated their lives to solving this problem. Tim, I mean, this is real. This is a nucleus here in Utah that we can actually make a real difference. But ultimately, it's actually all of you that have said, this is a problem that I want to learn about and a problem that I want to be able to be a part of the solution in the future. So thank you for coming and thank you for actually understanding what's happening here in Utah. But it's really the world. It's a problem that society has, a responsibility in our generation. Like when all of us were born, we didn't have the cell phones. We didn't have the internet. And when we pass on, we've got to pass on a better legacy than what's currently there. So thank you for Chris and all the hard work that he does to put this together and those at the state that truly are aligning with this effort. Because I know it's not easy to put these parts and pieces together. When we went and searched the world, we could not find a body like this. We went to the government in the DC. We went here. We went in. It's just amazing to see the heart, the alignment to support someone like Cindy who 10 years ago lost a son.

That's real. In this university. That young man went to this university 10 years ago. And here we are. So thank you for being here and understanding some of these concepts.

TALK VI



afternoon-01-11-15--01-21-17-Steve-McCown

STATE ENDORSED DIGITAL IDENTITY SUMMIT · TALKS · 10:01

Thank you. All right. My name is Steve McCown and I am a commissioner on the Utah Privacy Commission. I'm also chief architect of Anonomy Labs. And I'd like to talk to you about surveillance and tracking today and what SEDI does to get in the way of that. Years ago, I worked for the US Department of Energy as basically a computer hacker. And one of my assignments was to work on compromising cell phones. Another part of my assignment was what they call open source intelligence. And this is the collection and analysis of data gathered from open sources, think internet, and in order to produce actionable intelligence. And in that capacity, I was able to be given target sites and and pull together enough information from the internet that resulted in classified reports. So the first I wanted to look and see when the first open source intelligence was taking place and this is January of 1862. A publication called Harper's Weekly was publishing articles about force movements during the US Civil War. And as you can see here, the text talks about a general's expeditions and where the troops were going, what assets he had. And while the specific targets were secret, they also were able to surmise where they were going. They went so far as to draw pictures of the target locations and the forces attacking the other forces. In modern times, let's talk about surveillance for modern times. So how do email marketers know when to call you? So sometimes, and this happened to me personally, I was reading an email and within five minutes of reading the email, I received a call from the sender of the email and I engaged them in conversation to find out how they were doing this. Here's an example, one of many examples of what we call tracking beacons. So what they'll do, an email is simply like a web page. It's an HTML-based email these days. And they'll put a one-by-one pixel transparent image on there. And for those of you who know HTML, there's a little tag called image that's supposed to load an actual image. And instead of loading an image, what it does is it contacts the internet and pings a web service. And that web service can do a variety of things and you can add a variety of information, username, email address, GPS location, whatever you can get your handle, whatever you can get a hold of and your email client allows, you can then send that off.

So that's a modern example of open source intelligence. And this leads us into what we call surveillance capitalism, which is a concept in political economics which denotes the widespread collection and commodification of personal data by corporations. It's not limited to corporations. Governments can do this too and there can be collaboration between the two. A couple of interesting points about surveillance capitalism is that it operates without meaningful mechanisms of consent. It just happens to you. And you can lose your self-determination through the manipulation of advertising and other practices that might happen as a result of this. Duke University with West Point University with the Army, they did a study back in 2023 about data brokers and the sale of data on US military personnel. So data brokers using these kinds of methods were able to collect sufficient information that it became of interest to foreign entities. And so as part of the study, they were able to approach the data brokers originating from either US domains or .Asia domains and purchase information on US service members and veterans. And when they ordered in bulk, it was about 12 to 32 cents per record that you could get on US military members. Think of all the things we do on social media and how that might be used as we heard this morning for blackmail in order to invoke espionage.

This is a real problem yet it's also the way the web kind of operates these days. Their recommendations were federal privacy legislation and also to restrict the collection of data on current and former military personnel. So how SEDI helps protect our identity. So one of the things, if you look back to SB 260, it says in a couple of lines in here, the state-endorsed digital identity enables an individual to selectively disclose elements of an individual's identity. So taking the driver's license as an example, when you go to

a government entity, say the Department of Motor Vehicles, you don't really have an expectation of privacy. You're going there to give your information in order to get a driver's license credential. So we don't really have an expectation of privacy in that regard just by the nature of that interaction. However, when we go to the bank, you don't need to give your height and your weight and your donor status and all that kind of stuff. And so you can selectively disclose what the bank requires. Then if you go shopping on Amazon or somewhere other than payment information, they need your name and they need your address to ship whatever it is you're buying. They don't need your driver's license number. And so over the summer, Apple has allowed MDLs to be used for website logins. And that may create some very unintended side effects about the transfer of information.

Another aspect of SB260 is asserting with zero correlation. So part of the one of the lines in that bill says verify that the individual's age satisfies an age requirement without revealing the individual's age or date of birth. So for example, if I were to go to the Department of Alcoholic Beverage Services, which is where you buy liquor here in Utah, the assertion you need to make is I'm 21 or older. That's what's required in the law. You don't have to give your name, your address, or any other information. There should be a way to give only the information that is required. And that's what SEDI is after. So when I go to a concert at the Delta Center and I want to use that neat fancy digital ticket, I need to be able to assert that I purchased a ticket that I am authorized to get in having paid my money and so forth without having to give all the other information that may sometimes come with digital credentials. I want this to be a process of least disclosure, not full disclosure. Now, when I go to the hardware store as a veteran myself, I'm offered a 10% discount and I get that by scanning everything on my driver's license. That includes obviously that I am a veteran, which is on my status. It includes whether I'm a donor, my height, my weight, my address, all these things that are unnecessary for that transaction. So SEDI gives you a choice. Here's a quote from the US Supreme Court from back in 1995. It says, anonymity is a shield from the tyranny of the majority. It thus exemplifies the purpose behind the Bill of Rights and the First Amendment in particular. To protect unpopular individuals from retaliation at the hand of an intolerant society. Now, whether you're on the left or the right, this should resonate with you, maybe for different reasons. But this is a really important principle because if we don't enable you to disclose only the information that's required in an untrackable sense in some situations, what we will end up with is what's Scott McNeely from Sun Microsystems said back in 1999, you have zero privacy anyway, get over it. And so SEDI is giving you the choice of what you disclose and when you disclose it and they put that choice in the hands of the holder. So that's what I would hope that you would take away with and you would go back to your respective companies, departments and states and and pose this to your constituents because we want a private identity system that keeps individuals safe. So thank you very much.

TALK VII



afternoon-01-22-14--01-31-45-Simon-Wood

STATE ENDORSED DIGITAL IDENTITY SUMMIT · TALKS · 09:27

– Excellent. Thank you. Okay. Good afternoon all. Apologies for being your remote speaker of the day. Unfortunately, I couldn't get across from the UK to join for this. But I'd like to spend the next 10 minutes looking at something slightly different in terms of the presentations that have happened so far. We've heard an awful lot today about what SEDI can protect from the fraud, making sure everything is assured, making sure we have the assertions, making sure child age verification and adult age verification can be put in place. I'd like to spend a few minutes looking at the flip side of that and looking at economic benefit as a result of a state-endorsed digital identity and what can be achieved there and bring forwards a proof point to show that this has happened and the sort of values that can be expected from that. So, Simon Wood, I've been involved in identity systems for a long time now. Most recently, Group CEO of Ubisecure.

Ubisecure is a UK company but deploys a lot in the Nordics. Ubisecure has deployed a number of platforms in Finland and Sweden and the case study is taken from there. One of the things I'd just like to touch on before getting into that is a differentiator that McKinsey makes on digital identity versus advanced identity.

Everything that has been spoken about today, I would say falls in that advanced identity category as defined by McKinsey. In the UK, we're obviously reeling at the moment from the brick card announcements and so on. And the McKinsey report is often rolled out as one of the values for having an identity and it's referred to as digital identity in the general sense. But if you read that report in detail, you'll see that to benefit from the advanced capabilities and the returns and the GDP increases that are positioned there specifically for the US and for the UK, it needs to be advanced identity, which brings in additional attributes, additional information, and additional features as well. You've already seen a number of demonstrations of those today in a SEDI context. And that's what we're looking at here. We're looking at those advanced capabilities beyond just authentication and authorization, which is McKinsey's classical definition of digital identity. I want to run you through a very quick scenario. You've seen a couple of diagrams like this already today where we have a chain of delegation. Fiknish's example here, we'll look at setting up new company in Utah. So, the CEO of that company to be contacts the Utah division of corporations, goes online and uses their steady identity to register that company. The Utah division of corporations automatically passes that across to the state tax commission because there will be taxes to pay and collect from that organization. And the tax commission will send a request back to the CEO using let's assume that there's a secure mailbox capability from a SEDI implementation. So you can securely contact people who have that identity and request that tax registration. The CEO will obviously go to that website, register to submit the taxes, but then the CEO themselves will not be undertaking that work. They will delegate that capability to the CFO of the organization. So that delegation will be done through the website. The CEO will invite the CFO to that system using their SEDI identity as well. And so a delegation chain is built. You've seen examples of such a delegation chain already in a couple of the demos that have been delivered today. But if we consider that tax is reasonably complex, you might have three different types of sales tax, corporation tax, employment tax. Maybe the employment tax is outsourced to an organization. So that organization can be invited in and delegated to. The administrator in the organization can pick that up and then onwards delegate to an internal accountant. So we've got a chain of delegations running through individuals and organizations using an identity that's highly assured and available to them. This delegation chain builds and allows all of the tax to take place and not once as the state tax

commission being involved in that they've just provided that service to allow it to happen. Now this seems like a great scenario. If that were true, what would deliver us? Well, that does happen already in Finland. There is a platform delivered in 2008 Wait. Hi.

I believe so. Are they not coming through? That will help. How's that? So, just to reiterate that previous slide so you can see what was there. It's a delegation chain across individuals and through an organization there towards the bottom as we have around here. Chris, I assume that's coming through now.

Is that okay? I think that's okay. So, So this platform was delivered or it is delivered in Finland. It's called the Katso platform delivered in 2008. It is a state operated platform as opposed to state endorsed back in 2008. There was not this distinction and this understanding of privacy and how important that that is as we acknowledge today. State operated platform integrates with the business registry to generate that link to the tax office. In 2018, the Finnish government published stats on the savings as a result of of having that platform. And when they published that at that time there were 450,000 users registered on there, the 420,000 organizations and 104 different online government services using that platform.

One of those services was the tax office and it worked exactly as I just described in that delegation chain that's there. In terms of the stats that were collected on that, a significant reduction in physical service points because everything was online and everything was driven by the organization that was registering, they could massively reduce the physical points of presence that allowed them to make a 20 % year-on-year tax admin staff reduction, repurpose them to more profitable areas and the cost of servicing the tax transactions when they went from the old physical base to an online basis dropped from 35 euros per tax transaction to 30 euro cents. That's a 99% reduction in cost per transaction measured by the Finnish government. That's the value that they achieved deploying a highly assured identity that has delegation capabilities, that has the ability to work across individuals and organizations.

Within that, you've heard me talking about organizations. Organizations are an important part of the identity chain. Incorporating an organization identity enables the really advanced identity use cases and that's where we see a lot of the economic benefit coming from. Now, it would be wrong to assume that organizations are just legal entities. We get a lot of utility and benefit from lower assurance levels of organizations. Just like individual identities, there can be low assurance and high assurance, and we see economic savings at higher assurance levels. You've heard multiple times today that SB260 already considers organization identity in the form of family units and family structures. That is an organization. There's no reason not to have the ability ultimately to extend that to bring in private sector legal entities as well to take advantage of that massive uplift in utility and economic potential that comes from there. So to conclude from there, we've seen already that SEDI has phenomenal potential for protection for implementing privacy and for making sure that state citizens, the public gets the protection and the facilities that they need need. But once that's up and running, then extending that to organization identity will bring significant benefit as well. We've heard again a number of times that we shouldn't let private sector define this and I fully agree it needs to be run at the policy level, generating the privacy that's needed, ensuring that's first and then bringing utility and benefit to public sector organizations afterwards. But incorporating those public sector organizations and allowing them to leverage that information and be involved in there and integrate their platforms and their systems to that will bring significant benefit. And what has already happened in the Nordics and in the Baltics gives very strong proof points to show what can be done and the level of savings and level of return that can be achieved there. I've run through this

very quickly. I realize this is remote and a little bit more complicated. But I believe the slides in this recording will be out later. So you can always contact me afterwards or Chris can put you in contact and I can provide more information if that's useful. Thank you very much.

TALK VIII

A

afternoon-01-32-08--02-32-06-Chris-Bramwell

STATE ENDORSED DIGITAL IDENTITY SUMMIT · TALKS · 1:00:00

It was today. I was obviously here all day. Actually, it looked like I missed some meetings today. I assure you, I work really hard. I really do. All right. This is actually, I think, going to be the most exciting part of the day. This is the final discussion. I am going to ask and we didn't plan on some chairs. Could we get a couple chairs just for some of this? We're actually going to discuss how are we going to move forward. We have enough brain power in this room. We have enough policymaking authority. We have the ability to create legislation. We had Senator Kullimore here earlier, our Senate majority leader. I've already heard there's going to be discussions happening with some other state Senate majority leaders. We have counterparts parts and states. We have companies we work with. So now the discussion for this last hour before we leave is how do we move forward?

You never want to have a summit like this without some outcome and some deliverables. We have a lot of momentum built and in order to keep this going, you don't stop. That's what usually slows government down is then you go back and you review. So the question is how do we keep the momentum going? I think three will be good. So we're going to ask Representative Cutler to come up and then is Alan Fuller? in here? Alan, if you'll come up. So this is we're going to have we'll just have one mic for us to share, but then the rest of the mics we'll have some interns around and we want to discuss what are we doing next? What are our next action items from our side? But then how do we engage with states to go ahead and get this consortium going? And then I see the clock here says 14 minutes, but I think we're just at the end, right? So we haven't four timers, right? Okay. So let's actually check.

I think it'd be beneficial if we explain some of what our next steps are actually going to be. Alan, do you want to take the first? Let me just get started by saying that Senate Bill 260 gave the Department of Government Operations of which Chris and I and Marvin Dodge was here are a part are all part of and it tasks us with coming back to the legislature with a specific proposal and the input we receive here and the input we receive through a request for information that we put out many of you responded to that RFI. Thank you for that. We over the next couple of months are going to be putting together a proposal to go back to the legislature for our SEDI program going forward. And you know, we live in the real world. We have to, if we're going to create a system that's going to have provide identity for millions of people in the state, it has to be something that works really well as performant and secure as private. And so all of the principles that we've talked about today need to eventually come together in a real life system that actually works. Maybe we can turn over to you and represent Cutler. Sure. One of the thoughts that I have is in order to, we can, I mentioned this before, we can pass the policy, but we need our industry partners and we need a large enough coalition that we have a critical mass. So what you can do to help is encourage our industry partners that you, by telling them, look, I'm interested in in this or let's work together to get something done.

Communicating that you're interested in being part of a critical mass to move this forward, even if we don't necessarily agree on all the finer points, I think is really important. I thought the gentleman from the blockchain co-inventor that was real wisdom that working together, even if it's not perfect, we can make a tremendous impact. So, but we can't do this without our industry partners pushing very, very hard and getting products that we can put in an alpha phase or a beta phase and start testing and finding the flaws and finding the successes.

Two practical things that I think we can expand. Here in Utah for the last couple months, we've actually held a private sector stakeholder group every Friday we meet, whether we're exhausted or not, to engage with the private sector. I do think we should expand that to invite all private sector in other states.

If you are ready to participate and you want to engage, you want to help be part of building the solution, we can expand that and get that set up so you can come and coordinate. And this doesn't have to just be a Utah stakeholder group. This is part of the SEDI consortium. How do we make sure everybody's engaged and participating? We want a diverse set of ideas, you know, so long as you love constitutional rights. And but I think, you know, we all have a role to play here.

And for the private market, there's always going to be money to play. You can bring real value-added services. We don't want government to be doing beyond the bare minimum of providing a foundation to protect individuals. So this is amazing for you. This is going to be really disruptive in a good way to move that money from incumbent players to others that can help create a more competitive marketplace. So that's one thing we'll do right away. We'll open that up. I'll start on the communication for that and get invites out set next week. I think we had the National Chamber of Commerce Foundation here today as well. So I'm assuming you might be able to help us with that as well. How do we get this out to all the businesses that are part of that? The other thing is now that we're through the summit, we need to go back and start defining some of those baseline requirements. What are the requirements we're going to compare technology to and everybody should play a part in that. Obviously the RFI is closed. We have a was it a thousand or thirteen hundred pages to read. We have twelve hundred pages to read and I know we don't have all the info we need. So we're going to need everyone to participate to say what additional requirements are we missing? And then comes the hard work of the technology needs to prove itself. How do you meet the requirements? And then also I think to what you said earlier the hierarchy of values. That's going to be the hardest part. I know a lot of people in this room are concerned that we are going to compromise on the wrong things in the name of interoperability and efficiency. So as we define the requirements, we're going to have to create this hierarchy of values, which I have seen nowhere. I think that slide was the first time I've seen that presented in that way to have technology value at the highest level of that constitutional rights. So that's going to be a hard part in the requirements building list. but that's the type of stuff that's going to build trust with the public when they see what we are prioritizing. And I think it's going to be great. I think it's actually going to be great for government. Trust is at an all - time low. So this is a really good way to be very transparent to an extreme and let them know that we really want to protect them. One of the things I think that we should talk a lot about is something that Ryan brought up earlier in his presentation about the kind of practical side of rolling something like this out. and gaining adoption. We need to find a launch customer that not maybe customer is not the right word, but a launch tenant that can help us that will pick this up and run with it maybe in Utah like a Zions Bank or something like that that will help launch the whole process and also create the system in such a way that it incentivizes use rather than disincentivizing use. in order to get adoption. One of the big problems that we have with our current MDL program in Utah is that by charging the verifiers for the verification software, it's a disincentive for them to verify. And that makes it so you got an MDL that people can walk around with on their phone, but there's not very many places it can be used. So then you have not very much adoption. And we want to set this up systematically so that it will have adoption and incentives to use from the beginning.

– Kristen Allen, if people have ideas for use cases, where do they go? And I think I'm thinking back to our experience with verifiable digital credentials. We didn't start with the most critical key. We started with something easy that no one was it wasn't controversial. Though I think maybe there's some lessons learned here that How do we start this and get some use cases where we can learn from before scaling it? And what are your thoughts on that process? Well, I was thinking they should call the legislator. All the

RFI responses are protected, but I think I can semi-quote what was in them. One of the best ones that I read was it was actually from an entity that's not looking to compete. They were just giving advice of how they could best serve their customers with this. And they said, and this is actually a saying, I was in health, uh, human services for seven years before this role. Um, they said in that RFI response, help us meet the clients where they are, meet people where the use cases are. Um, and so they said, you know, TSA probably was not the best example.

That's not something that, you know, everybody is going to need, but there's lots of people who have their kids going to school every year. They need to, uh, to enroll and need to have a birth certificate or immunization records. There are use cases where we don't have to try to replicate what's already being done with MDL and is working and they're getting traction on that side. What are other use cases that we can tackle to tackle other more complex issues that are a different subset of individuals, but it's meeting people where they are and they're going to use it. And government's great. I love the saying, government can actually do almost whatever it wants because it's the only entity that can have a legal monopoly. So the only thing stopping us from getting the credentials out to where they're needed in a secure way and getting these use cases is I think that's the legislature. Speaking of the legislature. You need money. Yeah, if we need money, we know who to talk to. You know, this is not just about us talking.

We really want to this is audience participation. I really wanted to maybe start by asking the audience some questions, especially can I start with the legislators in the room? What do you feel like you've seen today or what questions do you have coming out of the conversations today? Would anybody like to please?

And introduce yourself too. Okay. Knowledge is power and you know getting more of us in the room or you know legislative trainings, et cetera, because it's hard to vote for something if you're insecure or ignorant of an issue. You're less apt to vote for something or even make any kind of progress if you are unsure of what you're voting for, which is a good thing. You don't want your legislators voting on things that they don't know about. So I think increase, I see a handful of us here today. Maybe it's because my colleagues just know all the things, but I've certainly learned a lot today. Appreciate especially those presenters who really broke it down into simplistic terms for me. And, you know, I'm a lot more comfortable. I was never against, not completely against it, but I definitely feel more comfortable after the things I've learned today. So I would just say, especially with our lawmakers, we need them. We need us in a room so that everyone can understand and then make the decision based on that. And I think that, you know, the more people learn, the more comfortable they'll be with the direction that we're heading. Thank you.

Anyone else? Questions out there? Yeah, let's open up to everyone. Other thoughts and… Thank you. Were you the one that works with the anatomy labs? Who is that? Anonymy Labs? No, he's over there. Steve McCown. So, I use MySudo. That's, yep. Excellent. I was curious. So, you're asking how we can implement this technology into that. I mean, is this something that's being implemented into MySudo? We do a wide variety of credentials. We implement and support a wide variety of credentials. And so, SEDI is definitely on our roadmap. out. What? Okay. Well, that's awesome. And I just think that this is excellent technology. My limited understanding so far, but I think from some of the policies that we've seen get passed, the app store identification, forgetting SB, whichever one that was, and just a variety of bills that Utah has passed has been, you know, for the children. It's kind of like the the messaging push behind it, but it's devastating to internet privacy and anonymity. like we've talked about some of these here, in my

opinion. And I think that SEDI is one of the technologies that can bridge that gap and that can really help us. And my understanding right now, it seems like this is some vital technology. So I just, I'm championing, you know, everyone here working on this.

It's great. So. Thank you. Question over here. So maybe not so much a question. It's just, you know, you talked about what use cases and things that you can do to make it move forward. So Eric Jorgensen, I'm the motor vehicle director out of Arizona. Jonah, fantastic conversation and discussion this week. Thank you very much for today for putting it on. I think a couple of things that I would just want to say that I think would be key was one is, you know, we already have a great head start on this with MDL, right? So somebody early on said, hey, let's not worry about the technology aspect of it. This is really about the underpinning policies.

And I will tell you, I've been involved with MDL for the past. 10 years almost. Over 10 years now. And I haven't heard a single thing today that like butts heads with that technology. And the good news is when we talk about adoption, 60% of the US population is covered by a state that issues a MDL today. So we already have it.

And in Arizona, by the way, we have over 1 .2 million MDLs issued. We have a population of 5.6 million driver's licenses out there. Biggest use case is not TSA. It's the motor vehicle division. It's state services. We use it now. We used it in a pre part seven ISO compliant way to do it, but we had it out there. We consume our own MDL and that became one of the biggest use cases. Massive driver for adoption for us. So something to think about and something that is in your control as you look at it is why not use it yourselves? That's a place where you can control both sides of the equation and make sure not only is the provisioning done in a privacy-preserving and secure way, but the consumption too and set kind of that example for everybody else on how to consume it too. So just a thought.

That's terrific. And also let's acknowledge Chris Keras. Chris, if you could raise your hand. He's the director of our our driver's license division here in the state of Utah has done a terrific job leading our MDL program. We're grateful for him. I think Jimmy Higgs is here as well somewhere. I don't see him at the moment who will be the next driver's license division lead after Chris retires.

We are I believe that my expectation and hope and this was mentioned to me today too from someone else that likely the states who are already doing MDL will be the first adopters of moving to more broad study because they kind of get it and have already invested in creating a credential like that. Let's see. I think I saw a hand up here. I think it was was it Sarah or Okay, we'll go here and then back. Oh, yeah, Amelia, please. Yeah. I know that I've obviously been working on this with you guys for years. Introduce yourself, Amelia. My name is Amelia Powers Gardner. I'm a county commissioner in Utah County.

And I've been working on decentralized ID and self-sovereign identity since 2019 pre -COVID. And, you know, as I look for as a county commissioner in the fastest growing county in the state, we're 43.6% of the state's growth. As I'm starting to look at capital projects and building brick and mortar to the tune of tens of millions of dollars because of for a growing population, the sooner we can get these services instituted in a way that we can start utilizing them to deliver services to our citizens in a secure, private way, that prevents me from having to spend millions of dollars. And so my question comes in, like, I know we've got the groundwork, but I mean, you know me, I'm like, I want to run first. I want to run first and then I want to walk and then I want to crawl on. We do need backwards compatibility, but when are

we going to have the ability for an organization like mine that has already done some of this work? when are you going to give us the ability to start adopting this on a broad scale? When do I start getting the schema and the requirements so that I can start implementing this for my citizens so that I can deliver services to my citizens without having to spend tens of millions of dollars building brick and mortar buildings? Was that chastising us, Amelia?

I'm joking. Yeah. Yeah. Yeah. So there's a lot actually going on in Utah for those that are from other states and just, you know, we work with Amelia all the time. So we've had this discussion. For every state, you actually have a unique opportunity right now. Every state nationwide is pretty much non-compliant with their records management and data governance laws. And Amelia is shaking her head, but this is the opportunity. So when I say that, what I mean is you all have antiquated laws from the 70s and 80s that require certain things like disposal of data according to retention schedules. Most systems have not been created to dispose of data. Most states haven't established the purpose and use of data.

Most states haven't been giving privacy notices. And that sounds really bad, but the great thing about it means there needs to be a modernization anyway over the next decade. And so you're in the unique spot of because you know there's non-compliance and I'll actually I'll share out after if one of my team can take a note, we had interns over the summer actually research all 50 states' laws to determine where they are legislation-wise. So you can see where is your state with privacy, with records management, with data governance. You'll know you're non-compliant, but now that you know what's coming with digital identity, you know you need data governance. And now what Amelia mentioned is the schemas, this concept of what are the rules? What's the schema? What's the formats of the data that needs to be collected? When Amelia is asking what's the schema, it's hey, when somebody applies for a building permit. What is the exact data the county should be collecting? What needs to be on the forum so they can automatically ingest it, automate that process with AI or machine learning, and then move toward the efficiency that government can get. So what I'm saying is now is actually the perfect time to learn where you are. And it takes about a decade to transform. Utah is about three years in on this journey. And that's why we've been modernizing our laws. We've been getting comprehensive privacy law. Amelia, but the schemas will come sooner. We actually have on our team we're doing modernization of then the data governance structures, the rules around the data, how long can you keep it? What's the legal basis? What's the purpose and purposes and uses? We're starting to define what are the immutable records, which records are immutable public permanent records, which makes sense to go on a blockchain. These are the things you need in a schema to then implement technology correctly. If you jump right to the technology without having these things, you end up having to backtrack. So I don't know if that's the answer, but it's coming soon. And the schemas I think will be very soon. We have some almost ready. Maybe Sarah? I just want to echo thanks again for having this event. It has been really, really powerful learning a ton and getting to make sort of leaps and bounds forward. So thank you. I think there's an opportunity to create a more sort of like formal digital space where those things that you were just talking about, Chris, if you could post them, playbooks, I think this opportunity of how can we learn from you also share what we are doing in Colorado and other states so that we can learn together. I was reflecting on the statement about MDL and opportunities around MDL. We recently discovered that the standard MDL contract with the big tech wallet companies, Apple, Google, Samsung, in our case, have a clause in them that says they are sole and exclusive provisioner and revoker of MDL. And like, that's something I want to share with

you all about like one particular thing, because it does conflict with the SEDI idea. And so how do we join forces together and say like, hey, Apple, Google, let's not have that as the standard clause. Yeah. All of us are sort of against that idea. So I think that there is an ask maybe and how can we contribute?

It's not just an ask of you. Can we host it? Can we do something so that we can do that knowledge sharing and really accelerate our co-growth? We will be emailing out after the summit. One, obviously we had the white paper of what is SEDI. We have some resources that we've created of model legislation, model resolutions, model executive orders. For us to do a formal consortium, there should be something you want your elected officials, governor or legislature to authorize. We've had this discussion with our governor and let him know we wanted to do a consortium, which is why we've invited you all today. If one more state for, I mean, we've had a couple reach out and say, actually, we're very interested.

If you can get the formal approval, we'll start seDI.gov. And it's not seDI.Utah .gov, seDI.gov. You need at least two states with formal approval. And that's where we start building that multi-state formal consortium and we can start then advocating for ourselves and for our citizens and put these resources there and we can build it together.

Yeah, that works. Okay. So first of all, thank you. This is actually turned out very well as an event and I think there's been a lot of really great interest. I always talk about this as an idea when we talk about off-Broadway use cases as representative Kohler mentioned, but I think the idea of vital records is something that is not so much any having anything really implemented yet. And I always like to say death records because everyone needs one one day. Death and taxes are the two things that they say are inevitable. And there's a guardianship mechanism and a burial permit mechanism and a plot of land. Kind of have everything at once. I do have him the treasurer of a cemetery, so I would love some funds. We're actually going to have George McKeown make a comment about how are we engaging vital records. The amazing thing actually about government is once we start saying we want to do something, it opens doors with all these organizations.

I wasn't anticipating getting on stage. So one of the things we've done is we've reached out to Napsus and I just gave a discussion to their security and privacy group last week. We are actually talking about the schema that they have for a national standard for a certified birth certificate and their digital schema. So we have committed that if they want us to come out to their December event, we will bring a SEDI compatible version of that. So they're close on their standard. We just need to wrap it in the appropriate cryptography to make sure that meets the SEDI threshold. And I think we'll be there. The real goal will be is in June of next year when they have their annual event that will really move that forward with them and kind of codify all that.

One of the this session as we go in to make recommendations for the SEDI program and we also we need to recommend what would the next legislation look like part of that does need to be prioritization of credentials and that's been a very common ask. How do we get these other value-added credentials not just mobile driver's license or a driving credential but it was birth certificate, your immunization records, your death certificate and And so I would anticipate that would be part of the discussion we have this session is not only do we need to get it out there, but then we need to work with the group. So we had I think we had part of the group group here from health and human services today where vital records is, but I think that is a low hanging fruit use case to get out there. We'd actually love to know what are you

going to use that data for if people have it? What's the private sector able to provide value for if you have those records though? And Scott, I think you had a question, right? I have three things. One, excellent day, really outstanding.

Two, incrementalism is important, but there's a cart and a horse kind of aspect to this. And so, how do you get to trust? And I think that's one thing that we really need to ask ourselves in terms of who is trusted to each of us. And if that's our teacher, our professor, our doctor, our lawyer, our banker, I mean where that comes in, I think really it might help you define use cases and how to go after those early and first. And third, if you want an example of one state that I, if you went to Hawaii anytime during the pandemic, Hawaii did a really excellent job of making sure that they could reopen their economy, which is tourism, by making sure that they had the smart health card for people to come in and show proof. You had to prove you were vaccinated in order to visit at that time.

And they did a really a great job of it. People were motivated, of course, to fill this out and an ID for it. But it's just one example that you might want to loop in Hawaii on. All right. So listening to all the constituents here, the challenge I think that we have here is a scope problem. There's lots of things that can be done, but the way to get something done is iterative. And it needs to start with the core of what you're looking for. So you've done two things. You've said, we're going to have a state endorsed identity. Okay. And you have a law. So you have two things to build upon. I think you start there. What is the state going to do whether you have paper to present to the state to endorse, but it has to be focused on the first and foremost thing, which is how do we issue a state-endorsed digital identity and start there? And then use cases will come once you have that established. If you don't have that established, what's the SEDI project? So that needs to be the absolute core, and it needs to start with a risk assessment because there's a million risks we talk about today. but there are only certain risks that can be mitigated by a project like this. And that will drive the scope of how you can mitigate the risk to the degree that the state can accept. And you take the law and all the requirements that you have in the law and put it in the governance framework and the set of requirements. And at least you are have you have momentum. You need to start with momentum and leadership and others will come and use cases will come.

But it has to be right down the road for what you've done. Don't lose focus on that. You have law to drive a state -endorsed digital identity. Make that happen. You have the means to do it and you have the expertise in the room here to start for sure.

So Matthew Helston here from Brigham Young University and I think transcripts and educational data is a very complex use case and been working on this since 2016 with SSI space and we've made a long way so it's really amazing but I wanted to emphasize something that I think about with decentralized identity I think is important is that just because we have a credential and a set credential doesn't mean we have a ubiquitous identifier. So we don't want to have a unique identifier that correlates us wherever we go. We have the possibility of using that identifier where we want to, but we can create an ephemeral identifier with our credential and make a connection with another entity to present our information. That's really important that when we think of our use cases, we're not thinking of I can be correlated wherever in that a great user experience and that may be true, but I may not want that as an individual and the technology needs to support the privacy policy of me being able to choose to create an identifier to present my interface and my information through. So I want to emphasize that. Another thing I wanted to emphasize is credentials need to be intentional. They don't have to be where everything is stored in one credential, right? I can have a very micro credential for a specific intended purpose and

the technology stack allows me to take multiple credentials and draw selective disclosure information from each of them and aggregate it into a presentation for the verifier. So that means as an issuer of a credential I don't have to solve all my use cases where I think my credential is going to be used. I just have to focus on my data and give that to the individual. individual and let the verifier define their own data contract that really empowers them from a data model perspective of verifier defines their contract and we can fulfill it from a number of credentials. We can give an example of that with our the first credential and this is what representative Cutler is referring to is our off-highway vehicle training certificate which we put out a verifiable digital credential for this training certificate to drive your four-wheeler on the roads. Yeah, thank you. And we have, but it doesn't say who you are. So you still, it doesn't provide your identity. You have to have both an identity and this credential to say, you know, who you are and that you've taken the course. Let's see, where are we with our microphones? Maybe here. Yeah, go ahead. Yeah. Phil Long from the US Chamber of Commerce Foundation and T3 Innovation Network. I just want to bring us back to the actually the first presentation that was given this morning by Ryan First. first who are Ryan. Yeah. That reminded us that we really need to look at the examples of failures of the things that we're looking at as potential priorities to try to learn from them because we tend to dismiss that was done by them. It was done at a different time perhaps a year ago. It may not be relevant, but there are things and lessons in there that will be extremely valuable if you look for them. So that's one thing. And the second to reinforce several of the comments here, which is to pick the two or three to start with that are win-wins for all of the stakeholders involved because everybody's going to have resistance to it at some point in this early stage. So where you can come up with one where there's beneficial time savings for a government office to get something done, that time savings benefits the individual who's making a request and the benefit of the credential actually has direct value to that person for what they're trying to do. Those combinations are absolutely critical and I applaud you for doing all of this. Thank you. Do we still have Jeremy Grant here? I'm going to steal a line that he said, we can't build identity or what did he call it? It says we can't build identity or we're a bunch of identity weenies building identity for other identity weenies. And so we can't be identity nerds trying to build this really small use case of like, Yeah, it'd be great to use a verifiable credential to… I don't know, Timothy, what's a really weird use case? You can probably think of one off your head. What? Okay. You got a use case? Oh, yeah. What about the beekeepers license? Okay. Beekeepers license. That's a pretty small use case. And does government go and actually check beekeeper licenses? So, but we have to build identity for people that it's going to have value and we have to meet them where they are. How are they going to get value?

How is government going to get some value? And I think that's also where I said we have the ability because we are a monopoly to solve the catch-22 of well let's create that instance where both can get value and we're already spending money on it. So it's let's move those resources to actually realize the savings that can come from that. All right. So who has ideas of how we can work together with other government entities?

Hello, hello. My name is Mariano, Mariano Green. I'm from Mexico City. I'm very glad to be here with you guys. Even though that I'm born Mexican-American, I'm more Mexican than American. I live most of my life there in Mexico. So I have learned a lot with you guys how we can implement. We have been working with clear companies, try to like develop the Mexican an environment there. But we came to the conclusion that it has to be a grassroots movement. It has to be with the communities. The community has to endorse their own, not only the identity, like yes, identity has to be more broad, but it's something that this movement has to be more locally. I have been talking with some of these persons here and a lot

of those persons came to the same conclusion, you know? And that's the way that I think personally the human being has to like has to move towards to that because if not that will happen with centralization and control power. We all know that. So this idea of stay indoors, I will say it more like community indoors. That's my grain of salt. I like that community indoors. One of the I had the opportunity I think it was as representative Chevrier still here. She invited me to speak at one of her events for Stand for Health Freedom a couple weeks ago. And we had a really interesting discussion of you mentioned community of how to decentralize the proofing process out into the community. A lot of cities and towns and school districts or even our post offices are in the community. Do you need to go essentially to a DMV to do proofing or can we have lots of entities doing it? Move it out to the community so there's more trust because these are their neighbors that work out there. If you can standardize the identity verification and proofing process, there's some real low-hanging fruit and we can eliminate some of those inefficiencies or barriers for people that can't get it currently. And if you could just go to your local city recorder or your local treasurer or your local postal office, why don't you have all the options? And that's, I think, a great way to get that grassroots going of those communities that want it. We know Utah County and some small cities have been saying we want it. If we could build it, bring it out to them. Pat Brooks with the state of Missouri judiciary.

I'm not sure how many people here are familiar with the standard called NEEM. Anyone familiar with NEEM? NEEM is the national information exchange model and that started as what was the predecessor of that was called GJXDM and that was a global justice data exchange change model. And what you're talking about doing here is following the same path that that program followed. You have a grassroots follow along with the gentleman just before that people had a need to do something and the standards were established and not so much in legislation but in adoption from a technology perspective to say this is how we can get the work done. Going back to the comments of publishing schemas, publishing standards that people can adopt. And the organization that started that was a multi -state organization and it was in the justice domain. And what happened to it was it saw a need to exchange information in multiple domains. And identity is one of those domains. And so I would encourage you to make sure that if we're establishing a standard for multiple states to follow that we look at if there is RA something at the national level that could be more readily adopted than maybe building something from total to scratch. You have governance that you have to issue. You have to have vitality issues. You have technology standards. But I think this is a wonderful idea and I think that it can be well served to see how others have done something similar and going forward.

Michael Proper, I have seen this dilemma that we've been building and sitting upon for years, well over a decade actually, and the solutions right in front of us. But will we really see it? And what I mean by that is we know that we've all got to come together and adopt a system and we know that there's a political side of it and there's a technology side of it. But what if they really existed? Would you really adopt them? Would you really use them? Even if it had the beekeeper scenario built into it and 86 other certificates, permits, licenses that already exist and already use these standards. standards. Would you really use it? Would the state of Utah really use it? Would the state of Arizona really use it?

Would Mexico really use it? Mexico doesn't know. It's a community thing. It's the person that would actually be the ultimate decision maker if they're going to use it. That's why MDL has such… I think Arizona has a ton of adoption. 17% adoption. If we could do that with a decentralized system where the individual actually will throw.

If we could do the same 20% of MDL energy into a decentralized system and people knew about it, the awareness and adoption would go through the roof because it's around the individual first. If we want to be true and honest around what's going on, Cindy who has a son that's dead is one very small proof. It's not just a person's life and their breath that's gone. It's their time on earth that sucked from them, from these corporations. Whether they're slumming around pornography or they're slumming around video games that are taking the youth. Or we're allowing AI to be able to replicate and take not just from the next generation, the grandparents, our parents, our children. This is our responsibility. In Hawaii, it's our kuleana. It's our time. And I look at what Chris and Phil and Sam and Tim, these people have dedicated decades of their life. I too, 19 years, $28 million of my own hard-earned money into this technology for the state, for the countries, other countries, for no price. Would you really adopt it? Would you really look at it? Because if you do it here and you can do 10% of what we're talking about, other states will get on board with it. If you give it back to the individuals and truly let them own their own identity, their own data, their own payments, their own assets, and pass it to the next generation, instead of the state sucking out hundreds of millions of dollars of unclaimed assets because people don't even know where they are. The technology is here today. It's not just in some proprietary phone that's really open. It's not about a phone. Even though Cindy's parents, Cindy's son, that's how they that's how he took his life. That's how they stole him. As a parent of six kids, I want to be able to say, I did everything that I could. So that my son that went to this university And when I sat on the board of this university, when her son killed himself, was responsible enough to say, you know what? Enough is enough. We got to stop the games. We got to come together with the policy. We got to come together with the technology. And we have to actually act. Charlie Kirk was killed 500 feet from here, 150 feet from here. The action behind his choice network was all what it's about acting. It's about doing. The technology's here. People have seen it. People can live it. They can adopt it. You can download it. Utah life. Go to your app store, download it, log in.

It's simple. This isn't hypothetical. These are real systems that really function better than Bitcoin, better than Ethereum, better than the banking system, better than the current identity management systems. And I'm sorry, I want to slow down and I want to just let the process take its process. And Chris, I emphatically support everything that you're doing. But we don't have time. We don't have another 10 years for another decade worth of kids to not only stick bullets in their heads, but to stick bits in their heads that takes them away from the life that they've been given. It steals their time. It steals their souls.

It steals their hearts. I'm sorry that this means so much to me. But I can see the solution. Thank you, Michael. And our timeline is that 10 years is data governance. Our time on lists is as fast as we can. Senator Collin Moore said this on KUTV last week and he said, we have to get it right. You know, we don't want to cause more harm, but the time is as fast as we can get out there. So parents and individuals have the tool. So that's our timeline and that's our commitment is we're trying to get it out as fast as we can. Obviously, we have to follow the law, but we understand the importance and that it's needed now. This is not something that we want regular bureaucracy to just sit on. And I think that's why we're all here. This is not normal bureaucracy. This is not a normal meeting. This is something different is happening and this is going to get done right.

I'm not going to try to follow that, but my question is for those in the private sector partners who are helping us, what can we do to help move this faster? Understanding that we have to do it right, but how can we move faster? Tim, should we go here?

I've been working in the space for over a decade now. It's like trying to push a really heavy rock uphill really hard. A lot of failure. A lot of things we tried in different ways that didn't work and then very optimistic about SEDI and what's happening in the state level? I think the answer, I've always been a small government guy. And the reality is that now that government is getting into the digital identity space, it's several decades behind private industry and private industry has turned the digital identity space into this just incredible surveillance mechanism. But now government's getting into the digital identity space. And government at the end you said has the monopoly on whatever it decides to do. Government will dictate how much privacy or freedom or autonomy we have or don't have in the digital realm is my prediction after all I've seen. So to answer your question about how to finally solve this, I think Utah has to be successful in getting other states and create momentum. I know that Utah has deprioritized interoperability, which is really interesting when you look at Utah's hierarchy of values for a lot of identity initiatives specifically, but technology in general, the highest priority is interoperability. And so what gets sacrificed is security and privacy. Specifically with the MDL standard, there was a country that said we need to have phone home and they didn't call it that.

We need to have server retrieval and it was baked into the standard because a country demanded it. Different culture. It's not our culture. Someone else's culture demanded it. It got baked in. A bunch of us squawked about this a couple few months ago and they have now separated it thankfully. But the point is that was made earlier.

We as Utah need to do what's best for Utahns if even if it means that we're not interoperable with the rest of the world. We have to deprioritize interoperability and do what's best for the privacy and security of our citizens. And so what I think is the answer to your question is to get Utah to be more than just Utah that's doing this, to get some representatives from other states who are here to actually move forward and join. It reminds me of the end of the movie, A Bug's Life, where the grasshoppers were were bullying the ants through the whole movie. And finally, at the very end, the ants realize they're more powerful if they lock arms. I, I, this digital identity community thing is so big and I see grasshoppers everywhere who are the bullies in digital identity and I think the only way we do it is Utah's an ant and we need to lock lock arms with other ants and scare the grasshoppers out of this space.

My name is Jeremy Furster from Cardano Foundation in Veridian and I'm going to say that I'm in the technologist camp or stakeholder group. And normally when speaking to policymakers, there is a view from technologists that you're way off the mark with what you're presenting as policy. However, that is not the case at all when coming to SEDI. And I think the engagement that you receive and the interest that you're receiving, the reason why it's so high is because fundamentally the policy makes sense for the constituents. We've been able to demonstrate with our demo that today SEDI is not just policy. It can be codified. It can be implemented. And I would ask, do you see a path where you can eat your own dog food? Because when you look to implement SEDI, you need that first user.

A very easy low-hanging fruit could be having a SEDI wallet to have a passwordless login to a government website. And if you do something like this, it's very low risk to actually get things started and have something put into production that is end-to-end.

Well, I'm going to make a quick comment because I actually got some text. I get texts every weekend, just you guys know from citizens that are like, I hate this. What are you doing? And they actually sent a text and you may have been about to go here where they're going to say, Hey, They were like, what is this Utah ID I now need to use to log into a system? It's a just a single sign-on portal, which any it's any sin-

gle sign-on system is going to have tracking. It's a centralized. Yeah, it's a username password type system. So there's low hanging fruit. And I think there's discussions already happening. So we know constituents have identified the system.

They actually have said they want SEDI on. We have the man here in charge of it. So we have a couple of initiatives that we're working on. And we have first of all, we have our we have in a beta form our next version citizen portal which we branded MyUtah and you'll probably see Governor Cox making an announcement about this early next year. But the goal and we don't have this quite here yet. I'm looking at but we'll be getting there where we hope to be able to have people authenticate with a SEDI credential for that. And we don't quite have the SEDI credential yet to do that, but we want it. And so that'll be one of our first and best use cases to get that going. And we also want to look at state systems. So we have our 22,000 state employees and we have identity and access management that we log them into our state system and we like to have a SEDI credential so that they can log in as employees and we would like to move away from passwords even with our multifactor.

We don't love them. We'd like to move to a more secure SEDI type credential for login and use in identity and access management systems across the state. hopefully that'll be one place we can start to get rolling. I'm Mark Allen. I'm with Citizen Portal, my brother today, Ancestry.com and we're trying to work towards government transparency and accountability. And Chris, you're spot on when you say that most of the state of Utah is not compliant. I think our stats show about 15 % of public meetings are being recorded gavel to gavel. I think some of the low -hanging fruit that I'd suggest for authentication and certification would be within your own home of state government.

I have been branded a vexatious litigant as of last night, but the judge of Charlie Kirk case because I asked for a court record. Let that sink in. I asked for a WebEx video hearing. I can't get anybody in the state of Utah to give me a certified record. When I'm doing grammar, they say, oh, it's a duplicate request. I want state certified, authenticated, genuine record that I can take to the bank and say, I'm innocent.

But when I ask for that, I get branded a vexatious litigant. So my admission admonition as a state and county delegate is also with what we're doing is clean up your own house first, not at your level, but at the clerk level where they won't give me a certified record where the keyboard is the weapon of today. And I'm the first victim probably in the state of Utah of lawfare. And, but if I had everything that you've been talking about today, SETA, ability to authenticate, ability to track back into the record to see who was the ghost that hit the keyboard word to backdate a record by two years. I wouldn't be as smart as I am now, but I've learned a lot in the last 10 years and I'd say Utah, let's get it right first. Let's start in the judiciary where the problems are. And then my personal identifying information, I can control and protect it, but mine's been scattered to databases around the world. And I don't know how to undamage what that's been done. We also have a problem with all three branches of government in Utah.

They're not watchdogging each other. There's not enough healthy friction. I'd like to see a little more healthy friction between stuff. So, and this is not specific SEDI related. It really is civil rights, my personal protections. And I don't need to go deeper down that because I really appreciate what you're trying to do. If we would have had implemented what you did, what you're talking about 10 years ago, my life would be totally different. But I've seen how China weaponizes and surveils. I've been surveilled in Utah, Provo, Utah. So court certified records, definitions are really important. What's a certified record? What does a certified record look like to you if I go down to the court and try and get a digital copy or something that someone will go, oh, this is, we made a mistake.

How do we undo the mistake. So that's a personal use case scenario, but I think our courts they don't on a standard basis do a transcript. You can't get a certified record unless I pay for it. $2,500 for me to get a certified record. So I would start within the court judiciary and start certifying records and start doing court transcripts if it were me. That's low hanging fruit that would benefit most of Utah. Thank you, Mark. We are All right. We're going to have one more question.

We're at time, but Jeremy Baker is a Utah privacy commissioner. If you don't know, governance structure in Utah, we have a whole commission dedicated to privacy. So take that back to your state if you don't have one. Go ahead, Jeremy. So I'm actually going to take this from a different perspective, and this is from my private sector experience with being someone that integrates security and identity into software applications. And it's related to how do we get the private sector to adopt this. A lot of private sector companies like even Roblox or others, they end up using identity providers like AWS Cognito, Okta, Azure, B2C. All of those they've added in different integrations for identities. So you have like your social media logins that are allowed in there as well as like the current adoption of passkeys, which has been really slow to roll out across the entire private sector even though they're significantly better idea than passwords and usernames. But to get SEDI adopted across all of them, I think the framework like what we've talked about today having an open framework where those major identity providers could bring that integration in as an authentication service under the umbrella to have it as an option to add directly into applications that are currently working with their products. I think that that would be a significant push for adoption. – Thank you, Jeremy. Okay, we're going to close up first by raising hands who wants to help get SEDI going forward. Okay. And if it's not up, okay, everyone got it up. And that was the worst thing to do because I am shameless. One of my tricks in government is I have no problem asking for your time. So you will all be getting calls in your states to move this forward and we'll be shameless together to take this national. We are so thankful that everyone came today. I know this is a long day and this was a lot of information, but you now are ready to actually have the in -depth discussions. So we will go back.

We'll do some of the grunt work to get organized. We'll set up and we'll make our materials available. We'll reach out to the states to get at least one more formally involved so we can get seDI.gov .going going at seDI.Utah.gov doesn't have the same, you know, ring to it. We want seDI.gov. But we'll get rolling on that and And we're going to meet back here again in less than six months for the next SEDI summit. And from what we're already hearing, it's probably going to be twice as big. And by that point, with the pace we're going, not only will we have more legislation, but hopefully we have a lot more to share so other states can take it, steal from our tax dollars and take it to your state so you don't have to pay for it. And let's get SEDI rolling. So thank you everyone.

Thank you.

TALK IX

L

lunch-00-20-51--00-32-51-Jay-Stanley

STATE ENDORSED DIGITAL IDENTITY SUMMIT · TALKS · 11:55

— Thanks, Chris. Sorry to interrupt so many great conversations, but this is when I've been told to speak, so you're stuck with me. Again, Jay Stanley with the ACLU. I've been working for a long time for the ACLU. I started in 2001 and I've been dealing with a lot of tech issues since then. Things are constantly new, so it keeps us on our feet. And the ACLU has always been against a national identity system. We don't like a national ID for a lot of reasons. For one thing, it does take away your individual identity and it makes it a bureaucratic artifact and it threatens to create a system of tracking in which government agencies and big businesses have a unique identifier, a key that you are stuck with and you cannot get rid of that will track you across different areas. If one company is tracking you here, one government agency is tracking you there, and somebody else is tracking you there and they all have their silos, that is good for privacy. A national identity system creates a unique identifier. And we've always… So we oppose RealID because it basically turned our driver's licenses into a de facto distributed national identity system. Now, a lot of the bad consequences that we feared that would come from that have not materialized. It's sort of a low-key national identity system that we have. But a lot of that is because it's physical.

And what we worry about with a digital identity is that it will fully bring forth the negative potential that Americans across the political spectrum have always worried about with a national ID system. And I work on privacy issues. I have always gotten support from the left and from the right. I think among all the issues the ACLU works on, it really is the least partisan. And I think with the national identity issue, in some ways it is it is the left and the right against people who aren't really thinking about it and just marching forward. And I think that, you know, the driver's license started as a license to drive. You need to, it's probably in the public interest to license people who are drivers, but it has become something much bigger than that. It's become something much more central to our society. And as it moves online, it's going to become much, much bigger. And that is the goal of the digital identity proponents, of course.

So, we, I was ignoring the digital identity issue for a while because it seemed like nothing was going to happen. And then in around 2001, I wrote a big report because it seemed like this MDL thing was really happening in the States.

We were starting to see a lot of uptake. It was like, okay, this is real again. And we were very concerned because it was created by an international group, the ISO, which included, as we know, some big tech companies like Apple and Google and some government agencies like DHS and AMVA. And we don't know who else is on it.

I asked them who else was on the committee and they refused to tell me. And also you couldn't even see the standard without paying thousands of dollars and it was copyrighted. What kind of a way is that to make public policy? Maybe that is okay for light bulb standards or something like that, but for something that's going to be at the heart of the relationship between government and the governed, that was very dubious. And in fact, the ISO standard, the MDL standard, reflects the interests of who was at that table, which is the verifiers. We're going to do everything possible to make sure that nobody can ever fool a verifier about their identity, but it doesn't reflect the interests of the holders, the people who are holding the identity, the people whose identity has been granted to them by the DMVs under this thing. So, we did a report in 2001 called Identity Crisis. And then over time, me and my colleague, who is our technologist and others, refined our thinking and put out a last year a set of state legislative recommendations for state legislators with proposed language. It's kind of a work in progress. That's a version 1.0.

We're working on a second version now. But the question, you know, we've been hearing talk all day today. We need a privacy protecting digital identity system. We're going to have digital identity needs to be privacy protective.

Well, when the rubber hits the road, what does that look like? What is privacy protective? And that's what we set out to answer and put some meat on the bones there. And so this report basically has 12 items that we think state legislature should pass and basically say our state shall not have a digital identity system unless it has these technological qualities and comes with these policy envelopes and protections because you can't do everything through technology.

Although we think you should do as much as you can with technology because it's much harder to change and to back out of. So let me just I'm going to mention quickly we're going to run through the 12 just so you have a flavor. You can look it up if you're interested in any of those more. I might highlight one two, which might be interesting that people have thought about. And then I'm going to finish with a couple thoughts and then I'll be done in the next five minutes, which is how much time I have. So one of the big features is no phone home. If I show my driver's license to a liquor store clerk, they look at it. End of story. Nobody's the wiser.

If it's digital, there's the capability to create a record. And in particular for the issuer, the DMV, the government or the companies that are their contractors to see that that I've done that and what time and at what liquor store and everywhere else that I show my ID. Locker's offices, etc. And it needs to be built without that feature. There should be no phone home. We can build it. The ISO standard allowed for that. And that is something that we've been working on. We think that a key privacy feature is verifier unlinkability. If I show my digital driver's license at six gun shops or six liquor stores or six doctor's offices, the companies involved should not be able to… First of all, if I, for example, if I have to prove I'm over 18 or I'm over 21, they should just get a binary which a binary bit which says, yes, no, this person's over 21 and it's encrypted and proofed. But there shouldn't be a unique signature or any other unique identifier that is passed over as part of that that can later be used to correlate all your presentations. And there are there are readily available cryptographic techniques that can make that possible.

And that needs to be a part of a privacy protecting digital identity system. New Jersey, which may have outside of Utah the best digital driver's license law, has this. They say their law says, which was just passed a couple months ago, the system shall ensure that a digital driver's license or non-digital license includes techniques and methodologies that ensure that multiple presentations of non -unique data by a the holder cannot be linked together by one or more verifiers.

The selective disclosure we think needs to be mandated that basically you should have the right to disclose the minimum amount of data that is necessary for the transaction. You are over 21, you are not. You are a resident of the city without sharing your address. Whatever the use case may be, people should… relying parties, verifiers shouldn't get any more than they need for that transaction.

Here's an interesting one and I talked about this in one of breakouts, there shouldn't be a government's kill switch for your identity. And I think that's where the philosophical approach of the government endorses your identity and doesn't create or bestow upon you your identity. But in bureaucratic sense, that's what is happening in some senses. And there is a real potential that the government is going to have a significant power that it has never had before. Three steps. Step one, create a digital identity system. Step two, allow a bunch of dependencies to be built on that. And some of our proposals are try-

ing to avoid this so that your digital identity doesn't become the key to actually doing your ability to do anything in life, which is a real threat. Make it so you can't live without the digital identity system. And then because some governor doesn't like your politics or whatever, pull the rug out from those people, revoke their digital ID and make them an unperson and unable to do many things in society. And that is a power a government has never had before. But with a central digital identity becomes a very real possibility and danger. We think that there should be verifier accountability. You have to verify yourself to whoever wants you to prove something about yourself. You should have a verified identity of who that is and make sure that you actually are identifying yourself to who you think you're identifying yourself with. That hasn't really been implemented. We call for an open wallet ecosystem so that people have a choice of wallets. We think that like forcing people to run government code on their personal phones is bad idea.

It should not be government code. If it is, it should certainly be open source. But it's better to have the free market provide lots of different wallets provided that they meet security standards so that people can pick whose wallet they want to put it in whether it's Google's or Samsung's or Apple's or maybe you know Mozilla's or a privacy protecting group that you have more trust in or what have you. And we call for and one of our biggest things is restrictions on ID demands. The real threat here is that once this infrastructure is created, it makes it really frictionless to present your ID. When you go into websites, unless they really need you to approve ID, they do not ask you to approve your ID. They're not going to like make you get a camera and go in different angles and show your ID. It's too big an ask. They'll scare away customers and they know that. But if they can send you a pop-up says click here to send us your digital driver's license, they will. They'll have a bunch of incentives to do it for advertising and to make sure you know who you are as cookies go away potentially. for security and forensics. And so the real danger is that we wake up one day, say, oh, you want to watch this YouTube video? Well, just click here to send us your digital driver's license. You click no. Sorry, we can't. It could be used for surveillance pricing where companies set their prices for you based on who you are and everything they know about you rather than offering the same price to everybody else. And there's a lot of abuses there. So let me just… I'm running out of time rapidly. Let me just finish up by saying that that the really important thing here is that legislators decide. We have our 12 things that we think are important parts of privacy.

Maybe some people disagree with we're going to have disagreements over some of those and the details and they're complex. But I think we should all agree that it should be part of the political process. It should be legislators who are making these value judgments. We obviously don't want legislators getting the nuts and bolts of technology, but this should be back in the hands of the legislature. It should not be in the hands of secret international committee, China and Russia.

or I'm part of the overseeing committee of the smaller committee. It should not be technologists in the DMV who are just been told to implement it or get to make the decisions in the dark of night. It should not be unaccountable private organizations like AMVA. No shade on AMVA, but they came out of the old world where it's about licensing digital driver's licenses. And this is much, much bigger than that. I'm sorry, licensing your ability to drive. This is much bigger than that. And it's, it can't be left to a private organization that asserts copyrights in its policy documents. It won't let people publish them. let alone not being subject to the privacy action FOIA and so forth, checks and balances on government. And it should not be the TSA. The TSA right now, because of RealID, has the power to shape what our digital identity system looks like. It should be legislators and the political community. And one of the things that's really fantastic about SEDI, and I think that there's a bunch of traps and there are questions and I

don't know what it'll look like as it evolves and what the ACLU you will think of it, but I think it's fantastic that these decisions have moved from people who are not involved and are not going to be affected to the political level, which is where it belongs. Thank you.

TALK X

L

lunch-00-33-30--00-41-34-Jason-Chipman

STATE ENDORSED DIGITAL IDENTITY SUMMIT · TALKS · 08:04

We are probably the primary voice when it comes to privacy among private groups in Utah. One of the things that we did was we actually helped get Chris a job. We were very heavily involved in getting the privacy commission created. So you owe us one. Don't forget that.

So a couple other things that we've done in the privacy space. A couple of years ago, we became the first state in the nation to require a geofence warrant. If law enforcement want to use geofence, they got to have a warrant to do it. We did that. Two years ago, we became the first state in the nation to put guardrails around the use of real-time surveillance. To my knowledge, we're still the only state that actually has that in statute. So this is something near and dear. This is one of our core privacy core principles as an organization among many different things. One of the things that I learned a long time ago was to hire people that are smarter than you. And this person that works for me is smarter than me. And so she wrote this for me. And I'm going to read what she said before I give my remarks. So, as you know, countries like the UK and the EU at large are pushing hard to create a mandatory surveillance regime through digital IDs. These are intended to trace every activity, every service, all of these things that we've been learning more and more about. We supported Senate Bill 260 as a vehicle for rigorously examining the risks and potential pitfalls of the digital identity systems, including a study to probe whether a truly voluntary and untraceable option is actually feasible in practice. As the state prioritizes teen mental health online through privacy-invasive age verification, we recognize the intent behind exploring alternatives like SEDI. But we have to be straightforward about it. ID systems, even innovative approaches like SEDI, amplify government involvement in identity from static issuance to dynamic, always-on oversight that could over time challenge user autonomy as seen in many international examples. We appreciate the legislature's commitment guided by the state's Privacy Advisory Board to examine these realities through the study process. We lend our support to continued research and discussion with a focus on the high bar of preserving constitutional protections and individual freedoms amid these systems inherent challenges. The most fundamental reason for our engagement in Senate Bill 260 is an appreciation for the study's focus in probing the tensions between digital ID frameworks and the privacy and autonomy they seek to preserve in service of Utah's broader goals of safeguarding individual liberty. However, there are some things that we would like to see changed, kind of like the ACO you said. We want to require opt-in for all data beyond absolute minimum proofs, just like they said. I can see a scenario where you go into an establishment where you need to show your ID and all they need is a picture to prove that you are who you say you are and your date of birth. And they ask for everything else because they want to package that off and sell it to data brokers because it's a way for them to make money. So, we have to be able to say, no, you can't do that with this. You know, we have to say that you don't need that and you don't you cannot require that for somebody to use your service. We want to bar government access to SEDI data via third-party brokers. This happens all the time. There was a presentation in a committee hearing on Wednesday here in Utah where a transportation company talked about how they gathered Bluetooth signals to track traffic patterns in Salt Lake City over a period of time to determine where construction was affecting travelers. And then right after that, there was another presentation about population data and how they were gathering all that. And Representative Chevrier had some very good questions that went unanswered in that committee hearing. And I will say that those people who were speaking at that, they weren't really happy with her tone throughout that. After the hearing, I heard them talking outside. So that's something you want to follow up on next time you talk to them. We also want to establish a right of action against government agencies for violations. The easiest way to hold somebody accountable

is make them accountable. Make sure that they don't do the bad things. Tell them they're going to go to jail. Tell them they're going to lose money. This is something that I propose whenever cities try to violate. This is so I used to be a legislator in Missouri once upon a time.

I'm still recovering from that. one of the things that we did as a legislature was we put a cap on the amount of fines and fees that cities could impose on anyone, on their citizens. And if they exceeded that, the state could take action. One of those cities no longer exists. We disincorporated them and they got annexed into surrounding cities. Cities have no constitutional right to do anything.

There's no government agency that has a constitutional right to exist. There's a fallacy about co-equal branches of government that That doesn't exist. That was made up by President Nixon a long time ago because, well, he was weird. The fact is the legislature is the supreme branch of government because it's the only one that can fire members of the other two. And we have to remember that. And this is the reason why going through the legislature for this is so important and not allowing the agencies to just kind of do whatever they want. You know, we're working on a bill this year for privacy that doesn't allow law enforcement to do anything with surveillance unless the legislature has already given the go -ahead. So there are no free trials, no demos, no free stuff from the feds. And then they come back and say, well, sorry, it's helping us. We're doing stuff. It's like, no, you can't do that. And it provides a private right of action, removes qualified immunity. It makes them accountable for doing things they're not supposed to do. We also want to impose ironclad bans on unwanted federal overlays and revocation overreach. State-to-state portability is a goal, but the federal systems like real ID expansions to co-op SEDI without consent eroding state control. The study must recommend explicit prohibitions on such national integrations preserving voluntary state cooperation alongside strict due process requirements for any endorsement revocation to guard against escalations of centralized power.

So in a nutshell, we are very much in favor of the study. It's going to show us what we can do. It's also going to show us what's going on that we should be worried about. But, you know, this is very much one of those things where we're trying to shove a camel through an eye of a needle. And if they can't figure out a way to do it, we need to slaughter the camel and burn it to the ground. That's essentially going to be our stance. This is good until it's not. And once it's not, we're coming full guns blazing at you. You know, so we've shown that we have been effective in some of our other endeavors in the state. And I'm hopeful that I hope this works out. You know, I'm not going to lie. I hope it works out. out. I got five kids.

My oldest is 16. I worry about what could happen to them. As a legislator, I've heard all of the horror stories from my constituents about my kids doing this. Can you do something? Can you do something? You know, if something happened, can you do something? You know, sometimes government does need to do something.

Sometimes they don't. But legislators, having been one of them, often feel like they have to do something. And sometimes the best thing they can do is nothing. But I really do hope this can work out the way we want to. But if it's not. Somebody has to be held accountable and we have to be able to just say it's not going to work.

Remember that other people, other organizations have different incentives. And so until they realize that our constitutional rights are the primary incentive and nothing else really matters in the situation, we're not going to be able to be successful at this. So I'm hoping that Chris and his team and this process

will lay out all of the pros and cons. All the things we can do, all the things we shouldn't do, you know, so it lets everybody know ahead of time kind of what we're getting into. Thank you very much.

TALK XI

L

lunch-00-41-41--00-48-06-Jeremy-Grant

STATE ENDORSED DIGITAL IDENTITY SUMMIT · TALKS · 06:25

You have to admit, we've brought a diverse group of opinions today. And as Governor Cox has said, we do know how to disagree better in Utah. And I assure you, I have not slept well for four years balancing all of these different requirements, but we're doing a good job. I am really excited to announce the next person who's going to address us, Jeremy Grant. So he's managing director in Venable, Venable's LLP technology and innovation practice. this. But I think most interestingly and most importantly, he coordinates the Better Identity Coalition and has been working in the space for decades and is going to be an extremely valuable member as we move forward to learn how to work with those he represents. Thanks, Jeremy.

Hey, thank you, Chris, for the invitation to come out and great meeting so many of you today and also seeing a few old friends. So Better Identity Coalition, I just want to say from the start, we're really thrilled to see this today and that if there's one thing we have been consistently calling for since the coalition was first formed in 2018 and published our initial policy blueprint.

It's that as a country and an individual state, we need to be thinking about this constructively and strategically. We have not had a strategy for digital identity in the US that outlines what good looks like and how to get there or for that matter what the bad outcomes could look like and how to avoid them since the last time we had a strategy was one that I ran. It was an Obama administration initiative that was launched in 2011 that was called the National Strategy for Trusted Identities in Cyberspace. And there were some things that worked well in that program and some things that didn't. But I think one thing that everybody should take away is that for the last 10 years as our peers across the globe are all thinking about identity different ways and they're thinking about it strategically, we've been tackling it really on sort of a siloed approach, something for age verification, something for government login, something perhaps for KYC for banks, but there hasn't been a holistic approach. And so this is what we've been, in some cases I would say, begging policymakers to take on. And so seeing what Utah has done and other so many officials today from governor's offices and state legislatures and other states, it's awesome to see. In terms of who we are, so I mentioned my time running the NSTIC initiative. I was also dual - hatted as the guy who led the digital identity research and standards team at NIST in the DC area and helped launch the privacy engineering team around identity that still does a lot of great projects today on that front. The coalition is an interesting group. So we've got big tech giants that some of whom people have been calling into question what they want today. So Apple's a member of Google, Microsoft. We also have companies that help pioneered or led efforts in decentralized or self-sovereign identity companies like Gen Digital or Block. The coalition's really driven, however, by those that I would say are on the buy side of identity. Our origin story was around this time eight years ago, there was a little breach that happened that wasn't in the news of all from a company called Equifax where they lost 141 million social security numbers and it also raised some bigger concerns around identity in that the default way we would prove who we were online say to open a bank account or apply for a government service was to use knowledge-based verification. Here's five questions from your credit report or you can answer them. It must be you. Well, we all know that hasn't been true for a long time given all the breaches we've had. And so we were largely founded by the buyers of identity who just need better solutions to run their businesses. So think companies in banking, payments, fintech, healthcare, telecom. We have some of the vendors at the table as well, but it's a pretty motley assortment and the companies probably don't agree on much other than we should be thinking about digital identity strategically. I called Jay in 2021 when he published his paper, which is a great read by the way on the risks of digital ID because he talked a lot about the shadowy identity industrial complex that was pushing for things like mobile driver's licenses.

And I said, I think I'm running that. But the good news is we mostly agree with you on the issues that are in the paper. We actually think they did an amazing job at highlighting the risks to digital ID along with potential decisions in terms of architecture or policy on how you could be designing things like MDLs. Chang was mentioning before the great work that's happening at NIST right now through their National Cybersecurity Center of Excellence to come up with a family of standards and our playbook of standards and best practices to help states including you know the folks who are here set a high bar for security and privacy and ensure interoperability. Five states are participating alongside Apple and Google and seven banks and a lot of other big players right now. It's a great example of how you can actually get interest from all across the board to collaborate on you know achieving good outcomes here. So you know we're out there you know quite a bit sometimes excited about MDLs not because we think the DMVs are the most awesome place for identity to be housed. But it is at the end of the day, the one place that most adult Americans go through and prove where they are in person to get either a driver's license or a non-driver state ID card. And so we think as we look to get away from companies who are basically trying to hoover up a bunch of data on us and guess who we are. Look, I live in DC. I went to the DMV three years ago to get my real ID driver's license. It was not a pleasant experience. I've gone through a similar process with the post office at the who partners with the State Department to issue passports. If I'm trying to open an account online and there's a legal or regulatory requirement that they need to know who I am, why can't I ask the DMV or the State Department to vouch for me? That idea that we should start to give people the ability to ask government to provide this to them as a service in a way that actually is secure and privacy enhancing, that's really what we're calling for. So I mentioned before we published a policy blueprint at the end of 2022. We published one specifically for state policymakers. I hauled a bunch of them over in my suitcase this morning and they're in a stack downstairs if you'd like to grab one. But I think my final message would be for those of you who are engaging on the policy side of this, we'd love to work with you. So please don't be shy about reaching out. You know, our goal, look, the reason our members are all funding this effort is because they want to have an organization that can engage and collaborate constructively on getting these issues thought through properly and, you know, get good outcomes for everybody. So appreciate the invite again and look forward to talking to you. Thank you. Thank you.

TALK XII

L

lunch-00-48-12--00-52-35-Christian-Reza

STATE ENDORSED DIGITAL IDENTITY SUMMIT · TALKS · 04:24

We are next going to hear from Christian Riza, who's from the he's the Utah chapter president of Stand with Crypto. And for those who aren't aware, the crypto enthusiasts I think are pretty excited about the decentralized identity approach.

And the Utah Blockchain Association has gone way out of their way to bring together stakeholders and even many in this room that they've been working with for years to help educate them on SEDI and bring their support to help make this happen. Christian.

So I do I represent Stan with crypto. I am the chapter president for the state of Utah. And it's my rep it's my responsibility to represent the 20,000 pro crypto voters in the state of Utah and mobilize them on initiatives that really align with our values. Now, you're probably thinking, okay, crypto, that has nothing to do with SEDI. Cryptocurrency has nothing to do with SEDI. Why are you here? What does this matter?

Our assets, our finances and our assets have been digital for years. We've just never had the ability to take ownership, to take custody and to have those in our control. And likewise, our birth certificates, our social security numbers, all of these things are already digital. They live in a database somewhere. We've just never had the ability to have true ownership and custody over those pieces of our identity. Recently, I had the opportunity to go to our community and really ask them and have some honest discussions and a bunch of different chats throughout the state. And, you know, all of these people, the crypto and blockchain people are extreme skeptics when it comes to this kind of stuff because frankly, you know, all they know is we want to have control over our assets, our finances, all these things. We don't want the government involved in these things, right? So at first gut reaction of, hey guys, what do you think of this initiative? It was, no, no, what? No, please don't do it. What are you talking about? Like, no, this is terrible. And what I did was had everybody actually dig in and And Will Segos as well, which is he's here. We had some conversations in deep, in-depth conversations with a lot of these community members and had them really dig into the underlying protocols. They're technical people, right? And after having reviewed the information and the framework and how it's being proposed, it was an emphatic yes. And I've got some quotes here from some of these people, which in this case, it seems great. It seems too good to be true. I'm surprised the state is backing this. Definitely the best approach that I've seen, this actually makes sense. I like it. There's no way the state of Utah would go for it. And my favorite one, if the state of Utah did this, I would be proud. I'm not a policymaker. I don't come from, you know, I'm not here representing a big tech enterprise. or anything like that. These people that we represent are just people.

They're regular Joes, regular community members, and they deeply care about their privacy, their control, their ability to hold these different things, parts of their lives, their identity, their assets, and these things. They deeply care about these issues. And based on the SEDI framework, some of the things that ACLU has said, And, you know, the way that SEDI is structured and framed today, the community emphatically wants to support this. And so I guess I'm here to say that, you know, as a community member, as a person that represents people in the community, you know, if you move forward with SEDI in this way, the state of Utah and other states that are here represented that will support that. And we hope that you will. So, thank you.

TALK XIII

L

lunch-00-52-44--00-58-51-Scott-Stornetta

STATE ENDORSED DIGITAL IDENTITY SUMMIT · TALKS · 06:10

this. I'm not going to say which company. We have had the first company that is now reincorporating in Utah because of what we're doing with SEDI. I'm not going to say what state they're leaving from, but this is a valuable economic, it's a value add. People will come to your state because they want privacy. People are crazy. craving this type of freedom. So you can think about that. What is it that this offers that other states or other countries can offer? And it really will be an export, but it's going to attract people to your state. And I think for all of you, the message is resounding. This is something people want. We just have to work through and figure out how we're going to get there. All right. The last comments we are going to hear from, I think this is probably the coolest person we have in attendance today. So we have Scott Stornetta, a co-inventor of the blockchain and mentioned in the Satoshi paper, for Bitcoin. Sorry, where do we have Scott? Oh, right here in front.

I think Stuart, my co-inventor, is actually the coolest person here. I'm Scott Stornetta and I speak for the trees. Actually not. I just for years wanted a situation because I'm such a Dr. Seuss fan to be able to give that line, but whatever. I am grateful for the opportunity to speak briefly.

By way of introduction, Dr. Haber and I began an effort more than 30 years ago at Bell Communications Research, part of the old Bell Labs family. As research scientists, we published an influential paper outlining a method to create immutable digital records through widely witnessed public events through widely witnessed events made public. This is what we now call a blockchain. While I don't endorse any specific cryptocurrency or blockchain application, the data integrity mechanisms that Stuart and I pioneered have proven reliable and they now safeguard over $3 trillion in digital assets. That's trillion with a T. What does this have to do with identity? Well, let me address it first philosophically and then technically. Philosophically, the SEDI initiative holds that a person's digital identity is an inherent human right in the digital age, created and controlled by the individual. Yet, as Locke and Rousseau argued, individuals choose to enter a social contract with a community governed by the state. This creates a need to link personal identity with state requirements, hence the concept of state-endorsed digital identity. Technically, this aligns very well with the principles Stuart and I use to construct the blockchain. To build trust in immutable records without relying on any single third party, we spread the trust mechanism across the user community. This is what is now commonly described as the principle of decentralization. Similarly, decentralizing digital identity, keeping it under individual control, well reflects the inalienable rights. You know, they wanted to correct Thomas Jefferson and call those unalienable rights, but Virginia prevailed on that one. Inalienable rights articulated in America's Declaration of Independence and echoed in many declarations of human rights both in Europe and in varying degrees throughout the world. I must emphasize that I did not participate in any of the work leading to this summit. So I'm offering an outsider's perspective. Born in Maryland and a New Jersey resident for over 30 years, my view is not Utah-centric. though I do confess my wife is from Ogden and Dr. Haber similarly confesses that he has at least flown over the state in route from New York to California many times. Okay. Point is we've been entirely external to the process, the legislation and the technical details. With that said, I endorse this effort. Not because I agree with every part of the legislation or descriptions. because no initiative is perfect at birth.

And this one is evolving. I invite you to listen to a later speaker today, Scott Kelly, who will talk about the word iterative. I'm a fan of it. But we shouldn't let the perfect be the enemy to the good. And so I invite you, especially those from other states, to join this call. Not because it's flawless, but because your

involvement can refine it. Not because you fully agree politics is the art of the possible and it often requires compromise but not compromise of principle. But because good people united at a good cause can achieve more together.

I close with a unifying phrase from late 17th century Europe originally in Latin but I will spare you that part. in necessary things unity in undecided things liberty and in all things charity if we're guided by this principle i'm confident that we collectively can achieve something of value to many many people across

TALK XIV



morning-00-03-34--00-18-20-Chris-Bramwell

STATE ENDORSED DIGITAL IDENTITY SUMMIT · TALKS · 14:48

I'm the director of Utah's Office of Data Privacy located in the Department of Government Operations. I want to thank the Herbert Institute of Public Policy, the Department of Government Operations, and the Utah Legislature for all helping to host this event and also to UVU for allowing us to use their facilities. I also want to thank UVU. We had many employees and students and interns help to bring this event together for the last few months and so we couldn't do this without the work that they've been putting in. And I want to thank all of you for coming to Utah to participate in this event. We put a lot of thought into how would we actually host an event to cause change. And we thought about just doing a virtual event and we knew that it's going to take a lot of passion and a lot of work to pull off what we're going to be proposing today. So it was important to see who can we get to come in person that cares the most about it to help us build what we are going to be proposing. So I thank all of you for coming. Those from states, we have 12 states represented. Those from academia, those from executive branch agencies, those from legislators. I think we have more than a dozen companies represented. We have concerned citizens. We have private interest groups. We have the national ACLU. So we have the start of what I think is going to be a really great consortium.

Now, the purpose of today is simple. We invited you all to come here to one, receive an education about a very complex topic, is digital identity. The second reason we've invited you is to help you understand the problem and what we think is a really big opportunity for America to lead out. And the third and final reason that we've invited you here today is to actually invite you to join the SEDI consortium, the state-endorsed digital identity consortium, so that we can move forward and work together on what we think is a big opportunity for America. Now, I am an optimist by nature and I'm very optimistic about digital identity if we do it right. And I believe that we can build technology that reflects American values, that protects freedoms and strengthens families and builds trust in the digital world. But I am also a realist about why this effort is needed. I am very concerned about some of what I see happening not just in the United States, but what is happening around the world. There are many of you in this room that have expressed those same concerns. That is why Representative Cutler and Senator Kullimore sponsored Senate Bill 260 this last session, the first state-endorsed digital identity bill in the and the nation to begin addressing these concerns.

So I want to share with you some of our concerns. I am concerned for my kids and your kids who can engage online and video games and social media and they do not know and we do not know if the people they are engaging with are actually who they say they are. I am concerned for my and your elderly parents and grandparents who continue to be taken advantage of by individuals pretending to be family members in distress. I am concerned for young men facing exploitation and sextortion online. This is one of the fastest growing crimes in America and in Utah facing our young men. They are being driven to despair and even suicide in a world where anonymity and manipulation coexist without protection. I am concerned that fraud enabled by identity theft and impersonation is now costing the United States hundreds of billions of dollars a year. I am concerned that algorithms based on profiling and scoring are influencing our behavior and quietly shaping the concept of even freedom and free agency. I am concerned that the free market is being distorted, that those who control personal data are facilitating monopolistic behavior that maximizes exploitation of individuals for profit instead of driving a free market based off of competition and best prices. I am concerned that nation state attacks on future digital identity systems will occur and we have to assume digital identity will be compromised. I am concerned that government-sponsored digital identity systems both in the United States and around the world have been created that are capable of tracking, surveilling, and controlling. I am concerned that governments, corporations, and technol-

ogists are rushing to create digital identity systems that are compulsory and are required and that these are being created without the comprehensive governance its frameworks and protections needed to protect individual rights. And I am most concerned that in democracies around the world, digital identity systems are being designed and implemented in ways contrary to the first principles of America's founding. And that is that individuals have individual inalienable rights that they are endowed with that is innate to them, including identity. Government does not give identity. Government does not create identity. And any identity system built on the premise that government is giving it to you means that they can also take it away, which is in opposition to this founding principle. So the truth is there is no trust in the digital world today. We don't know who or what is real.

We do not know. You do not control your digital identity. Usernames, passwords, even mobile driver's license can be taken away. They can be compromised. There is currently no national strategy for digital identity and we know that there are many, both foreign and abroad, who would love to control your digital identity and compromise it for their own gains. So the dilemma before us is that if we do nothing, we will be left with a system created by others that do not share our same values. But this is not the end of the story. It is the reason that we are here. All of us in this room are in a position to influence. Some of you have the power to create laws. Some of you have the power to create and dictate public policy. Some of you have the power to create technology. Some of you have the power to fund new businesses to create the solutions that we need. Some of you have the power to create governance frameworks. And some of you have the power to create standards. And some of you just have the power to raise your concerns and create trouble for the rest of us, which we need. So you all have something to contribute that is needed to create the solution necessary to address our concerns and create a better digital identity. So there is a path a path forward by building digital identity in a manner that prioritizes rights and dignity. This is what state endorsed digital identity is all about. So I want you to imagine for a minute a future. A future 10 years from now after we've put in a lot of hard work.

We need to agree today and in future summits what that work is going to be. But a future where our fears about digital identity theft, manipulation, impersonation, exploitation, loss of control have been replaced by trust and authenticity. Where parents know their children are safe online. Where our elderly are protected from scams and impersonation, where there is trust that government is protecting your digital identity and rights above all other interests. That is the world we need all of you to help create. So through the SEDI consortium that we are proposing and inviting you to join today, states will work together to define an American model for digital identity, one that protects citizens, and instead of importing surveillance and control-based standards and technology from abroad, we will export freedom by design, showing that privacy, security, protection of rights and protection of individual rights and innovation can coexist. The benefits and capabilities of SEDI will be profound. It will provide the foundation for individuals and businesses to derive value and utility for the free market, to create new and and innovative solutions. We know there will be new solutions for proof of identity. There will be new solutions for replacements of usernames and passwords. Imagine that if you don't have to worry about your passwords being compromised. There will be new solutions for consent and management and agreements that individuals control. There will be new solutions for delegation, empowering families and guardians and organizations to act safely on behalf of the vulnerable and those they serve. There will be solutions for agentic AI where artificial intelligence operates with your explicit authorization and not in your place, extending your agency rather than replacing it. So many of you are probably wondering, how would we ever get from the current state to that future state? And we do that the same way all great things are done. And

we have to do that together. We have to create a plan. We have to agree on our values. We have to create a structure. We have to roll up our sleeves. And then, as my teenagers and young kids like to say, we have to grind. We're going to have to get out there and actually do the work to make it happen. And it is going to take a long time. And under the SEDI consortium is where we can take the fruits of all these labors that we are about to do and give them away to everyone else so that they can follow us. We know not everybody is going to be able to do this. We don't have all 50 states here. Not everybody has the funding, but but we are public entities. We can create it and we can give it to them for the good of everyone. So the work we're going to do is going to include comprehensive governance frameworks, model legislation, resolutions, executive orders, defining SEDI requirements, technology and policy controls, conformance programs, RFIs and RFPs. We're going to have to do security assessments. We're going to have to do continuous engagement with civil rights groups and watchdogs. We're going to have to have absolute transparency and we're going to have to have absolute transparency and we're going to have to have going to have to do much, much more to move the digital identity market in America to align with what are going to be the SEDI standards.

So today you are here to learn about digital identity and some of the principles that will guide the creation of state-endorsed digital identity. You will understand the concerns and the opportunities ahead of us and I hope you will accept our invitation to join. But to end, I'm going to teach you just one of the founding principles and requirements of state-endorsed digital identity. This is the very first one that we identified when Senate Bill 260 was written. And this is probably the most foundational and fundamental difference compared to what you see happening in the rest of the world. Identity belongs to the person, not to the government. The government's role is not to create or control identity, but to endorse and protect it as a matter of public trust. SEDI recognizes it is the role of the state to act as a trusted endorser, verifying an individual's digital identity and then issuing an endorsed credential mathematically bound to a digital identifier that individuals alone control. The state does not create the individual identifier cannot revoke it. The state simply endorses that the person is who they say they are and then provides a credential that empowers the individual to say to the world that I am me and the world will accept it because it has been endorsed and backed by the state. The state will have no control or ability to surveil or to track the usage and the state cannot take away the underlying digital identifier. The state has no role to take away anybody's digital identity.

So with that said, we have a very busy day ahead of us. This is mostly about introductory education. This is going to be a very fast-paced style to get you information. We'll have a couple breakouts throughout the day where you can ask questions and you can participate and learn what it means to help define policy and technical controls. We're going to end at the end of the with an hour-long discussion of how can we actually move forward together as states. This morning, the run of the show is we're going to have Ryan Hurst speak to us and educate you on what is digital identity. We will then have Cindy George speaking to us about her family's experience with sextortion and impersonation and the impact it has had on them through their son's suicide. We'll then have a legislative panel of Senator Kullimore, Representative Cutler, Representative Chevrier, and Representative Shepherd to discuss with you the importance of this work, why they are supporting it, and why you should be a part of the consortium. We'll then hear from Daniel Hardman who will teach us about the current lay of the digital identity market. Phil Windley will explain why Utah is the first state to formally take the decentralized or first-person identity approach. And Joe Jackson will teach you why we are moving forward with backward compatibility to help the entire market move forward. So with that, Ryan, I'll invite you to come up. Thank you.

TALK XV



morning-00-19-05--00-29-15-Ryan-Hurst

STATE ENDORSED DIGITAL IDENTITY SUMMIT · TALKS · 10:09

As 10 minutes is a short period of time to get quite a bit done. I am… looks like this mic is live since I'm going to leave this here. I'll make this quick here. So, I've been in working for companies like Google, Microsoft, Amazon, and others for the last 30 something years focusing on technologies like authentication. And so, today what I'm going to talk to you about is what is digital identity. And this was a little bit of bias in this, But I'm going to try to get through about 30 years of lessons in what I have left here. So identity is not new. This is a picture of a clay tablet from 1900 BCE. Merchants used to put their thumbprint into these clay tablets so that you could authenticate that this is legitimate. This is a point that authentication is of transaction actions is something that we've been worried with since the dawn of time and this is the earliest example I could find.

But we've been trying over and over to solve this problem and each generation of has to approach this problem slightly differently for the environment that they exist in. I've got a few examples that exist in this timeline below here. We won't go through them today, but at the end of this presentation, I have a QR code that talks a little bit about successes that you can follow for a paper on successes and failures in this space as I'm going to go fairly fast here. So what identity is not is as important as what identity is. It is not a better document.

Digital identity is materially different than the one-time issuance of a document that we would use to authenticate at a government office or when traveling. It is more of a living type of credential that lives for a long period of time. And that living nature means that this is a governance problem. This is not a technology problem. So why is this important? Because seven out of ten of the projects that I've looked at over the last several decades and then you'll see those in that white paper have failed and they failed because they looked at this as a government not as a governance problem but as a technology problem as IT or procurement. And so that's why it's important that we're all here today and I'm really excited to be involved in this conversation. So this is a model shift.

State issues document you carry it it, verifier inspects it. That's what we're all used to. But as we look at what does it mean to have civic digital identity, it's much larger than just my name is Ryan Hurst. There's many endorsements about Ryan Hurst that might be material to the verification. I'm a motorcycle driver.

That is certainly a driver's license thing, but I also am a parent. I also have other attributes about me that are important and the state is involved in many elements of those and being able to prove that to third parties is becoming increasingly important and I'll talk a little bit about some of those cases. This expanded role of identity in the online world is something that means that we have to change the way we look at this problem and we have to start with a set of guiding principles which is why again I think SEDI is an important project. So one of the biggest differences that we'll see as we look at digital identity versus our paper history historical analog is that they actually codify the policy that you all come up with. And this is important because now when you make a change, that digital document and the systems that verify it may also need to be changing. So we have to think a little bit more holistically than that issuance moment. We have to think about how are we going to manage this over its entire life cycle. If we think of this as we bought a solution to print these digital identities and declare victory, we will fail. That's the number one pattern we see when we look back at the failed systems.

So what is maintained over time? Well, there's a lot of status changes. Licenses get suspended, whether it be medical or driver's license or credentials may get compromised and may need to be replaced. Algorithms may need to be changed over time. These are probabilistically secure methods to

prove these things and so we may have to change them. For example, post -quantum cryptography is coming in the future. And policies change continuously faster than ever before. And this all means that how we govern these systems is going to become increasingly important. So if we look at these failure patterns, there's many that we can point at. One of the ones that I like to point at is the German solution. Germany came up with a national ID card that was technically pure and perfect. From their definition of technically pure, and perfect and it was an abysmal failure. Nobody adopted it because the governance model was not right. They put the burden on the constituents. They made it very complicated to adopt. They didn't have a core utility. So it was massive amounts of money spent with no return on investment.

So not something that we can afford. UK is another great example. I can't go into the details today, but they wasted $233 million in a decade of time roughly because they didn't look at this problem holistically and they didn't measure it in the right way. Some of the successes we can point at Estonia. They started with a list of three or four utility scenarios that they were going to enable and as a result, their system continues to exist. We can look at Sweden. They looked at what was practical to deploy and achieve results with and their existing exists and is loved. Very rarely do you find a government service that is loved, but I think that it's fair to say that that particular program is. U.S. government has its own as well and there's others that have elements of success but we'll go into those later in that paper I mentioned. So why is this important? I'm from the state of Washington. We have the honor of I believe being the largest COVID fraud for distribution of COVID funds. I think Africa got more than we did. So this is a big problem and it's a problem because we didn't invest ahead of time. We didn't build the infrastructure to enable the government to be able to identify its citizens online and we can't let this pattern repeat again. So why does this matter now? I mentioned COVID, but it's much larger than COVID. We can look at AI, for example. Today, I can generate a fake utility bill, birth certificate, and whatever easily with just a few types of on my keyboard that you're going to believe is legitimate. I can do real-time deepfakes that are nearly impossible to distinguish. The voice will be the same. You cannot rely on a video call to authenticate who you're talking to anymore. And so this means that we have to invest in infrastructure to be able to strongly authenticate who we're dealing with so that we're able to prevent mistakes like that one from happening again. I also think it's important to note that in the context of security breaches, 88% of security breaches tracked by two companies, roughly that figure, I think they have two slightly different numbers but very similar, were just using stolen credentials. They didn't hack anything. They logged in. And so it's important that we pick strong technologies that solve for the problems and don't have externalities that make things worse. This is you are the foundation of how the federal government interacts with Americans. You are the foundation of how the rest of the world interacts with Americans online. And we have to solve this problem. This is not something that we can ignore. So why does this matter for you? you don't manage digital identity in abstract. There's a lot of different examples of this that exist inside of your organizations. You may not think of them as digital identity.

Different people have different definitions of this term, but I view all of these things as part of the life cycle of identity. A birth certificate is my child's ID until they're old enough to get a driver's license. Many of these other elements, my wife carries our marriage license because she's from another country. When we travel because it's part of her digital identity. All of these things are part of that package that we have to use, that the state produces, that the rest of the world relies on to verify who we are. So before you commit to any approach, I think it's important to understand what digital identity tells you or what questions to ask. I didn't word that particularly well. So since this is a codified thing, the question becomes when policy changes, how does the digital identity get affected? it. Because it's policy-based, how are you

actually going to create demand for this thing? If you have no utility function for your deployment, some scenarios that are enabled that are actually meaningful to your constituents, they're not going to go through the hassle of doing it no matter how beautiful the solution you build is. Because it's how are you going to maintain the entire life cycle of this system? This is like any IT investment in that respect.

And because it's civic identity, you have to pay attention to who's excluded. My parents are not particularly good at using things online anymore. And so we don't want to exclude an entire segment of our society and there's of course other examples as well. So what does success look like? You've identified anchor tenants, you've budgeted some amount for continual governance, you've addressed how are you going to deal with interoperability with existing systems, you understand how your platform is related to the various dependencies that you have, and you understand the equity implications for this system and how are you going to manage them? And you've defined success metrics and how you're going to continually revise those metrics so that you can make sure that your system is delivering on the promises that you should have set out to do. So that is my presentations. Ladies and gentlemen, I appreciate your time today.!

TALK XVI



morning-00-31-20--00-55-41-Cindy-George

STATE ENDORSED DIGITAL IDENTITY SUMMIT · TALKS · 24:17

But I'm here to tell you about my son's story and the horrific experience that he went through. First of all, I want you to get to know my boy. This is my Jake, my baby boy, one out of my two kids. And, oh, those dimples. Everyone commented on those cute little dimples. I was this fifth grade teacher, which every kid's nightmare, right? To have your mom as your teacher. But I was this fifth grade teacher, so I was able to see what a kind -hearted, thoughtful, and caring kid this was. Not just as a mother, but as a teacher. I remember one day after school, he came up to me and he kind of had glassy eyes, you know, almost teary. And he said, I said, what's wrong? And he said, mom, something happened today. And first I need to give you a little background. We had a little boy in our class that had a medical issue that didn't have control of his vowels and oftentimes he smelled and the kids really made fun of him. He had no friends. He was picked on. Don't touch these guy cooties type stuff. And Jake was his friend. Jake had a group of friends that he hung out with that he loved and they loved him, but he saw this little boy and he befriended him. And after school one day he came up to me and he said, Mom, he said, they're being so mean to Brian. And I said, I said, what happened? He said, well, at school at recess. He said, I said, come on, Brian, let's go out. And we were walking out on the playground and my friends were like on the basketball court and saying, Jake, come over, come play with us. And he's like, yeah, let's go play. Come on, Brian, let's go play. And we got over there and they said, just you, Jake, not Brian. And I said, well, Jake, what did you do? How did you handle that? And he said, I just turned to him and I said, nah, it's okay. Brian and I are going to go play over here. And so he actually gave up his friends because he saw this little boy I had no friends. That's the kind of kid my Jake was.

When he was in middle school, he would spend his days off. He'd say, mom, can I go to school with you? And even in high school, mom, can I go to school with you on his days off? And he would come to school with me and he would help tutor the kids. He would help them with math or he'd read to them. The kids in my class always knew Jake.

Jake loved donuts. This was his last birthday. I made him a cake out of donuts and he said, Mom, that was the best cake ever. He also loved about the donuts every year when he was in high school and he had his own money. He would show up on my birthday and he would show up with three dozen donuts so he could give donuts to my class for my birthday. That's the kind of kid Jake was. He also was an animal lover.

This was his best buddy Bosco and he loved dogs. He loved animals. He also loved music. When he was a little toddler, he'd be in the backseat. It was amazing because I'm big into music, so I'd have the music blaring and he'd be in the backseat as a toddler in his little car seat going to the beat of the music. Just even as a little toddler, he loved music. He loved everything and a big variety. He loved Linkin Park all the way to Elvis and Buddy Holly and I was like, wow, that's a huge, huge thing. One of my sweet memories is on Mother's Day, he bought me tickets to the Styx REO Speedwagon concert, but it wasn't for me to take just anyone. He gave me one ticket and the other one was for him. And we went as mother and son and rocked out to Stug's and REO Speedwagon. That's the kind of kid Jake was. He was a great student. He got his associate's degree while he was in high school, which was a great achievement for him. Most of all, Jake loved his family. My two nephews were Jake's best friends and they did everything together, including pranking me. That was their most favorite thing to do. And then I got my first grand-baby and that just made Jake an uncle and he was so proud to be Uncle Jake now.

Sorry, I'm having issues. Okay. Jake and I had the fall break and so we went on a road trip together. Just the two of us. And we went to the Grand Canyon. We went to Bryce and just had mother and son time. These are the pictures. from our road trip as well as the one that's up here. This one he had never seen the Grand Canyon and when we got there it was full of clouds and so that was his picture with the Grand Canyon was clouds in the background. This right here was our last trip together. Two weeks later is where I'm going to pick up with the story.

It was the day before Halloween and I was a teacher and I had a teacher work day and I was sitting at my desk when I got a call from the Millow County Police Department. I said, is this Cindy George? And I said, yes. And he said, do you have a son named Jake? Jake? And I said, yes. And do you have a place in Kanosh, Utah? And I said, yes. And that hit me. Jake's at our little place. We had just little getaway place there and he must have he must be there and they must think that he's breaking in or something like that. And I said, yes. Yeah, that's my son. And they said, he has taken his life. in your home.

I just argued with him. I said, you got the wrong kid. My kid was not on drugs. My kid did not drink. My kid was not depressed. This did not make sense. It couldn't be my kid. And I argued with him until they described his car and explained that he had taken a gun and he was gone.

The rest of the day was kind of a blur. And why? Couldn't even fathom how this could happen. And they the police department, they faxed a couple of his letters. He wrote seven letters. This is kind of kid Jake was. He wrote letters to his sister, to his friends, to his nephews or his cousins. This one's to me. I'm just going to read part of it. It says, Dear Mom, I love you so much and it pains me to write this. I wish I could live with what I did. I know this will be hard for you, but I need you to continue on with your life. I hope you don't think too bad of me for what I did. I know this is sudden, but the hell that I went through Sunday through Thursday was too much for me to handle. I love you dearly, mom. You will always be my mother and I will always be your baby boy. But, Jake, it still didn't make sense. What could possibly make him do this? And so four months later, the police department gave me back his phone and the last letter that they held. And it says, My dearests, (and this is for all of his friends), I'm sorry for what I have done, but I have nothing to live for anymore. I have made a huge mistake that I can't live with. Look at my phone and read the messages that are in the Kik app. Start with the girl profile named Alona Home and then move on to the profile just for fun. These messages will explain everything. From Sunday to Thursday, my life has been a living hell and rollercoaster of emotion. The one person that owns these two profiles will be using Facebook to ruin my life. There's a good chance I will lose my job and get kicked out of school as the person attacks me there using Facebook. I urge you all to control what happens on Facebook as much as possible. This person claims that they will copy some of your profiles and attack your friends also. This person attacked my three most important things being my school, my job, and my family.

Please don't change your lives for me. Hold your children and grandchildren close. I love you all. Jake. So, I'm just going to take you a little timeline. I got his phone back and I read. I just took it aside and I read the whole conversation. And I understood the pressure and the hell that they put him through. This happened in five days. I was with him on Sunday and Friday. He was gone.

I read the conversation how the predator talked him into sending him a nude photo. After grooming him, they talked him into sending one nude photo. And kind of like, I'll send you one, you send me one. Talked him into it. I saw the high pressure that they put him in. And then I saw how they sent him names of family members and said, we're going after them next. And I think that's where it put Jake over

the edge. So I'm going to take you a timeline what his life went through in five days. on Sunday they get him to send after grooming they got him to move to the Kik app I'm not sure where the original source came from because he was on some dating sites and he was on Facebook I believe it came from Facebook but I'm not sure on that but they got him to move to the Kik app which is common or this type of a thing After they got him to move, they said, now we've got you. Or after they got him to send a picture, they said, now we've got you. Just added and saved all your Facebook friends on my laptop. I am going to send them your nude photo and post it all over your friends' Facebook timeline and also to your job on UPS Facebook page. But I will not do that if you send me the money right now, okay?

After constant threats, high pressure, get there, get to the Walmart, get an application. Let me see the application. Get to the ATM. Let me see the money. He was having to take pictures of everything. They were on him. Just didn't give him time to even process and think this through. He finally at 7.06 that night, he makes a payment of $300 at a Walmart at Saratoga Springs to a Marie's Abril in the Philippines. Then Jake asks for her to please delete the picture like you said.

This was the response he got. he said, they said, do you know what a genie is, Jake? And he said, yes. He says, well, you are my genie today and I have found you. So you have to grant me three wishes. And he says, which are, which you means you're going to have to make three payments.

After begging for her to leave him alone, saying, I'm just a college kid, please leave me alone. Jake ends up back at Walmart that night to make another payment of $130. The torment and constant threats continued for the next few days. Jake paid them everything he had, $680. And after fulfilling the three wishes that she required of him, Jake then begged her to now please delete the photo.

And the reply was, you work at UPS. In two weeks, you'll have another paycheck. And Jake realized this is never going to end. He says, please delete it. I can't live the next two weeks with you blackmailing me. I gave you his total that he had just given his last payment. And he said, he said, you won't get any more money if I'm not here.

The reply was, five guys committed suicide because I posted their nudes and ruined their life, but I never care because it's their choice, not mine. You will be the sixth and I still won't care. On Thursday, Jake buys a garden hose. and heads at a Home Depot in American Fork. And then in Richfield, he buys a ream of paper and a box of envelopes and he goes to a hotel. And I assume that's where he wrote all of his letters. And he left one on the desk in the hotel saying the person that was in this room is going to take their life. Please contact. And he said Brandon George, which was my husband at the time, his brother that lived in Kanash and said, please contact him. I'm going to be out in the West Desert.

Then on his way out of town, he bought a helium tank, which was later found empty in his car. Along with when I got in his car, I found the hose and it was black on one end. And the helium tank was empty. And I think that he tried to take his life using that method. And I think it was just taking too long and he could not do it.

and he knew that my husband at the time had a shotgun in Kanosh and he found the key and he took his life. The hell that I go through thinking of those last moments as he's sitting there in so much torment and having to pull that trigger because of these evil people and what they did. No mother should have to bury their son. And it was so pointless.

I could not catch this person. I was told because it came from the Philippines, there was nothing that could be done. There's a program on the National Geographic called Trafficking with Mariana Van Zeller. They contacted me out of the blue. I don't know how they found me. And they said, we want to do your son's story.

And we want to go to the Philippines and try and find who did this. And so she came to my house. They did the interview. And then they proceeded to investigate. And they found the source in the Philippines. And it was a call center. A huge call center. This is going on and hitting so many of our children. It's a big business there.

She actually talked to one of the people that does this and he was hooded so all you could see was his eyes. She said, do you know that people are killing themselves because of that? And he said, yeah, I watched one of them do it. That's the kind of evil we're talking about here. Something has to be done. Brandon Guffey, a state representative in South Carolina that I have spoken to, had lost his son Gavin, his 17-year-old son Gavin, to sex extortion. And after his son died, he actually got contact. He was contacted by the perpetrator. And they sent him a laughing emoji. And it said, did I tell you your son begged for his life? That's the kind of evil we're talking about here.

This is coming from Nigeria. This is coming from the Ivory Coast. This is coming from here. We need to do something to warn these kids. I cannot catch the people that did this to my son. Brandon Guffey, I saw on his Facebook about six months ago, he and his wife were holding a set of handcuffs on his page. And they have Gavin's name etched in the in his handcuffs. And they went to Nigeria and they found who did this to their son. And they extradited them and they've been charged. What a great thing that they were able to do that. The Philippine government were not so accommodating when the National Geographic went over there. They know who started the whole thing in the Philippines and she's been arrested and then let out.

I asked for your help because I can't catch them. My son died so needlessly. I can't catch them, but the only thing I can do is warn others. Please talk to your grandkids, your kids, your neighbors, your nephews. Talk to them so they won't take the bait. That's the only thing we can do is educate so they won't take the bait.

And we need to also talk to them and let them know no matter what, no matter what is happening in your life, that they can come to you. I wish Jake would have been able to come to me. I wish I could have comforted him and said, it's okay, they can't destroy your life with a picture.

Don't ever think this This can never happen to my child, my nephew, because I can testify to you that it can happen to the best of kids. Thank you. Thank you.

TALK XVII



morning-00-59-44--01-29-30-Legislative-Panel

STATE ENDORSED DIGITAL IDENTITY SUMMIT · TALKS · 29:43

Do I have it on? Is it on? It's on. Okay. Thank you. For me, there's a lot of distrust in digital platforms that are going on right now. And there's, as you saw today, and as you already have known, there's been many people that do bad things that will really scare people. And one of the things for me is that your personal data is just scattered and having the opportunity to have Utah lead in this area and to be able to make it that we and recall that we own our data. The government doesn't own our data. We own our data or we should at least. So it's important to me that we have privacy, autonomy and with our state having the consent of the governed I have many constituents who reach out to me even as of yesterday telling me a digital ID is not the way to go. But as you'll hear today, there's many reasons why we should go with it. And I have a firm belief that even before I took office that we have the right people in the right place here. And I think our other states need to join us with this one and making sure that we don't do like other countries have done with our data. Senator Collin Moore, Representative Keller, You got SB260 passed unanimously through the House and the Senate a couple years after there was a different digital identity bill which I've heard there were pitchforks in committee hearing and it did not come out.

Why are you supporting and championing SEDI? I'll start. I've been fortunate to be able to work on technology policy in the Senate over the last several years. It started with data privacy just in the consumer aspect and recognizing how important that is. We've since passed a government data privacy, the first of its kind, which I think is also important. But in the middle there, we're also working on social media bills and social media policy because government with technology typically is always, well, government by its nature is reactionary, which I don't think is necessarily a bad thing. But in some of these technology policies, it moves so fast that we are not in front of this and we are allowing people to be exploited. And the way the internet came up was using data. The way this has been monetized is using our data. Facebook, Instagram, Snapchat, Google, any of these services are free to us because, as we all know, you are what's being sold. You are the commodity. and that in and of itself is scary and that's what we're having to deal with as social media right now is social media companies have exploited that to the detriment of our kids. They're not only affecting their mental health but they're causing actual real world harm like we just heard about and it's terrible and putting that same type of power into the government's hands that has even more control over so many aspects of our lives is just super scary. and something that we need to avoid. We need to flip the script of how this is being developed and what this actually means. We need to put the power back into the citizenry, into people. People are not commodities. And that is what the digital age has created. We are all commodities now. And I think that's one of the fundamental evils of our day and age is when we commoditize human life, that's problematic. And if government is going to do that, that's even more problematic. And so we needed to find a way to flip the script. SEDI, the bill that we passed, is really just the first fundamental step. It's laying the foundation for flipping the script and saying, no, the power is back in the people. The power is back in the individual.

If we look back at history, history shows us that fighting technology advancement is often a futile effort. Whether you're a buggy maker, maker trying to put laws to stop the automobile or trying to fight industrialization that technology is going to move forward because there are so many benefits to society. So we have a choice to be proactive and influence and control these standards or we can stick our head in the sand and say, no, I don't want this. I don't I want to fight it. And I choose to try to be part of the solution. Digital identity is coming. I think we all, especially everyone in this room recognizes that. And the only choice is do we want to influence the standards and the adoption of this to protect freedom and in-

dividual liberties or will we acquiesce to efficiency and monetization. There are bold visions out there for artificial intelligence. We hear all around us, hey, the future is agentic AI. We're going to have all these agents acting on our behalf, acting on behalf of an entity or software program.

The security concerns are very real. You are not going to feel a smart security person will not allow an agent to take on a task on their behalf if there is not trust. And as has been talked about, our digital trust structure is under constant attack right now. And in many areas it fails. So we have got to come up with a better system for verifiable credentials for trusting people and eventually entities if this agentic future has any chance of making a real impact without doing incredible harm in our society. I'm going to go off script here for the rest of the time.

Utah in my view has been unique compared to what I've heard actually from many in the audience and how we work together between branches of government. We have CIOs in the audience. We have chief privacy officers in the audience. We have legislators in the audience. We have civil rights groups in the audience and I've heard them comment of how is Utah able to do these things it's doing. So I'm going to ask this to Senator Kullimore. What is it that Utah is doing differently than other states and what should they know so they can go back to their states and replicate the success we're having across our government on both sides of the aisle?

Well, you know, we have to put we have to set aside our trying to be humble here because there are some things that work really well here in Utah and we call it the Utah Way. But the Utah Way really is just recognizing that we are here as public servants. We're servants of the people. And when you approach these types of policies, you have to have a little bit of humility to say, I don't know everything. And that's especially true in technology, right? Like I fundamentally believe in certain principles, but I don't actually know how the technology actually works, right? And so sometimes you want to implement a law and we're talking about very basic things right here, but whether it's like whatever the type of law is, I think it's critically important that you bring in all the stakeholders and who best than the private sector and academia. And so whenever we've worked on these policies, we have good working relationships between the Senate and the House. We have good working relationships between the legislature and the executive branch, the regulators who are actually enforcing this or implementing the laws that we pass. And it's important because the policy does not actually work if the implementer just has their own idea and goes a certain direction. And none of this actually works because most of the time people in government don't have the technical expertise to know what they're actually talking about. And so we have one of the shortest sessions, legislative sessions in the country. It's 45 days, begins in the middle of January and goes to about the first weekend of March. And we are a part-time legislature. That is becoming less and less a reality. We're becoming more and more full-time because really that January to March, that's game time, but it's happening all year round. And so we're meeting with stakeholders and most of the best policy that we pass involves academia, people who have the research and the background on their private sector, people who are actually developing these technologies or deploying these technologies or using them within their business, policymakers, and and the executive branch. And so I don't think we've passed any tech technological policy in the state of Utah without input from all of them. And sometimes it takes time. The consumer data privacy bill that we passed, I think we were the fourth state in the nation to pass it, but it ran for three years and we were getting input from everybody and it gets whittled down. We passed a digital asset bill that recognizes what digital assets are. And it started out as 16 pages even when it when it was introduced in the session and because of input it got whittled down and said no let's boil this down to the fundamental principles and then build on that and I think that's what we've

done here with SEDI is we haven't made this I mean it's policy it's agnostic to what the technology is and in fact the technology is not even out there right now that could be implemented but it's steering the boat and it's steering the direction of how that technology is going to be implemented and so So this is the opposite of being humble, but using humility to get to these policy decisions, I think is what helps drive the advancements that we've seen in Utah. Chris, I'd love to comment on that.

I think we have been successful as Senator Kolemore, and he deserves a lot of the credit for bringing people together, as do you, and making some policy. But it's premature to pat ourselves on the back yet and say that this great. We have some good policy, but we haven't seen adoption. And we can't do adoption on our own. We can't do adoption by just the legislature passing a policy. Adoption requires industry to come up with tools and use cases that are compelling. And also because Utah is small, to be successful, we need your help. We need other states to join together and show that we have enough of a consortium to get attention from the big players to say this matters and privacy and security and individual rights are important. So while we've had a little bit of success, we need to replicate that by having you join us and agreeing on some key principles and some key standards where we can move forward together and have a larger coalition.

Representative Chevrier and Shepard, I'm actually going to ask you the same question. You two probably represent some of the most conservative areas in the nation in Utah County. And the fact that this bill is passed unanimously, I think one is representative of the work done, but what is it that's different about this approach that is helping to win over or at least gain the trust of those that each of you represent?

– I can go first. So I think this is going to be off topic for a second, but it's really on topic. We have a system of government in Utah that is different from most other states, and that is the caucus convention system, which makes it so that the grassroots are far more involved with their legislators than they are in most states. And I think that that's been a huge factor because both Representative Shepard and I have been very involved in the party and in the caucus convention system. We have built trust in that arena that allows us to help transfer that trust to the legislature and to this technology that we're talking about. So because we have that opportunity to build trust, I think that makes it easier for us to help people understand because they're willing to listen to us because we have built trust with them through that system. Does that make sense? Okay. Okay.

Part of being elected, I had a town hall and I had experts in this area come and speak to those who came. And yes, of course, we use it through the caucus convention system that we have that allows us to have a direct report and be held accountable by delegates. And that is where you get the biggest pushback. In honesty, delegates are very engaged aged and they know issues and you can't hide.

And it's a great, actually a really great process. And I appreciate that. I appreciate the accountability. The delegates and my voters that I have talked to about this by knocking on the doors, they want us to leave them alone. They want to be able to be safe in this community, not only physically, but also digitally. And I believe that the relationships that having served on a state level in my party and served just across the entire state and worked in some national areas. I believe that that does open the door to when I bring experts to my district that they're willing to take a chance and listen. And it has changed the hearts of some of them to actually listen. Sometimes we get stuck in our ways and think that we have the answers and something is the boogeyman. But honestly, when you listen and Chris Bramwell has come to my district along with Timothy Ruff and when they have when they have spoken, people in my district

have listened and that's what I really appreciate. It's the opportunity to bring these experts as the good senator to my left here has mentioned to bring these experts and to trust them. We have to have trust in the experts and our people that we represent have to have trust in us. It's quite the partnership that we have.

Chris, can I add one thing to that? I think your policy of engaging with critics has been key to some of the success. There are some times where in politics where you don't engage with the critics, you say, I have a majority. I'm just going to pass this through. But that hasn't been how the privacy legislation that Senator Colomore has helped with or this legislation has been handled. You've held town halls where you invited critics to come and poke holes and things. You've brought in key members of staff and industry to come and engage and you slowed down the process to help convince the critics that this is the right way forward. And I think that made a big difference. Thank you. We have six minutes. I actually I'd like to ask does anybody have any questions? Any questions that maybe I can do it. What is this? The Murray show? Hi, my name is Sarah Thunberg. I'm the director of the Colorado Digital Service. Thank you for having us. We are watching very closely the work you've done and are talking about our own legislative agenda as the legislature, the legislators that moved a lot of this forward. Do you have any recommendations for those of us to take home with us? How we can model lessons learned, things now in retrospect, you think maybe we would have done it differently?

I'm not sure about the done it differently, but I'll tell you what we've done that has been working in it. And Paul, we well, we've all talked a little bit about it, but Chris has been very proactive in interacting with the people who are most likely to be the critics. And so Lisa and I have been able to set up these town halls where we can bring Chris in and have him explain to people. We've set up meetings with individuals who are all at night and on weekends, by the way.

Yes, it is out of regular business hours always. But we've been able to have discussions with the most vocal critics, people who have large followings on social media and we've been able to help them understand what it is we're actually doing because the reaction is visceral. I had somebody on Facebook this morning say to me that having you endorse digital identity was not on my bingo card. It wasn't on mine either, but here I am because I believe that this is the right system and I believe that we either have to choose a system that is going to respect privacy or we're going to get the other one. And so we need to make the choice and we need to make it soon. I'm going to make a comment too. You need a champion in your state. When Senator Kallamore and Moss created the CPO role, they empowered it to be a champion. You need every government entity fights for certain rights for the public. Public safety is to provide safety. Lands is to protect the public lands. Health and human services is to ensure there's public health and human service. do you have a privacy or digital identity champion in your state that is empowered to even fight for this issue? It's a balancing and that's part of the governance framework. So if you don't have that, get it going or be the champion. I'll just add, you know, as state legislators, what's awesome about being in state policy is that you can pass a bill and then you see the effects of it like almost immediately. And that's pretty rewarding. The downside of that is you want to do everything right now. And that's just not possible in these types of bills. We could have said you will implement these policies and forced it upon all the government agencies and all the political subdivisions of the state and cities and counties and it would have fell on its face and we would have got zero adoption because there's no way to even adopt it right now. We're doing about that with government data privacy. We wanted all of the cities, the counties, the state agencies, our schools and everything like that to adopt all these things and you will implement data privacy right now and you will implement all these retention policies and you'll get rid of

this stuff. And it's just impractical and you're setting yourself up for failure. And so you do have to reel back a little bit and say, you know what, I'm just gonna let's just pass this right now and let's build that. And even as Chris said, you know, we did a data private or we did the chief privacy officer a few years ago and we just keep slowly building on that. And so you do have to have patience, which is not always a virtue of state legislators.

– Good morning. I'm Shanna Durant with the Department of Public Safety. Thanks for having us. I have a question particularly for representatives. You say you've had a lot of town halls. I'm curious about how often you're having them and how much you're publicizing them because you say that we're talking to a lot of people who are social media influencers. But for example, Representative Cutler, my parents are actually some of your neighbors. So they've never heard about this until I talked to them. So how much is their public outreach to more than just social media and advocacy groups? And what can we do on our side as public entities as state entities to assist in that but also give other solutions to help you with an enhanced identity and what can we bring to the table in order to make it better.

Thanks for the question. I think that's important. So when I mentioned all these town halls, they were fairly targeted and the efforts to focus on the policy have been targeted with those who are probably the fiercest advocates either for or against. Let's be honest. Most regular people, most people, this issue hasn't hit them yet because there is nothing for them to adopt. today. Yes, they could adopt our mobile driver's license, which they may or may not be able to get through Homeland Security.

But we don't have a digital identity for them to adopt yet. So the efforts for advocacy were targeted at the key stakeholders, those who are most concerned about privacy, those who are most concerned about the technology used. And the next wave once we have a solution ready to be adopted would be to go out to all the citizens and explain how this is used, how this helps your life, how this can help verify ages on social media, how it helps protect their family from online fraud, which are real pressing problems that we all recognize and we're all trying to deal with. And we've got to get to a point where we have a solution for them.

So we have a policy solution today. We do not have a market solution until we get your help to agree on a standard and products. And I know we're out of time, but it's a little bit of a catch-22, right? Because if you go to a town hall, you've got, you know, I'll publish a town hall for thousands of people and the same 12 people show up and they're a little bit older oftentimes and they're not technologically savvy. and I would bring up some of these topics and my wife would be there and she'd be like, you've got to stop talking about that. They don't care.

It goes over their head and I think you're just scaring them anyways. So it's a little bit hard, right? Because you have to find these focus groups of people who are like keyed in on this, tuned in. But to your point, we've got to find a way that people understand that. I do believe this is critically important. And as we're moving into this digital age, if government does not get out in front of us, of this, it's going to be a problem. It's going to undermine democracy. So I will say the approach for communication though has been to communicate with every elected official where a town hall is being held. So UVU was partnered with for that. So they emailed every elected senator, representative, county commissioner, mayors in every one of the areas where the town halls were. So it was very much focused toward who are the people actually elected to represent the people. And then they were asked to communicate it out. The other thing I'll say though is This approach we're talking about SEDI doesn't even exist yet. We're so early in bringing the public in. You have 29 states already going down a digital identity path with mobile driver's

license or with W3C credentials or others in California or Colorado. This is unique of how early this is happening and people don't realize the train has already left the station in some way and we're having to move the market to try to move everything in this direction and we're needing to now come in with new policies and standards that we need to have all of that stuff now go back and be compared to to make sure it can meet them. Let's end 15 seconds. What's your pitch for states to come and join the consortium? I'll throw out on this. Many of us recognize that we let tech giants and the market determine the principles by which social media operates and and is distributed and affects our families. I think we have a lesson learned from that that we need to think carefully about in this AI world, how do we want to change that or influence how we control digital identity so we don't have the mistake of people who are kids accessing things they shouldn't. So this is a chance to help solve that problem with youth identity and to solve the economic problem of how do I put Greece in the system to allow economic transactions with trust to happen across the world? – I think we need 49 more Chris Bramwell across the country. That's a definite statement. And his team. I've seen the hard work that they do and the innovation. Utah's famous for being innovative. And we need the other states to join us. We can't do this alone. I think get your states to get a data privacy expert and an officer, a director, whatever your role is, all of the above.

And get your teams of the experts in the field. I'll tell you, I was on a panel here for synthetic data. I'm just a normal person just carrying the voice of the people. And I sat there and every other person had a PhD. I'm looking at one right now. And they are incredibly brilliant. They are the ones that have come up with the solutions. We're the ones up here that are helping to implement those across the country. So we need your help. Are you going to go? I'll go. Sure. So I have zero confidence in Congress getting anything done in this space. I have to the extent they get anything done, I have less confidence that it's going to be done right and not influenced by the big tech giants that are looking to again commoditize our data and our people. We need to get back to the principles of America that made us great. We are the laboratories of democracy and if we want to push this policy, we need a critical mass of states that align with with these policies, adopt these principles, and we will see mass implementation and mass adoption of these types of principles and policies because the states are going to lead out. And that's why you're here. We need you to help us. We need you to join with us. And your idea might look just a little bit different and that's okay. But if the states are working together and leading this effort, the interoperability that people are concerned about will happen naturally because we're working together and we don't have to rely on the federal government nor should we. That's not how our country was set up. We can find the solution here and we encourage you to join us. So I think since I'm last, this is what I want to say. We have worked together as a group in our state and we would like to now extend that out to other states and start bringing each of you in. We'll talk to you one-on-one. That's what we've done here. Anytime there's somebody who has questions, Chris will go and talk to them. Now there's only one Chris, so we can't we can't we don't want to spend him.

But what we can do is help people to understand this one-on-one. Nobody that we've talked to that I'm aware of has been opposed to this once they understood it. So I think the key is educating people on what it is we're trying to do and what the stakes are and the stakes are very high. So for future generations let's work together and let's get this done. Thank you. Let's give them a round of applause.

TALK XVIII



morning-01-30-34--01-41-59-Daniel-Hardman

STATE ENDORSED DIGITAL IDENTITY SUMMIT · TALKS · 11:29

– Hello. Okay, great. My name is Daniel Hardman. I am a CEO of a company that is in the telecom space. I've been working in identity for many years. And I got an almost impossible assignment from Christopher and crew, which is to try to summarize the state of the identity landscape in 10 minutes. And that's almost impossible because there's so much that's happening and that has been happening. So, you know, being a progressive thinker here, I said, I'll ask AI to help me find a list of things that are going on in the space. Now, I knew that this was going to generate massive amounts of stuff. So, I said, just find 40 headlines that have been in the news recently in English about things that are going on in identity that have been widely reported. So this is what it came up with and this is of course an AI summary but the point of this is not the specific headlines. The main point of it is how many of them there are and how hard it was even for the AI to pick from all the different things that are going on in the space. And as I was watching this list come in from AI what was going through my head that is that Billy Joel song, We Didn't Start the Fire. You know what I'm talking about? There's just so much that's happening and it's virtually impossible or overwhelming to keep track of it all. So to summarize in 10 minutes is very hard, but what I'm going to do is I'm going to try to explain how it looks to me as a practitioner in the space at a high level. I'm going to make some generalizations. These generalizations are partly subjective, perspective, but I think they're a useful mental model for people to understand if you're not thinking about identity all the time and you want to kind of wrap your brain around it. So, my generalizations basically say that there have been three waves of innovation in identity and I would start the really interesting and this is digital identity by the way. I would start these waves going back to something like maybe the Diffie-Hellman. Diffie-Hellman was a cryptographic technique that was invented in 1976. You could possibly go back to email which was a little bit earlier than Diffie-Hellman. But anyway, and then I would say that there's these three bands of or waves of innovation and they have characteristics that are common or commonalities in the way they think about things. These aren't exactly perfectly aligned technologies in each of these bands, but they have these common characteristics. So I'm not sure what happened there. Maybe my laptop is still alive. I'm going to keep talking. Maybe we can get it to come back up. Okay. So the first band here, central or federated governance, it was an assumption that when you built identity systems initially there was going to be some central body that did it for you. And it was an assumption that you were going to use this brand new cool thing called Diffie-Hellman and this brand new cool thing called asymmetric cryptography and all that kind of good stuff. And that you were going to use keys and certificates. That was kind of the new kid on the block that was cool at the beginning. And a lot of innovation has happened since then that kind of keeps those key assumptions. solutions. And by the way, when I represent these three bands here, I'm not saying that there's bad and okay and better so much as I'm saying it's kind of like a classic car that had a carburetor and then a car that has a fuel injector and a computer and then an electric car or something. These are waves of technology. There are reasons though why we learn from our experience.

And so there is thinking in these later bands that looks back at what was done in the earlier bands and says there might be a better way to do this and there's advantages to tweaking our mental model. So the second band of identity innovation I would kind of track back HIPA is kind of an outlier in the fact that it came about pretty early and by the way HIPA has Utah roots. I didn't know that until yesterday I was talking to somebody. But anyway, really kind of when blockchain started impinging on people's consciousness, there were a number of things that people said, oh, wait a minute. That means there's a different way that we could do this. Oh, there's a different way we could do that. And there were some dominoes that fell and it brought about this yellow band of thinking. And the thing that's different mainly between the red and the yellow is that we're using generation two techniques where we're not identify-

ing people by keys. Now we're identifying people by identifiers. And we're using probably upgraded cryptography like elliptic curve and so forth. And there's a lot of blockchain, although it's not all blockchain oriented in the yellow band. But there's a lot of the notion of wallets, digital wallets was a big deal. And then there are a lot of dissonance around privacy issues as this yellow band kind of came about. out. The third wave of thinking here, this green band is typified in my mind by a much more sophisticated and nuanced view about the governance that has to be in place. And that doesn't mean that people that are making yellow banded stuff or red banded stuff are ignorant about governance by any means. But it's kind of like playing a symphony. There's a lot of different instruments and I think in the green band the full range of instruments is now much more apparent. And big emphasis on auditability of what's going on in a system and a big emphasis on recoverability. If something goes wrong and you assume in the green band that things will go wrong. So the question becomes what do you do when things go wrong? wrong, not how do you prevent things from going wrong, which is an unrealistic question in some ways. And there's different cryptographic primitives. There's identifiers, yes, but they're upgraded to autonomic identifiers which have certain desirable properties, so forth. And an emphasis on look post -quantum is going to be a reality soon.

Are we ready for it? It would be really foolish to build an identity system that's not ready for post-quantum at this point when NIST has already announced post -quantum standards. Okay, so enough on that slide. I can't spend that much time because there's just like I said 10 minutes is nearly impossible here. What I see in the market is that there's major tensions. There's things that are pulling solutions to the yellow and the red band. hands and you can see what I've said roughly kind of argues for yellow and red solutions today. And then there's things that pull people towards the green direction when they're designing solutions.

Enough said on that. I could go into this for hours, but let me just talk about the two biggest forces that I see in the market today. I just returned from living in Europe for several years. So I've lived personally through the EUDI initiative a little bit and what's going on there. And the EUDI initiative has enormous, enormous momentum. It's a juggernaut in Europe. But it doesn't, it's not without its challenges. many different countries have built systems and they kind of don't all get along, but they're trying really hard. And the state of play in the United States is a little bit different. You have state level initiatives, which is why this conference makes so much sense. States are making the decisions, not a central government. There are things that are being built with generation one solutions or generation two solutions in the United States. Absolutely. SEDI is an example of a generation three solution and there's reasons why I think that's really exciting. The strategic trends that I'm aware of, I'm not going to say them all, but you can read them there. I'll just say that the thing I would bet on, bet my bottom dollar on, is that last bullet. Security pressures are going to grow and legal pressures are going to grow. I guarantee that's going to be true. If nothing else that I can forecast, that one's for sure. Remember what that might imply about what kinds of solutions are wise. I'd like to end with a thought here and that is we sometimes hear solutions described in terms of formats. So, you're going to hear today about ISO mobile driver's licenses and you're going to hear about W3C verifiable credentials and so forth. I think that's the wrong way to think about decisions. Up here you have two pictures of the same person and one of them is the lossless view that you get off of a digital camera when you take an image and the other one is a JPEG. Now, are JPEGs bad? No. We use them all the time and they're very useful. But if you're a professional graphic artist, you would never want to deal in JPEGs as inputs to your graphic projects. So they have different uses. And I'd like to suggest that permanent evidence needs to be lossless evidence. And there are a num-

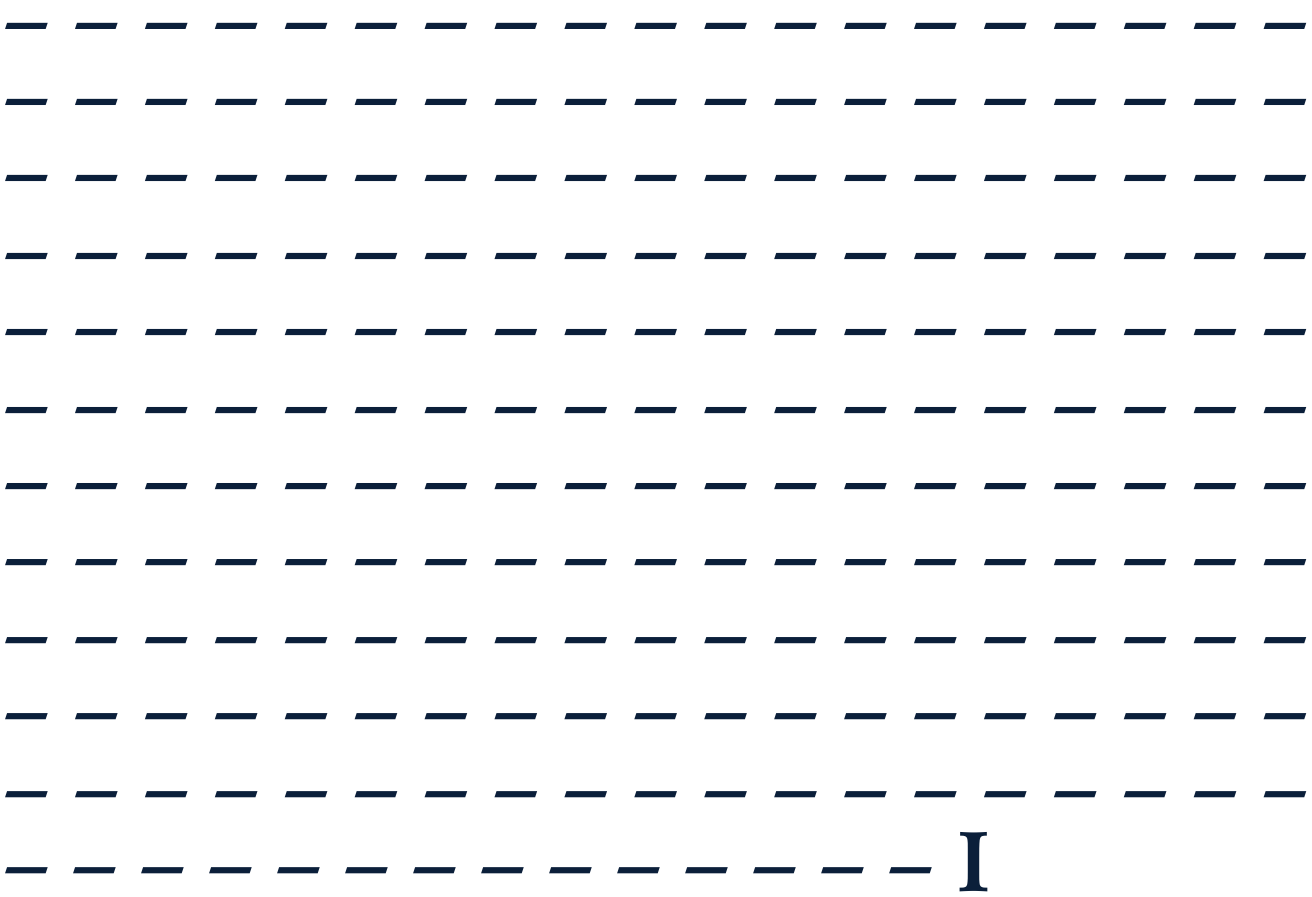
ber of dimensions to losslessness. There's time-related dimensions like how long does this evidence persist. There's governance -related dimensions to evidence. There's post-quantum cryptography related dimensions to evidence and losslessness. There's all kinds of stuff. So I'd like to just suggest that as you run into conversations about this, don't make it a debate about formats. Make it a debate about how to solve problems and you'll find that the format questions fall out. Thank you.

TALK XIX

M

morning-01-43-00--01-50-14-Phil-Windley

STATE ENDORSED DIGITAL IDENTITY SUMMIT · TALKS · 07:13



don't mean privacy. I mean it's private to Amazon. They own it. We call these administrative identity systems because they're designed to administer identity for a specific purpose in a specific domain. In this case, it's Amazon, but you know, there are millions of them. The system, the identifiers, how they work are owned and controlled by Amazon. They're the subject of Amazon's terms and conditions. They're useful for establishing trust within a domain, but they're not useful for establishing trust across domains. People are party to dozens, hundreds, thousands of these things. I have over a thousand entries in my one password.

In contrast, decentralized identity flips that model. The person becomes the center of trust and credentials about that trust flow through protocols rather than platforms. Unlike the decentralized identity model, decentralized identity provides a consistent experience for interacting with all of the relationships in your digital life. But decentralization alone isn't enough. What we really need is what I think is called first-person identity, a way for people to act as themselves online, not as managed account. I like the term first person identity better than decentralized because it's more clearly distinguishes that identity is based on the individual, the first party in a relationship. First person describes an idea that most people understand naturally. We're taught about we're taught this in grade school. First person is I, me, myself, mine. First person describes precisely the kind of thinking that will allow people to create their own online relationships without an intermediating administrator like a social network. In first-person identity, you might have relationships and credentials from your employer, from your bank, from your school, from the driver's license bureau, and so on. You can use these alone or in combination to prove things about yourself. In first-person identity, people are the integration point for information about themselves. ourselves. Now, why does this matter so much? It matters because something essential is missing in our digital lives. Maybe.

There we go. The real challenge online isn't utility or convenience. its proximity. In the physical world, we're next to each other. We rely on tacit knowledge that we gain from our senses to see when we see and speak with people. We use this tacit information to establish trust. We don't have that online. Online, we interact at a distance through screens and systems and platforms that usually are not controlled by us. Our relationships are mediated by companies rather than being direct. Let's talk about what that distance costs us and how endorsement rather than control can close it. Descartes didn't say, I have a Google login, therefore I am. He said, I think, therefore I am. We exist independent of anything else around us. Now, that's where endorsement comes in. It bridges the gap of distance. It allows people or anything half a world away to trust who you are because your own state endorses what you're saying, your assertions that you're making. SEDI, State Endorsed Digital Identity, doesn't give you an identity.

You already have one. Rather, SEDI endorses it. It provides the assurance we need to act confidently across digital distances. So the problem isn't that we lack digital IDs. We've got plenty of those. I've got a thousand. It's that we lack standing in the online world. We are ghosts existing only through the grace of some company. We are not embodied autonomous agents. SEDI changes that.

Again, it doesn't create your identity. It endorses it and gives you the ability to act across distance that can lead to something much bigger. A chance to reclaim our digital freedom. First-person identity represents a chance for us to declare our independence in the digital realm. to regain the freedom to act as ourselves.

SEDI enables that by supporting the individual and giving each of us a place to stand online. Freedom in a digital world begins when we act from our own identity, not one assigned to us and mediated by someone else. This is our moment to build a digital world that honors human dignity. A world where we are free to live and act as ourselves, as digital citizens rather than digital subjects. If we don't build it, someone else will. And it will reflect their goals, goals that probably don't align with the ones we think they should have.

For Utah, this is a chance to lead by example, demonstrating that trust in identity can scale without surveillance. Across the US, SEDI can mark a shift from digital subjects to digital citizens, people who live effective online lives with agency and respect. We have the opportunity to build a digital world that respects human dignity, a world where people are free to live and act for themselves. Let's not squander that opportunity. community.

TALK XX



morning-01-50-35--01-58-24-Joe-Jackson

STATE ENDORSED DIGITAL IDENTITY SUMMIT · TALKS · 07:48

Yes. Okay. Today, I want to talk about the evolution of technology and how backward compatibility is essential for growth. Technologies are in a constant state of change and they're always adding new features and and enhanced functionality to meet growing demands. The three phones that you see here are a perfect illustration of this. They represent the dramatic evolution of the simple telephone over just the last 30 years from a device tethered to a wall, to a portable gadget for calls and eventually text messages, to the powerful computer we all carry in our pockets now. The infrastructure to support the corded and the corded and smartphones are still in place today, but the first generation of mobile devices no longer function. This progression is a familiar story, but it holds important lessons for the future of other technologies, including digital identity. And the progress shown here is not always guaranteed. So I want to talk about two ubiquitous internet technologies that we all use every day but don't think about.

Some of you may not even know these exist. But they were both introduced around 30 years ago and their paths to adoption have been significantly different. The first is IPv6 and was introduced in December of 1995 and it's so foundational to the internet that it's literally called the internet protocol. IPv6 is the successor to the original internet protocol and it has struggled to gain traction only reaching about 50% market share today despite decades of effort and superior capabilities. Second technology is 802.11 also known as Wi-Fi. It was first introduced and standardized in 1997. And then Wi-Fi has been a massive success.

It's seen seven major releases, each one faster and more capable than the last and has become an indispensable part of our daily lives. So why the difference in adoption? Backward compatibility. Wi-Fi was designed from the ground up to be backward compatible. Each new generation of Wi-Fi routers and devices could still communicate with the older ones. This created a smooth seamless upgrade path for everyone. IPv6 however was not backward compatible with its predecessor. This meant that the transition required a complete and often costly overhaul of network infrastructure. This major difference is the primary reason why Wi -Fi's adoption has progressed so smoothly while IPv6's adoption has been a long slow struggle. Another way to allow for continuous improvement of technologies is to ensure compatibility with alternative standards. To illustrate this, think of the audio codecs that power our digital music and podcasts. Many different standards like FLAC, MPEG, and OPUS coexist today. For the vast majority of us, the complex process of encoding and decoding audio is completely transparent.

We just push play. Each codec is optimized for a specific situation, whether it's streaming high fidelity music or ensuring a clear voice call over a weak connection. While this isn't ideal, the ecosystem works because applications have the ability to handle the different types of audio files, seamlessly switching codecs as needed. New codecs can be added to the ecosystem while old ones are eventually retired.

So just like these other technologies, digital identity is at a crossroads. We have a mix of established legacy systems and emerging innovative solutions. The challenge is figuring out how to move forward without immediately abandoning the significant investments we've already made and without destroying the user experience or preventing progress. A core principle of the SEDI framework is to support backward compatibility. We believe the only viable path forward is one that embraces interoperability with existing options without being confined by them.

This approach will allow organizations to continue using their existing investments and infrastructure while providing a clear path to upgrade to newer, more secure and more capable technologies over time. It ensures that progress doesn't require starting from scratch or forcing adoption of a single solution across the ecosystem.

To show you what this looks like in practice, we're going to do live demos. We realize the risk in that. So, I'm pleased to introduce the participants for our technical demonstrations today and I'll invite them to start coming up on the stage here. In the upcoming demos for this session and later this afternoon, they'll showcase how several of the currently available identity technologies can be used together in a cohesive and interoperable ecosystem. While no technologies for SEDI have been chosen, they will present possible scenarios utilizing several different technologies working together for the first time.

You'll notice how the user experience is similar despite differences in the underlying technologies. So if you could start making your way to the stage as I as I introduce you. First we have Spruce ID. They're a US-based company whose mission is to give people control over their identity and data across all digital interactions. Here you go, Wayne. Wayne Chang is here and their software powers secure standards-based credentials such as mobile drivers licenses and verifiable digital credentials that can be used both online and in person across government and enterprise services. As a leader in the decentralized identity and credential interoperability space Spruce's technology supports selective disclosure unlinkability and no phone home verification. Their work with states, federal agencies and standards bodies demonstrates how digital identity can enhance access to services, strengthen security and preserve user autonomy in a connected world. GET Group North America is a US-based company specializing in identity management solutions with over 40 years of experience supporting governments worldwide and has been a leader in digital identity since 2017. GET was selected to deploy the technology for Utah's mobile driver's license in 2021, helping Utah citizens securely share their MDL details, prove their age, and maintain their privacy. The company has worked with government agencies and businesses to accept and verify MDLs, including the TSA, Utah Highway Patrol, UCCU, and AFCU credit unions. And then last, they'll be presenting later, but their technology is used in the demonstrations. The Cardano Foundation is a not-for-profit organization based in Switzerland which promotes the education development and adoption of decentralized technologies to build future-proof industry solutions.

Veridian is an open source digital identity platform developed by the foundation that delivers secure enterprise -ready verification services which protect user data and prevent fraud. Veridian's credential management platform led by Thomas Mayfield implements self-sovereign identity for individuals and organizations. And Veridian's core objective is to ensure authentic communications and verifiable identity protocols are easily accessible to all. So I want to personally thank all of the presenters for our technical demonstrations today. They put this together in a matter of weeks and we're really excited to see these technologies working together for the first time. So I'll turn the time over to them.

TALK XXI



morning-01-58-29--02-20-59-Wayne-Chang

STATE ENDORSED DIGITAL IDENTITY SUMMIT · TALKS · 22:34

about the different approaches, especially in the context of how do we start with individual rights, think about the policy before we rush to the technology, right? Because there's an implicit social contract, right? That is the use of these digital identity systems. And it is much better for that to be an explicit one rather than one that is the most convenient or imposed or anything else.

else, right? So I think we're all here for the same thing. And being able to move towards that, I have a pretty nerdy quote actually that I want to start with from a fantasy novel by Brandon Sanderson. Then be wise about it. There are two kinds of important people, Shallan. Some, when the boulder of time rolls towards them, plant themselves before it and throughout their hands. All their lives they've been told how great they are. They assume the world itself will bend to their whims as a caregiver once did when fetching a fresh cup of milk. Those people end up squished.

Others step to the side as the boulder passes, but are quick to say, see what I did? I made it roll there. Don't make me do it again. These are the ones who get everyone else squished. Is there not a third type of person? There is, but they are rare. These know they can't stop the boulder. They walk beside it, study it, and bide their time. Then they nudge it ever so slightly to bend its path. These are the ones who actually changed the world, and they terrify me for people never see as far as they think they do. And I think the wisdom in that is it takes a diversity of thought approaches and use cases and opinions to actually consider all the different facets of this. It's an enormously complex and ambitious undertaking to build digital identity in a way that minimizes the harms, but we're able to derive most of the benefits. So I'm really happy that we're in a room with a ton of diverse thinkers from people who are experts on individual rights, what constituents care about, what people actually feel, the technology itself, including the cryptography, security and privacy aspects of it, adoption, change management and user experience. So I think that we're very excited to show how these concepts from SEDI where you start with the policy and the rights and then the technology is figured out after that. That's really what we want to showcase and how it can help our existing investments we can derive value from those. And especially as we saw with the adoption, MDL is in I think 17 states at this point.

A lot of investment, a lot of great security people have been thinking about that model. The TSA spent over $250 million on machines that can accept the MDL. So is that all to waste if it doesn't comply? Or what are we thinking about here? What about everything else? And fortunately, you might even be able to shed some more light on this. Yeah. Thanks, Soren. And thanks for taking all our five minutes. But it's been actually an honor to work with Utah. Excellent team, excellent people. It has been a fantastic experience and we're really happy, of course, with all the work that they perform and we had the honor to support them to have a successful MDL issued and being used and utilized in many not enough use cases and relying parties including TSA and credit unions and law enforcement. But we're happy to be also part of this group that Chris put together to assist the best we can with our experience and knowledge and technology to make whatever next steps Utah chooses to take successful. So it's amazing. So what are we seeing over there? That's a verifier. A verifier is something a relying party would have. A relying party being anything, anyone that accepts and consumes a digital identity and MDL. And that can be a government agency that asks for your ID. It can be law enforcement. It can be anyone in the private sector. It could be a bank, could be AIDS restricted alcohol sales, tobacco, and so on.

Whenever they ask for that ID card of your driver's license, you can present the MDL or at least that is the purpose and you can use verifiers as simple as an app or in a fixed point with a scanner or eventually online. All that technology exists and hopefully it's going to be part of the ecosystem we all operate in.

Can you talk about what's going to happen between this SEDI wallet and And what kind of, you know, how is the data transmitted? What happens between this application running on your phone and an application that holds a credential on my phone? Well, yeah, originally the ISO standard, which is what the Utah MDL is complying to, along with our close to 20 other jurisdictions that issue an MDL that complies to the ISO 18013-5, which is the in-person standard. it had a phone home, it had a connection to the system on record that is no longer the case. And similarly, any verification we would conduct with a SEDI, it will only consume whatever you have on the phone and you present. – And it goes, this could work in the mountains, right? If there's no internet or anything. – Correct. It will be done offline because again, it will cryptographically analyze whatever you have provisioned in your phone as your digital identity. I always really like this part where it goes over Bluetooth and NFC proximity technologies that involve no servers, right? It's just peer-to-peer over device. That's actually the best privacy profile you could hope for, right? So there are parts that have had extraordinary investments that are really valuable from a privacy and usability perspective. And what we see in that wallet is not an MDL. There's no driving privileges there. It is a credential that is solely focused on identification, right? And that the reason that it is a SEDI credential is that it conforms to the code in SEDI, right? Is the idea. So if we start looking over here, I told you it would be a nerdy presentation, right? We looked in the Utah code, right? And there is SEDI enshrined in it as statutes. And when you click in, you're able to see the different definitions, and requirement from Senate Bill 260 that was signed into law by Governor Cox earlier this spring. And thank you to representative and senator for the work and the whole coalition. So it's really about controls.

It's really about these are the things we're expecting this credential to do and operate, right? That's what it represents. So data formats, everything else, those are things to figure out, but making it policy-based and starting it from there is the most important part because that is the social contract, right? To express the will of a people and have those as the agreed upon controls if someone is to participate in the system. So we just want to demonstrate that this model, right, can also work with the corpus of investment for existing systems that have been significant and growing in adoption. So we have looked into the mobile driver's license technical specification. Sure. We have looked at the sub component called a mobile document or an MDOT. And that is just a data format. That doesn't describe how to use it or anything else. And there are other pieces that we can build up to that we can agree with and are aligned to the SEDI framework. So that is the idea and what you're going to see with this demonstration. – And similar, of course, any digital identity, the benefits are you're not using your card, you don't share your card, you don't show any information, it's not copied, you don't flash past so-called whatever it is on the phone. and it respects the privacy of the user and you only share what you choose. So if you want just your age to enter a bar or alcohol sales, that's that is all you share, not the entire ID. Unless of course you're at a bank or you're applying for a loan or law enforcement is asking for the entire ID, that is when you share if you choose the entire information.

That's right. And the MDOC data format here point supports selective disclosure as part of that base. We like that. We're like, okay, that sounds pretty good. Let's take that part. Right. So we're going to demonstrate and there's no contact. You can do it's a QR barcode scanning. It is via Bluetooth through a good range or a tap NFC just like as everyone is familiar with the Apple pay and so on. Yep. So let's say that we're in a use case where let's call it law enforcement. Let's say there is warranted ability to request information, right? So there's going to be a lot of it being requested. – So you can see there it says all info. So I'm asking for all of the information from the user. – But this can be tailored to different profiles

depending on the context. And that's the really important policy work we need help with to figure out. So I'm going to share the identity by creating a QR code. You can either tap or create a QR code to share it. What it does is it brokers a secure connection over Bluetooth. So it adds encryption on top of Bluetooth because Bluetooth itself has challenges. That's how the MDL protocol worked. That part of the MDOC and standard seemed to be pretty promising. And we were able to show a QR code. So we're bringing up the scanner. No contact.

And actually it's going to consume. I get to decide what I share or not over here on this screen. Those are the fields requested. As the user, I get to make the determination. That's another feature of the protocol that was supported. And when I press approve, it's transmitted over basically the Bluetooth connection peer-to -peer. So this would work in the mountains without any kind of external connectivity, right? And again, this is being used at a ton of airports already, right? So we're just able to make sure that that part of the technology can also work for SEDI credentials. – So you can see that I'm seeing the information that he shared. I can bring up the picture, do one last visual check if I wish. And it has the document information. So I know it's from Utah, the document number and that's about it. Yeah. – As simple as that. Plus, of course, I have the verification on the age verification. – Yeah. Well, let's say I'm I'm at a bar right at night and I want to show I'm over 21 but kind of don't want you to know my full name and where I live, my address, right? How do we do that? – So, I will just the one that is asking for the information can can ask only for the age. So, unlike of what you choose, I can only ask for the age and whatever you share, I will only get the age. And of course, as you saw, once my hey, I leave that verified information I had is gone.

It's not saved. It's not tracked. None of that. And you cannot get a screenshot. Yeah. So the policy consideration here is that there are many different attributes that you could add to this thing and ask for, right? So those are the really important decisions to be made. Can we add veteran status, disability rating? Can we add how many dependents you have? These are all really relevant for programs like Wix and others that that require expedient access, but we also want to eliminate the fraud, right? So, and because it's the user consenting to display the information, you don't really have to go with one of these very complex interagency data sharing agreements if we faithfully present an opportunity consent for people, right? So, if it's tough to do across agencies and coordinate, just give it to the person and let them decide, right? All right. So, I know your age. You're looking too young to me. Thank you. Thank you.

Oh, is this the right one that you've requested? Did you configure it to just select the age only? – Just the age only. – Well, see, now I have the opportunity to deny all this stuff. – If you agree, I want to deny all this new age. Try again?

– Yeah. Yeah. Yeah. Because there is an option also to request I need find info or to project that one. Right. Because that was on. Oh for age. Okay. Yeah. Okay. So now I can let him in. So you turn on the safety. Let's see. Age over 18. Got a different set of things requested. But you know what? I'm really just going to get rid of all these things except my portrait and age. And that's all you're going to get. And the Verify will have to deal with it.

So I think there is a setting where I've definitely seen that work with this app though. – You want to try again? – Sure. – Let's give it an answer. Right. And you say okay. So those are the only data fields that ever left the wallet, right? During that specific interaction. So yeah. See us after will definitely show that you can do an age demonstration. I think that I have a version of the GT mobile app where I can just ask for the age of mine. But But you'll see other profiles where we can get it. So great. We have two more

things to show you really quickly. And one of them has to do… – What's the floor? – Okay, great. – And those I'm on setter by the way. – Yeah. – Okay. – Welcome. Thank you. All right. So the other two use cases.

One is banking and it's very important for people to get access to financial services. Many of the same methods are more or less used for benefits distribution when you're trying to figure out eligibility and identity verification for some of those things, right? So this is a generally useful flow. In fact, NIST has this National Cybersecurity Center of Excellence, right? And we're trying to figure out how are we going to do banking KYC? privacy with the mobile driver's license. I see some folks in here who are actually formal participants in this program. So that's great because a lot of federal agencies and other states are going to look to the output of this program and how that's going to work.

There are a lot of banks, a lot of tech companies, a lot of other actors, and basically we're trying to figure out how do we preserve privacy but also allow for these kinds of use cases. They're even talking about shapes that it's going to work. But right now it's just called the MDL program. There's no reason why it needs to be. It could just be digital identities, right? But that's kind of the only thing that popped up, right? So to have a credential that has steady controls over it would be very interesting, I think. But back to our banking example, and this is where a lot of tech companies have invested a ton of effort. They're best UX people. their best security folks. How do we make this really good? And the interface is mostly for the MDL, but those technologists have agreed that, hey, other things might be acceptable here. Passports, EIDs in Europe are not driver's licenses, right? So MDL isn't so strongly applicable in some areas. So how do we allow a diversity of different credential types to be accepted? And there have been great strides in the user experience towards this. So we're going to basically open a fictitious bank account.

And I'm also going to make sure that I can show you what happens in the wallet alongside that if I can figure out how to make this small again. There we go. So we're at Arch's bank. We're going to open an account. We're going to begin our banking application. and type in our email. I'll just imagine that I get a confirmation code. You've probably done this before. Go to your email, you find the code, you put it in. Multi-factor. So right now it's a phone number, but you know future approaches like pass keys and digital credentials will hopefully leave the need for this. So put a phone number in there. Same deal. Again, many banking systems just work like this today. And a social security number is required by FinCEN's customer identification program. So that's a Bank Secrecy Act requirement.

So, you know, you'll just see it as a requirement for banks. But at this stage, it's part of identity verification, right? And what a lot of institutions do today is they say, hey, upload a picture of your driver's license or upload a picture of utility bill. And none of those security features are actually valid when you just take a picture of it, right? Like that's the new world of security needs to be built on things that AI is bad at. That's showing up in person. That's breaking cryptography, especially post-quantum cryptography. That's making very complex computational predictions about physics and how light refracts on things or how you know something can change geometrically. And that's what a lot of the liveness algorithms are about. But it all starts with having a really strongly certified credential. And when you want to verify with it, then it uses the operating system level controls to say, hey, do you want to share your data? It's built on the same technologies as passkeys, actually, if you look under the hood. We want to share it. QR code comes up. We see on the wallet. I'll scan it. You won't be able to see everything. I think there's some privacy protections with the screen share, but you'll be able to see the important parts. So it tells me only

connect to devices you trust. And when I connect what happens, you'll see a lower popover. This is kind of like the Apple Pay experience or the Google Pay experience. It's part of the operating system and you get to pick which wallet it comes out of, right?

You've been requested a credential from somewhere. We're going to agree. And again, we have that opportunity to consent what gets sent, right? If we send it, then what happens is instantaneously a cryptographic payload is sent along with the data fields and that can be verified by a server. So it goes to from the phone to the laptop, goes from the laptop to the server, and then it gets verified way easier and more secure than uploading all those different documents. You submit and you're good to go. So getting easy access to financial services benefits a slew of other things requires really good UX, but we can't compromise on individual rights.

We can't compromise on security as we get there, right? So let's take those existing investments that companies put their best UX and security people on and apply it to a framework that is individual rights driven, right? So that's the proposal for ensuring backwards compatibility to a lot of these systems. A lot of the time you think legacy old experience, but these are actually some really great experiences happening, right? And the last thing I'll show is interoperability with a completely different system. This is the same technology harness. Thank you for the Veridian team for providing their issuance portal for this part of the demo. So different company, not Spruce ID. It's not like one company built all this stuff.

These are interoperable protocols. And there's something called the Global Legal Entity Identifier Foundation that is able to do identification for organizations to a high degree of proofing so that we can know who we're doing business with if a company wants to get a benefit or something else, right? So basically, I want to have another credential on my phone where I can have that employee badge or proof that I'm part of an organization Let's say I'm going to ask someone else for a credential or I want to open a business banking account. These are useful to understand what entity I'm associated with. What if you're part of LEO and you want to show that you're a real cop and you're not trying to just coerce someone to do something, right? So you can issue a credential for this. There's some numbers as part of it. I'll put my name. We'll just say employee and we'll issue the credential. And this is a totally different technology stack built on KERI and ACDCs, which protocol and format invented right here in Utah. You get to accept it and a new credential shows up as an official organization role. And then when we want to go request it, we can request a presentation from that wallet.

The wallets have been linked prior. It's a demo. Request a presentation. We will see the request happening and approving it. We'll see the request is updated, right? And these are different data formats entirely, but following the same control principles, right? So that's the end of my demo. Thank you.

TALK XXII



morning-02-21-20--02-32-35-Paul-Cutler

STATE ENDORSED DIGITAL IDENTITY SUMMIT · TALKS · 11:15

Present our presentation by Representative Cutler on the role of the state and how to keep the feds out of our business. That'll be later discussions. My boss is here, Marvin Dodge. I hope that joke didn't get me in trouble.

Oh. You don't last long with a personality like Maz do. So this is going to be 10 minutes and then we're actually going to do break out into two breakouts before lunch. I'll give some instructions after this for that. Fantastic. Thank you. Thanks for putting the break. I think the sound will work. – I will see if the sound works. If not, we'll bring our live demo team back up here to help. So, I brought a couple of friends with me to help. Let's see what they have to say. And the sound did not work.

Is your sound up? It's going to be off. It was muted though. One more try. Welcome to Utah, folks. Digital identity is fabulous. It's really great. You're going to want one. What is the state's role in digital identity? Wait, am I not in charge of all the digital identity around here?

If you see him, tell him he is in charge. That'll be just fine. We've all seen lots of evidence of the challenges with digital identity, the breaches that are happening around the world, often with governments involved in these and And let's talk about what the role of the state is compared to the role of the federal government or the role of private industry. And I would suggest to you that the role of the state, as we have heard so many times, is not to control or to create but to endorse. And the reason it's important for the state to be involved is a matter of trust. In our society, some of our largest tech companies have lost the trust. and the trust needs to come back to the individual. And as Phil Windley presented, put the individual back in control. So let's try this again on what the state's role is. Look, this is important. The role of the state is to endorse, verify, authenticate, protect, and guarantee an individual's digital identity. This is even more important. Personally, I really like control. But the role of the state is not to own, create, control, gatekeep, or surveil an individual's digital identity.

– In the age of AI, even a legislator can create terrible videos that could fool somebody who's not paying attention. I think we understand the points there. Historically, the state has had a significant role in identity. Often we think of, oh, well, you know, the feds have a passport, the feds provide a social security number. But this goes back to the presentation before. The root of the identity is typically a state-endorsed credential. We often start with a birth certificate that in most cases is issued by a state. And the state handles most of the vital records. They're often used by others in private industry or by the feds, but the vital records is primarily a state responsibility.

This was mentioned earlier, but I think this is really important in the crux of our argument for a state endorsed digital identity. In the tech world where many of us live, there is often a call for expediency and for efficiency. It's more efficient to use this or it's easier to adopt VHS than beta. It's easier to adopt or some people believe you know they like the Android interface or the iPhone or iOS interface. If we start with efficiency as our value, then we will get a completely different set of products than if we value protection, security, and privacy. I think if there's anything we've learned over the past few years, and when we think about social media, we think about online fraud, is that we have to be more purposeful in designing our identity systems and in the systems that are going to be used by millions and millions of people. Because if we make a mistake, that mistake scales again and again. So our argument is to think carefully about your values. What are your values as a state? What are your values as an individual? Do we put our rights protecting our children at the top of our list? Many people would argue that in designing social media, child protection was not the top value. And over the years we've had to pay a price for that as things have changed and that because that wasn't the most important value in designing these sys-

tems. Our argument is that we should protect the vulnerable. You've all read the articles of people, vulnerable adults, vulnerable children getting scammed by people. We heard a heartbreaking story today of what can happen when a bad actor takes advantage of somebody. We must look at our values and put our most important personal values, our most important moral values at the top of the list and not let efficiency, interoperability, or profit take over the design of our identity systems.

Those of you in the world of designing systems understand that we have to think big and we have to consider a lot of different elements in our governance framework. We've got to consider how are we going to audit these systems? What are the open protocols? Because historically, we have to agree on a protocol and a standard to to get mass adoption. We have to think about how will this be enforced?

We saw an example just a minute. Okay, if the enforcement and the verifier is so ubiquitous that it can be put on a mobile app, that'll reduce the cost to install readers in all of our places. Should we have a right to paper? That's going to be a debate that I think many of us will experience. Our friends in the UK have said everybody gets a digital identity. We have some people who don't want a digital identity. How do we help them move forward when 95% or 99% of the world is moving to digital transactions? Can we build transparency into the system so we can identify fraud? Will we prevent all fraud? You of all people know that preventing all fraud is impossible, but can we make the systems transparent so that we can identify that fraud earlier and quicker so we can take steps to reduce that fraud as we go forward. Okay. Last I'll leave you with this thought is that comparing the state controlled identity which we've been talking about and certainly we have some examples of that in other countries compared to a user controlled or a liberty -based model. And we discussed many of those key elements. Selective disclosure.

One issue we haven't talked a lot about but is really important as we think big is the guardianship. We've seen the importance of guardianship in social media. Should a parent be able to control what apps a youth has access to? With vulnerable adults, how do we design systems to take into account that there are going to be adults in our lives that we have guardianships over or youth and we've got to have that as a key mechanism to have a guardianship capability. So those are the key things that I wanted to present to you.

It's been mentioned by my good friend Senator that if we leave this up to the federal government, we're going to be stuck in Maya. We're not moving forward. If we leave it to our friends in industry, their hierarchy of values is different. They have fiduciary responsibility to make money. And in some cases, they will view making money as more important or interoperability as more important than protecting the vulnerable and protecting individual rights. It is our responsibility to exert our constitutional and moral principles of liberty, self-determination, and individual autonomy. Thank you for coming and for participating in this. And I think we're moving to the break.