Mon, Oct 03, 2022 1:00 PM ET • 51 minutes,31 seconds

AUDIO

https://netcaucus.org/audio/2022/20221003digitalid.mp3

SPEAKERS

Zach Isakowitz, Cara Mumford, Connie LaSalle, Sean Frazier, Jeremy Grant, Tim Weiler

Zach Isakowitz 00:02

Good afternoon everyone and welcome to October's Tech Policy Recess event. I'm Zach Izakowitz, the legislative director for Congressman Michael McCaul. Since it's Cybersecurity Awareness Month, we thought we'd focus today's briefing on a cybersecurity issue. It's no secret that the world today has become more digitized. Americans are spending more time at their computers on their phones, generating loads of data and the process. Companies are using technology to make their businesses more efficient and more profitable. But as we continue to opt to open up to technology, the cyber risks and threats change. This all leads to the question, How do we know who was behind the screen? Today we'll hear from some experts as to how digital identity can be used as a tool to enhance cybersecurity. But before we get to the panel, I want to note that this event is hosted in conjunction with the Congressional Internet Caucus and its co chairs. On the House side of the Caucus co-chairs are Congresswoman Anna Eshoo and my boss, Congressman McCaul. On the Senate side, it's Senators Patrick Leahy and John Thune. We do these tech policy recess events during about every congressional recess, so stay tuned for the November sessions. Today we have a panel of experts who

are on the frontlines of digital identity issues in cybersecurity. Our moderator today is Jeremy Grant, who is the coordinator for the Better Identity Coalition. Jeremy is also a former official at the National Institute of Standards and Technology. And with that, Jeremy, I'll hand it over to you.

Jeremy Grant 01:32
Great, hey, thanks, Zach. I appreciate the introduction. I'm excited all of you are able to join us today. I'm Jeremy Grant. I'm Managing Director of Technology Business Strategy at Venable cybersecurity practice here in DC and his accent in that role. I also lead an organization called the Better Identity Coalition, which is the one group that has been focused on what I would call the policy layer of digital identity. And this topic we're here to talk about today. I've been around identity and cybersecurity really as long as I can remember dating back to my time as a hill staffer in the 90s, but also spent time in industry building digital identity systems and had a second stint in government leading the digital identity efforts at NIST. So our discussion today is on digital identity cybersecurity is a new hope. And with the Star Wars themed title, I was tasked as your moderator with coming up with a not too ridiculous Star Wars metaphor to kick us off today. So here it goes. There's 19 years that passed between Star Wars episodes III and IV, 19 years where Darth Vader was just doing awful things to the Galaxy, and his preferred attack vector to get what he wants, using the force, the dark side of it at least to crush his enemies. So in the real world are adversaries, in cyberspace, be the organized criminals, hostile nation states, malicious hackers. They're the Darth Vader that we're up against. But instead of using the Force to attack us, they're generally using identity. What do I mean by that? Well, if you go back over the last 19 years, look at every major breach and cybercrime incident, it's been in the news, it's an anomaly to find one where identity did not provide the attack vector, whether it was the Target breach in 2013, the Office of Personnel Management in 2015, the Equifax breach in 2017, the 2020 Solar Winds incident or the Uber breach last month, the attackers got their initial foothold into the target by compromising passwords, or in some cases compromising the multi factor authentication that was put in place to guard against password centric attacks. All of these targeted but most people would call the authentication layer of digital identity, looking at the way that you're signing in once you've been issued an account. We've also seen a ton of attacks that are targeting what means what most people call the identity proofing layer of digital identity, which is that process you go through to prove who you are when you're first opening an account, say applying for a credit card or perhaps a government benefit. These are attacks that exploded during the pandemic. Just two weeks ago, the Inspector General of the Department of Labor published a report saying that organized criminals stole more than $45 million from state pandemic unemployment insurance programs. In most cases, they were using stolen identity data to slice through the weak ID verification systems that states had in place more smoothly than Darth Vader could slice off Luke's hand with a lightsaber. And these attacks on identity proofing aren't just limited to government benefits. Last month, a deputy director of FinCEN Jenny, Jimmy Kirby at the Treasury Department, said of the more than 3 million suspicious activity reports that banks were filing with Vinson in 2021. These are the reports that banks are filing when they see evidence of financial crime. The majority of them were tied to break downs in the identity verification process. So as we're sitting here today is the start of National Cybersecurity Awareness month it's really fitting we're taking some time to focus on the intersection of digital ID and cybersecurity. Now, I've talked a lot about the dark side of the force, but much as the force also has a light side that can be used for good so to this digital identity. That's the title of this session being a new hope because identity when we get it right can be what I call the great enabler. Delivering online experiences that are more secure that are better than

privacy better for privacy, and much easier to use than what most people are used to today. So when we get identity, right, it allows us to vanquish those attackers and adversaries on the dark side. So with that, I want to take a moment to introduce our panel, or even better, I'm gonna let each of them introduce themselves, and also say a few words about the work they've been doing in and around the digital identity space. I'll say up front, we've got Connie LaSalle, from NIST, Sean Fraser from Okta, Cara Mumford, from the Senate Homeland Security and Government Affairs Committee, and Tim Weiler with Congressman Bill Foster. Connie, let me start with you and just let you introduce yourself. Great. Well, first, thank you to our hosts for the invitation to join you all today. And thank you, Jeremy, for taking on the role as moderator, and for the excellent Star Wars puns to kick us off.

Connie LaSalle 05:52
So my name is Connie LaSalle. I'm a Senior Technology policy adviser within NIST, which is within the Department of Commerce. And I thought I'd start with a bit of background about NIST for those who could use a refresher to our work and our unique role. So first, mist is a non regulatory institution. And I highlight this I double down on this frequently. Because our status is non regulatory has allowed us to collaborate with industry as an honest and trusted broker since our founding in 1901. This mission is to promote us innovation and industrial competitiveness by advancing measurement science, standards and technology in ways that enhance economic security, and improve our quality of life. The impact of this work extends to almost every aspect of our daily lives, and often in ways that I know that I certainly take for granted. Continuing with the Star Wars extraterrestrial theme. An example of our impact is the NIST F1 atomic clock in Boulder, Colorado, which is part of a small collection of clocks that sets the official time for planet Earth. That's pretty cool.

07:05
I think at least. And specifically within the NIST IT lab, we work to cultivate trusted information technology, with the aim of responding to demand signals that we see from various markets, government agencies, and the general public. Our research has provided state of the art technology benchmarks and guidance to industry and federal agencies that depend on information technologies, including those that support identity management. So as a as a senior tech policy advisor at NIST, I have the opportunity to engage on a wide array of both policy and technical topics that NIST cares about including identity. So I'm really thrilled to be diving into some of those topics here with you all today. Thanks.

Jeremy Grant 07:51
Thanks, Connie. Next up wanted to throw things over to Sean Frazier, who is the Federal Chief Security Officer at Okta.

Sean Frazier 07:58
Hey Jeremy, thank you so much for having me. Good to be with this esteemed panel of folks. I've been doing this almost as long as Jeremy has. I started my career kind of back in the 90s at a little company called Netscape where we tried to get people on the Internet. And it turns out this internet is kind of a thing seems like it's got legs. I was a cybersecurity guy before I even knew I was a cybersecurity guy just because we used to have this thing at Netscape. And nothing really happens till someone tries to log into something. So it's one of the reasons why we still one of the first directory services based on

open standards to protect the applications that we're rolling out to folks. So I actually consider myself more of a user experience than a privacy or security nut. Because I really think about that being the unspoken thing around security, which is user experiences and getting people access to things quickly. And Jeremy talked very eloquently about the need to be able to provide better services to citizens and to to folks who need access to technology. Right now, I'm kind of running the federal program at Okta, where we're embarked on a lot of different programs and projects around what we consider critical infrastructure for identity. So FedRAMP High DISA high impact level for access to services for our mission partners in the DoD space and it turns out that identities pretty important for some of these things, and it's not the zero trust pillar one for by accident, you know, there's a reason that we talked about identities kind of being kind of the core construct as we roll out security and, and while people call me zero trust, true believer, which I kind of am, I just look at this as security, I think 10 years from now, we're just gonna be calling this security. We're not going to have any fancy names and titles to it. We're just gonna be looking at this as the way we just build security from the ground floor into good experiences for users.

Jeremy Grant 09:39
A great Thanks, Sean. Up next want to throw things over to Kara Mumford with the Senate, his guy? I care. Hello. Thank you, Jeremy. Thank you, everyone, for joining us today. My name is Cara Mumford. And I'm the Director of Governmental Affairs for Senator Portman on the Senate Homeland Security and Governmental Affairs Committee. It's a bit of a mouthful committee in our jurisdiction matches that it's a very, very broad jurisdiction, we have everything that is a government wide issue. So that would include digital identity. But we also have the Department of Homeland Security. And so we have that specific cybersecurity, tilt to it, our jurisdiction as well. And so I feel like we have a really unique vantage point because we get to kind of straddle that, you know, government wide, and then also security specific jurisdictional issues. So I have been with the senator since 2018. I've been on his GAC since 2021, when he took over as ranking member of the committee. And then the other thing I wanted to just mention, and preface my comments today is that, you know, here I'm speaking from my personal capacity, and not necessarily as a representative of him or representing his perspectives. But with that, I just wanted to say thank you to the rest of the panelists and for you all again, but looking forward to the conversation.

Tim Weiler 10:49
Great, thank you. And Tim, over to you. Yeah, thanks, Jeremy. And thanks, everybody, for being here. And again, Jared for moderating. My name is Tim Weiler, I served as counsel to the Representative Bill Foster, who's been very engaged in the digital identity space and more broadly in the cybersecurity space. Since his time in Congress, he's got one particular bill, the improving digital identity act and almost synonymous strengthening digital identity act, both of which tried to set up some NIST standards to ensure a government wide approach towards a better digital identity. The original, broader package had some grant money to states who are exploring mobile driver's licenses and such, as has been a keen interest of my boss for a while now. So we're happy that it's starting to get some traction, very excited to be here.

Jeremy Grant 11:44

Great, thanks. So we've now heard a little intro from each of our panel members. So let me start with a question to each of you. And to tee things up. In 1993, The New Yorker magazine published a cartoon where a dog is on his computer, and he turns to his friend who is being a dog, another dog and famously says, On the Internet, nobody knows you're a dog, I think this is year after year, The New Yorker said, says this is the cartoon that is most replicated, and that they're best known for from all the cartoons they've had over the years. But 1993 was a long time ago. Fast forward 29 years, the dogs from that cartoon are now sadly, a blessing memory because of dog years. But it seems like we're seeing the fact that it's still so easy to be a dog on the internet being actively weaponized against us. And you know, to that point, I talked before about the massive increase in identity related cybercrime earlier. It's also worth noting the majority of ransomware attacks start with a compromised ID. So sort of an open ended question for each of you from the unique position that each of you have. Where do you each see the greatest opportunity for digital identity to help mitigate cybersecurity risk and improve our cybersecurity posture?

Connie LaSalle 12:58
Should we just jump in? And jump in contact? Okay, great. Sure. I know. Yeah. So I think the short answer for me is that there's an opportunity for digital identity to play a role in almost any circumstance where access to something valuable is being brokered. And I'm not just talking logical access through device I'm talking physical access, as well as, as the merger of the digital and physical worlds continues to happen. And I don't feel like I would be doing my job if I didn't also mention that this digital identity guidelines lay out a risk based approach to selecting a set of of controls, including technologies, practices and processes that that organizations across sectors of all different sizes can implement, to improve their cyber posture while managing other risks and balancing those other risks related to privacy equity, usability and other factors.

Jeremy Grant 13:52
Thanks, other perspectives.

Tim Weiler 13:56
I think you you hit a very salient point with the unemployment fraud in general and Pandemic we saw that a huge spike in that mainly because I think we largely transact interact and broker online. And we're still using these types of legacy paper forms of identity to do that. So there's kind of an inherent mismatch there and an opportunity for people to take advantage of it. So we're hoping that a more secure digital identity would first off be way more convenient, easier for consumers, but also just much stronger. And that's actually how we kind of got traction for our bill in the first place through OGR. Because it just I think it was an unemployment hearing.

Cara Mumford 14:39
Thanks. Well, let me say, Cara, over to you. You know, I was just gonna say I think one thing that's really exciting about digital identity is that there's kind of a little bit of something for everybody. There's the security aspect, there's the anti fraud aspect, there's the Preventing cybercrime aspect. And so when you have an issue like that, you can kind of generate support on both sides of the aisle in a really productive way. And so I think that that kind of in and of itself is an opportunity for digital digital identity

to improve. Cybersecurity is not necessarily from the technical perspective, but more from the practical perspective of getting people on board and actually moving an issue forward.

Sean Frazier 15:15
Thanks, Shawn, any perspectives on where there's great opportunities on digital identity? Yeah, I think they're everywhere. I think part of me thinks that it's taken us a longer, much longer time to get here than I thought it would, considering how long we've been logging into things on the internet. But I also think from a positive aspect is sometimes the technology has to kind of catch up to where we are and provide those those good experiences. If I look over the years, and where we've done things, and smart cards are really good example this, they were great technology for the time, but my mom can't use a smart card, or she would have a really tough time using a smart card. So it'd be really hard to apply that kind of in the the citizen or the commercial sense from a customer perspective. So I think we're now at a at a really good inflection point where we have the technology where we've caught up where we can provide those strong security aspects, but also the great user experiences that I love.

16:00
X.

16:01
And you know, since we're in a policy forum, let me you know, turn to each of you. What are some of the policy issues that you're seeing come across your desk related to digital identity? And what are some of the things that folks on this webinar who are learning to, you know, looking to learn a little bit more about the intersection of digital identity and cybersecurity and what we might see the government do? What should they be thinking about here? Tim, I might start with you given?

16:29
Yeah, sure. So one of my other kind of primary roles for Carson Foster's, I handled most of his work on the fender Services Committee, and it's kind of a weird song and dance. Having him, you know, try to emphasize the importance of a digital identity is it's not really in a finished service committees jurisdiction. But it's a really important conversation I have and it comes up frequently, because you are constantly authenticating yourselves through your mobile apps, to your bank, your bank doing it on your own behalf. So whenever it comes up, when we say like, Hey, would this be, you know, at least a convenient application? Your banks are good. All right, Isaiah, yeah, of course. But it's just been kind of a strange go to, you know, have to talk about that in a, you know, a jurist committee where you don't really have primary jurisdiction. But on that note, it's just, it almost seems like a no brainer. Anytime this conversation comes up. I think it's just for for know, your customer anti money laundering aspects that just make things much easier, much quicker and save everybody a lot of money. So it's, it's certainly just a recurring theme. And we've just been kind of hammering the message on that. As Sean said, it's, it seems kind of crazy that we haven't gotten there yet. But, you know, we're happy to see that the wheels are at least moving.

Jeremy Grant 17:49
Cara, Sean, Connie, you perspectives.

17:53
I think as far as questions that I'm being asked frequently related to the the policy element of digital identity, privacy implications are probably number one right now, followed by topics around bias and equity, fraud and supply chain, risk management, creative ideas about how to stimulate market growth, and how enterprises of all kinds and specifically federal agencies should be balancing all of these different objectives, while they're designing procuring, or even federating with an identity solution.

Cara Mumford 18:33
Yeah, I would, I would agree that I think privacy concerns are a really big question when it comes to digital identity. And then the other thing I would add to that list is how, how both the federal government and the state governments kind of treat digital identity and how they interact. Because, you know, ultimately, a lot of the identity issuers are at the state level, but then you also have, you know, the State Department issuing passports, Social Security Administration. And so figuring out how to kind of get all of these entities to work together, I think, is a really big challenge.

Sean Frazier 19:01
I think the only thing I'd add, and I love Connie's comments about equity and making sure we're building things that everyone can can participate in. So it's not just a one class, the folks who can do really cool stuff, and the other class of folks have to do the hard stuff. That's super important. The other thing that's super important is to have flexibility and agility with some of these things, because the technology is changing so quickly, that I think, well, by the time we put a stake in the ground rents, oh, Gretzky, you know, saying about the skate to where the pucks going not to where it is, and we have the the propensity to kind of put a stake in the ground where the puck is and forget about where the puck is going. So there's the things we're building and we can provide some ability to be flexible and agile, as new guidance comes out as new technology comes out so the folks can kind of apply those or think about how to apply those in their future self versus where they are today.

19:49
Alright, thanks. I'm gonna come back to the privacy issue in a bit. But I wanted to dig a little deeper for with Tim and Cara, on talking about the gap between physical and digital credential.

Jeremy Grant 20:00
shows at least in terms of what consumers are dealing with. So Tim, you mentioned your boss authored the bill, the Improving Digital Identity Act that it's focused on this topic. And Cara, the his gap, just mark that were revised version of the bill last week.

20:13
And you know, that really puts a heavy focus on closing this gap between the paper and plastic credentials we use in the physical world to prove who we are, and the lack of any real counterpart, you know, in the digital space that we can use online. Can each of you talk just a little bit about the bill? And what might come next in, in the legislative process?

20:33

Sure, yeah, I guess I'll start mainly made these visits some of the task force with a couple different agency heads involved to try to set up you know, what a digital identity application would look like, here in America. And embedded within that is the important

Tim Weiler 20:55
sorry, my dogs about to get excited that the mailman. The important standards that NIST has to set for us to make sure that we're there was also a bit of grant money. I don't think that made that into the Senate version. But maybe that's where Cara can pick up.

Cara Mumford 21:14
Sure. So we in the Senate we worked closely with I think it was cinemas team and also Senator alumnus, his team to come up with a bill that we could put on our markup. And, you know, our perspective, I think, in building in editing, the bill that came out of the house was trying to come up with something that, you know, could empower the taskforce to come up with recommendations and not you know, necessarily, we didn't want to presume the outcome of anything that could potentially come out of the task force. And we wanted to make it so that the task force would actually come up with, you know, productive recommendations to move the ball forward, because I think that there's a recognition from everyone that this is a really important issue. And it warrants you know, really in depth study and attention, not just from the federal government, but bringing in outside stakeholders. And so that's, that was kind of our perspective. And I was glad that we could, you know, work closely with our other partners across the island, actually, you know, get it through the markup.

22:12
Right, thanks. And Tim, and Connie, I wanted to ask you about there was another portion of the original bill with Congressman foster introduced that was dealing with this work and digital identity, the need for framework that if I'm, you know, be at a local Vital Records Bureau who wants to do a digital birth certificate, or the State Department with a passport or a DMV at the state level, who wants to close this gap between physical and digital? You know, how do they have sort of a playbook of standards and best practices they should follow? And, you know, that was something that I know, Congressman Foster was successful and peeling off from the original bill and getting included in the history authorization that was part of the chips and science act that became law just a couple of months ago. So I wonder, you know, Tim, if you could talk a bit about the provision and Connie, now that this has been directed to take on new work here, you know, any thoughts on what we should be expecting?

23:06
Oh, well, I guess it was, I'll highlight the provision, I think Connie is probably gonna have a better read on what we should expect going forward. But I think it's managed to,

Tim Weiler 23:15
you know, directed NIST, to kind of tell us how we can make these systems interoperable, like you said, amongst different right now, it's a very kind of

23:27

segmented approach with our DMVs, our state DMVs kind of all do their own thing. So we need to find a way for them to talk to each other effectively, if we're talking about some sort of a national digital identity, something that's going to work in every state, kind of like the real identity regime. So we've kind of already have that laid out, but we need to transfer that to, you know, what we've put together for in the digital space. And also, you know, wants to make sure that we're using strong identity proofing, proofing, and, again, just a really robust privacy protection regime, in whatever we develop. So I think that's a really important, you know, set of standards that NIST is up to task with.

Connie LaSalle 24:08
I would agree, I think, symbolically, it is an enormous win that NIST's identity work has been recognized to the extent that it has been through chips and science. And it's not just for NIST, I think it's a big deal for all of our stakeholders who are consistently even to this day, communicating the value of our work, and calling on us to to do more in this space. And, you know, we can, we can do more with more as our is our go to response. So I think, expect even more of the excellent both foundational and applied research that the program has delivered over the last few decades. I think as we touched on earlier, there are a lot of challenges, and also new opportunities associated with identity verification.

24:57
And some of the ones that we want to explore more deeply include proving methods that balance security, privacy, usability inclusivity. I mean, I could just keep adding priorities to that list, but really finding the balance and offering additional options to both enterprise customers, but also consumers. stronger and more accessible authentication methods, not everybody has the same resources, whether that's bandwidth, or a mobile device, you know, consistent ability to provide identity evidence, that sort of that sort of thing. And then looking at various Federation models, and different approaches that can help to support greater interoperability just like like you mentioned. And I think in the near term, we're really focused on better understanding people's experiences implementing our existing standards and guidelines, so that our work is even more relevant, timely and responsive to those most pressing needs.

26:01
All right, thanks. So last couple of questions. I've been talking a lot about legislation looking at the consumer side of identity, you know, what, you know most Americans are dealing with in their day to day lives. But there's also the big focus on enterprise security. And I mentioned earlier, the role of compromised identity credentials played in the solar winds incident that led in large part to the strong focus and identity in the White House zero trust strategy, which was finalized in policy is OMB memo 2209, about nine months ago, Sean and probably Connie, again, with anybody else who wants to jump into just wanting to know if you could talk a little bit about that strategy. And more to the point, why is it that securing the identity layer of systems is so important, and essential to implementing zero trust architectures in the enterprise world?

26:46
Yeah, I think, you know, certainly, it forces us to think more holistically about security. And as I mentioned earlier, we can call it zero trust today, I don't care what we call it 10 years from now, where we're just calling it security kind of baked in. I think the the apt Star Wars metaphor here is that, you

know, if an 18 year old kid can can drop a torpedo into an exhaust port and wreck your business, then you haven't thought about security holistically. And you haven't really thought about what are all my attack vectors? And how can I protect folks who are trying to access things. And I also mentioned that, you know, identity is pillar one for a reason, because it's the foundation on which all other things are potentially built. Nothing happens till someone tries to or something tries to access something to access data. So zero trust is really all about, you know, kind of treating data as the crown jewel and figuring out what the access modalities are to the data, what the protection modalities are to the data, making sure you have all those protections put in place, I think one of the challenges that that we've seen over time is that it's taken us a long time to get to kind of full multi factor authentication. And while we've been doing that, the attackers have been taking advantage of that, because we really left it as low hanging fruit for the attackers. And I think up leveling those things like making sure that you know, strong phishing resistant multifactor is important, strong single sign on with strong protection are important. These are both not only, you know, security, but also and user enabler capabilities as well, if we think about them, because they enable users to kind of get access to things in a seamless way, provided we use mechanisms that are that are that seamless. But I think that really kind of starts there in regards to, you know, there's data that someone needs to get access to right away very transparently. And we've got to protect the mechanism that folks get use to get there across the board, not just for some, but for all. And that's part of the challenges, too, we've commonly seen, where folks will get kind of 80% there with MFA. And the last 20% is the hard part. So they don't necessarily get there. You got to get there for your privileged accounts for your user accounts for your admin accounts, you know, for your executive accounts, and you know, anyone walks into something, you got to be holistic across the board.

28:49
I can only say plus one that everything Sean just said. And I think as federal agencies and their commercial partners begin implementing their zero trust plans that were required out of the the zero trust strategy. I expect we'll learn a lot from them, including the good, bad and the ugly.

Jeremy Grant 29:09
Thanks, and wanted to ask a follow up on that. And actually, you know, tying to what you were saying Sean around the need for phishing phishing resistant authentication, I mentioned in my opening remarks and last month, Uber breach, the attacker has not only compromised passwords, they also managed to bypass the MFA who were had in place. We're seeing this happen more and more these days where some of the legacy tools that we use, like a one time passcode or pushing Yes, on a push notification. You know, you can socially engineer somebody to handing over a passcode or pushing approve, which is one of the big reasons M 2209 said agencies really need to move to MFA that is specifically phishing resistant so you aren't susceptible to those attacks. Where do you see the market going with MFA right now given you know that guidance as well as you know, the the fact that the attackers seem to have caught up to some of our, our, you know, first and maybe even second generation attempts with this technology?

30:00
Yeah, I would say of course they did. Because we made it easy for him for a long time with just the password and we add MFA, we made it a little harder. So we're pushing the attackers up the sophistication stack, which is good, it cost them more remember, attacking is a business. So the more it

costs them, the more painful is for them. But we have to move them further up the complication stack, and add way more friction for the attackers. And I'm a big believer in adding friction for attackers and not for users. And I think that's where phishing resistant authentication comes in. Because we can use something like a biometric on an iPhone or a MacBook, which is really simple for a user to use. I gotta go back to my mom is the limited litmus test, you can use face ID she can use Touch ID, that's pretty simple for her and by the way, is a stronger authentication.

30:41
Thanks, Connie. Any perspectives? Or Tim? Or Cara, if you want to jump in on that topic as well?

30:46
Yeah, I think just, you know, pulling on one thing that that Shawn has, has mentioned in his his comments, I'm hoping to see more phishing resistant options that are broadly available, affordable, portable, privacy protective, and easy to use, you know, if we're not hitting the all of those factors. I don't know how, how we can expect adoption gains, the way that we really need to to create that friction for the attacker to raise the bar. And not just one set of individuals at a time but but for everybody being mindful of the fact that again, not everybody is going to have you know, the same access to the same resources to raise the bar, at least not at first has to be part of the conversation so that we're not stuck back at, you know, square one, again, for certain groups of people. And so that we're not worsening existing inequities that are contributing to the kind of digital divide that we're now having to address, because we didn't think of it however many however many decades ago.

Jeremy Grant 31:55
Thanks.

31:58
And, Shawn, just one follow up. Again, on the octa side, obviously, you are a company that supports a lot of implementations, both in government and the private sector. Other examples where you're seeing zero trust architecture is really successfully implemented. And, you know, what are some of the lessons that the public sector might want to take from some of what we're seeing in the commercial sector? Or vice versa? For that matter?

32:18
Yeah, we see a lot. And I think the what separates the successful implementations from the ones that struggle a little bit is really just a mindset shift of how you, you you work toward zero trust, if you view it as as kind of changing your lifestyle, your security lifestyle within your organization and protecting the things that are important. So first of all, identifying what those are identifying what the access capabilities of the access modalities are to get to those things, you have a much better chance than folks who sometimes look at it as yet another unfunded mandate. So one of the things that the challenge is some folks as you look at and say, Okay, well, someone's telling me, I need to do this, I don't know what this is, this is probably something, I gotta go buy from somebody and just layer on to the other 10 things that I bought, if you're looking at it from that perspective, you're kind of looking at it in the exact opposite way of the way you need to, you need to think about how you kind of build it in holistically into your organization start and really start from a piece of data that needs to have access to

it, and then you build out from there. And if you kind of started starting to think about it, and I know it's hard because a lot of organizations, both commercial and public sector have a lot of legacy. There's a lot of stuff that's been hanging out there for many, many years. Were like, oh, gosh, I can't go back and touch that. Because if it ain't broke, don't fix it. So start with the things you're building now and work your way backwards and figure out okay, how do I, you know, can build this approach as I'm updating things because all things get updated, you know, even legacy things have to get updated over time. You have a plan, put a plan together, I think for the folks who look at this and think I gotta go buy something, I don't know how to implement it. That's a challenge. But if you put a plan together and figure out, start with the data, and then move your way out, you'll be much more successful. And we see a lot of folks doing that. Thanks.

33:49
So I want to shift a bit to the technology side of the house. And I say up front, I tend to approach identity from a technology agnostic philosophy, the idea being we shouldn't be leading on the policy side with a view that this particular technology is the solution to an identity problem. Let's first define the problem we're trying to solve and then select the best technology. That said, I think it's really hard to get too far into one of these conversations without somebody saying, but what about biometrics? And what about blockchain? So now that I've asked those questions, what about it? What do you all think?

Sean Frazier 34:25
I love biometrics not not so big on blockchain for identity yet, but we'll see. We'll see. I you know, I go back to my early days at Netscape and the reason the internet got so successful so quickly was it really was the the adherence to standards and building standards that everyone could build to. That accelerated a lot of things that we did back in the 90s to get everyone on the internet. I think we got away from that for a long period of time we're starting to get back and I think that's the one exciting thing for me about identities identities, kind of leading the charge on building an open standards. To get to Connie's point about you know, everyone should have access to this and everyone who has a phone in their pocket everyone who has a smartwatch on their wrist.

Jeremy Grant 35:07
Thanks, Connie, or Cara, or Tim, want to weigh in on technologies at all.

35:12
So I tend to agree with you, you should focus on the problem you're trying to solve, rather than create solutions in search of a problem. And I think that technology should be viewed as a wonderful enabler. But it is a means to an end. And I'm, I'm intrigued by the promise of distributed ledger technologies like like blockchain. I'm curious to keep learning about the trade offs. You know, just like other ones, novel technologies, I know the Internet has come up Cloud has not been mentioned yet. But it was sort of viewed as magic at one point in time. The tranche of technologies that that you mentioned, are exciting to me and potentially transformational. I think at the same time,

Connie LaSalle 35:57
they will, and it already has started to introduce some real challenges that that this community and others are going to have to contend with both technically, and as a matter of policy. And Sean, I

appreciate the shout out and supportive standards clearly sent our name, NIST is going to continue to advance those underlying standards. Plus measurement science plus all the research is critical to you know, whether it's distributed ledger technologies or cryptography. And we have every intention of continuing to play a role in shepherding in the next era of of more responsible innovation.

Cara Mumford 36:37
Thanks, other perspectives, I think, from the Hill perspective, and I don't want to speak for Tim, but at least from my perspective, you know, remaining technology agnostic is really, really important, because we're dealing with everything at the 30,000 foot level. And so the second that we start talking about individual technologies, and putting them, you know, into laws potentially like that, I think, sets up a really potentially problematic situation down the road where those technologies either get phased out, or they need to be, you know, they are no longer, you know, up to date or anything like that. And so I think that, from my perspective, I do a lot of work and a lot of thinking to try and remain agnostic and to build enough flexibility into the the way that we're thinking about issues so that they can kind of evolve, and you don't have to be changing laws are, you know, amending committee reports, which is not a thing, but, you know, to actually make it so that the thing still make sense.

37:34
Yeah, that's certainly been our outlook as well, as you know, we're just generally agnostic that, whatever way this gets done, you know, what we're supportive of, but, you know, generally what, we don't want to do something that doesn't make sense, five to 10 years from now. But I will say, particularly with biometrics, I think, if we're really trying to get away from these legacy forms of identity, unless we're gonna, you know, tie our digital identity, you know, if when you're signing up on your mobile wallet, or whatever, if you have to punch in your social security number, we're kind of defeating the purpose there. So on some level, you know, Biometrics is very well may have a role to play, but we need to make sure that that's done responsibly. And you know, that it doesn't leave anyone behind in certain areas. But certainly, second, everything that the other panelists have said is we need to kind of keep an open mind with this. And, you know, focus on a solutions based architecture here, instead of just trying to solve one problem, you know, do something that we're just building something from the ground up, we're not just looking to pinpoint one particular area to to fix here.

38:44
Thanks, Tim, if I could just ask a follow up. I know, Congressman Foster has been a, you know, very strong interest in the possibility of a central bank digital currency. And there's talked quite a bit about how he views

Tim Weiler 38:57
solving the digital identity conundrum as being key to enabling, you know, something like a CBDC. Can you talk a little bit more about that, and sort of where he's coming from on this and some of the work you're doing there? Yeah, absolutely. I think that was kind of his foray into this interest in the first place, was the just inherent need to authenticate yourself when you're using, you know, legal tender. Right now you use cash pretty much anonymously, but at the rate and speed of transactions that the CBDC would offer. using a CBDC would absolutely not be purely anonymous. I think everybody understands

the logical Nexus that we've seen play out with, you know, a US stablecoin or something of the like, so certainly very important and closely tied to it.

40:30
Thanks, essentially, we have a bunch of questions that have come into the q&a, I don't think we'll have time to address all of them. But on the privacy side, and back to the point you mentioned about anonymity. Is there a place for anonymous online identities and a future where we might be valuing cybersecurity over private or experimental expression? Is everything needs to be fully known? Or do we still have some anonymity in the future? Well, it?

40:54
I mean, in my mind, I think it operates, you know, the way that you buy stocks, you know, you don't know who you're trading with, you're doing it through a broker. So you're pseudonymized, you have your privacy and that way, but at the end of the day, if something goes wrong, there's a trusted regime and a trusted court system, you go to to say, Hey, I was frauded. Here, who's the guy on the other end? Can we track them down to see what went wrong? And that's just kind of an essential function of, you know, transacting. So if you're asking pure anonymity, I have a hard time seeing that play out. But certainly, there's areas where you just don't want to reveal, you know, all aspects of your personal information or your you know, if you're trying to buy a bottle of wine, they need to know that you're over 21, they don't even know your particular age, but you can attest to that with, you know, a digital identity that allows you to release certain aspects of your data selectively. So, certainly, yeah, I think that's, that's an essential function.

Jeremy Grant 41:57
Thanks, Connie, let me ask you to follow up a little bit on that you mentioned before, you know, NIST produces, you know, risk based guidelines, you know, in some cases, you need to be there needs to be no doubt in terms of who somebody is, in other cases, the risk might be such that it's less important. Can you talk about where, you know, risk might play a role in terms of anonymity versus being fully or partially? No? Sure. You know, I think our guidance really leaves it up to each organization, we, our main audiences, organizations versus a direct consumer, we leave it up to them to decide, you know, what level of proofing they think is probably necessary based on the potential impact should something bad happened.

42:39
And, you know, from from that perspective, I think we are preparing for a world in which all of the above needs are true, technically, where you have a high degree of proofing and confidence that's required just whether it's because of the the impact and the risk or because a regulation is telling you, you have to. And then on the flip side, I think there will be some interactions that are that are lower or negligible impact where forcing somebody to provide their identity might have more more harm than benefits. So I think just making space for all of those possibilities, and really interrogating them based on risk, is the approach that we've defaulted to.

Jeremy Grant 43:26
Cara, Sean, any perspectives on the privacy and anonymity question?

43:33
All right. Since this is a policy forum, we've been spending a lot of time talking about what the government can do on the policy side. But obviously, this is something government alone is not going to solve the problem. Where do each of you see a role for the expertise and solutions of the private sector

43:47
and all of this?

43:50
So I think, you know, speaking from the private sector, I think that there's there's certain best practices that can be applied here. I think one of the things that comes out and having conversations with this is that, and again, I'll lean back on the open standards a little bit is that really kind of future proofs you when you make decisions about technology, you can kind of plug in and provide a you're all speaking the same language and singing the same tune? You know, I happen to believe that octave is one of the best digital identity organizations on the planet, I wouldn't be here if I didn't. But you know, you can fire me and go to somebody else that provided you had the right open standards. And it's not, you know, it's not a big heavy lift, and it shouldn't be a big heavy lift, you should be able to move technology stacks. Technology changes over time, as I mentioned earlier, all kinds of new things come out, maybe blockchain becomes a thing and you want to plug in a blockchain identity system and you want to be able to have a tie in to the same open standards that we've been using for the last 10 years. That should be the ability and you should have the ability to do that. One of the challenges is when you get kind of locked into technology and something that it's not really benefiting you. You're kind of thinking about, Okay, this technology company I'm leveraging but they're not as good as they used to be, but it's really hard to unplug that. There's also the propensity to think about I can build this myself because I know all the things I need to do. I know my data, I know my infrastructure. I know my organization and you kind of build it very bespoke system. But organizations have gotten in a lot of trouble doing that too, because it's hard to update, it's hard to maintain, it's very easy to build a thing. It's very hard to support maintain a thing.

45:12
Thanks, other perspectives on the role of the private

Cara Mumford 45:15
I think for me, it's having a relationship and fostering open conversation between government and the private sector is really important, particularly for us on the hill, because, you know, most congressional staff are not technologists, which I think is, you know, a real bummer to a certain extent, because, you know, we have a lot of these conversations, and we don't always have all of the technical expertise to be able to make informed decisions about, you know, how we're, we think a certain bill should go. And so that's where I think that having the private sector there to really ask those questions of and say, What do you all think about this? What do you think about that? And how should we be thinking about these problems is really important, because it gives us a perspective that we don't necessarily have all the time on the Hill.

46:02
I agree with that. And I think that that's evident in our in this collaborative relationships with the private sector. I mean, we simply would not be able to do a lot of the research that we do without their their involvements. I do think, you know, shifting to specific areas where I see gaps and where some, some private sector exploration of those gaps and innovation could be helpful. We need more identity proofing options, of all strengths and of all types. And I think particularly thinking about the fact that I've seen that some some browsers might shift away from cookies, right, you'll see the role of third party data decrease, I think that leaves us with an opportunity to explore different different ways of interacting with consumers, thinking about how user experience and related research can yield the kind of information that that others might be collecting on an individual by individual basis, which could have sort of a secondary or or in some cases, primary positive benefit for for privacy, in addition to raising the security bar. So as a catch all response, I think privacy enhancing technologies, various implementations of digital credentials are also really exciting. I think it's, it's early days, but if you look at what's happening with mobile driver's licenses, and think about that kind of implementation, but for other contexts, is is exciting to me. And I can't wait to see what kind of innovations happen in the next couple

Sean Frazier 47:45
So a quick shout out to Connie's organization. There's a sub organization under NIST called NCC OE this Cybersecurity Center of Excellence that we participate in a lot of other private sector partners participate in as well. And that's a good mechanism for us to share information because we all know this is not a technology problem. But there are technology answers that can be gleaned from looking at how people interact and how systems get plugged together. And those best practices are really important.

48:13
Hey, thanks. Well, we had a whole bunch of questions that popped up during the Questions tab, we're not going to unfortunately have time to get to them today. Given that this was already a few minutes over the 45 minutes that was expected. But I was told by Tim, we could run a little bit over. Let me ask you one final question, which is, as your moderator, what was the one thing I should have asked you about today that I did not? And then what's the answer to that

48:36
question, of course.

48:39
Or any other final points or concluding thoughts? I would have liked a couple

48:46
a couple more Star Wars references. I think you started out strong. A couple more in the end within good. Thank you.

48:55
Other than that, you are great.

48:59
Final points.

49:01
I mean, I'll just make one. I think just wrapping up the conversation. My takeaway is that there are as many challenges as there are opportunities in the digital identity space today, it's a really exciting time to be in identity where there is a lot of a lot of stuff happening. There's a lot of momentum.

Connie LaSalle 49:19
You know, and it just we're we're working to tackle a lot of them. But but we need more people. So to the extent that you can recruit more people, whether it's on the technical side or or the policy side, I think you'll certainly be hearing from from NIST even more, and and the more the merrier. This is a great time to be involved in in digital identity.

Jeremy Grant 49:43
Thank you. Your final thoughts, Tim?

49:49
I was just gonna say kind of tying into your last the last topic talking about the public private partnerships and the role that you know, private industry plays I think at the end of the day that people Well, despite the healthy criticism of, you know, your government holding on to sensitive information or being custodians of it, I think most people agree that you want your government to kind of issue your identity. So it's, you know, it's certainly a role that we're excited to fulfill and we should fulfill. You know, it's, it's, it's just an important function that I think at the end of the day is, you know, should be trusted to the government. And we look forward to continuing the conversations with the private sector. And that's where we get, as Carol said, most of our experts, expert knowledge. So, you know, certainly I think that it's, it's, it's moving in the right direction.

Cara Mumford 50:44
Great. Thanks, Cara. Any any final comments? I don't think I have anything really profound to say wrap up. But I certainly appreciate the panel for being here. It's been a really great conversation and to you, Jeremy, for hosting us. This has been great. And I am really excited to see how these conversations progressed, because this is certainly not the last conversation we'll have about this issue. Right. Appreciate it. Well, Cara, Sean. Connie. Tim, thank you so much for taking the time today. Zack, thanks for the intro. And thanks to Tim Lordan to the Congressional internet caucus Academy for hosting this event.

51:17
You have a great afternoon and forget the follow up questions. Feel free to reach out to us or at least to me, I don't know if everybody else can talk. But thanks again, everybody.

51:24
Thanks. Thanks everybody so much. Have a good one. Thanks.