FINISHED FILE

INTERNET GOVERNANCE FORUM USA 2021

Why don’t we have better digital identity? What could we do if we did?

JULY 14, 2021

1:00 P.M. - 2:15 P.M. EASTERN

Services Provided By:

Caption First, Inc.
P.O. Box 3066
Monument, CO 80132
1 877 825 5234
+001 719 481 9835
Www.captionfirst.com

***

***

>> DUSTIN LOUP: All right. Hey, everyone. Welcome back from our quick little break there. We're looking forward to this next session. This is the first time that we, you know, had a primary role for digital identity in our program and I think that this is a great thing for the IGF USA and look forward to this being a good base line for future conversations that we have here at the IGF USA, and with on our communities.

So I will hand it over to Jeremy Grant who is the coordinator of the Better Identity Coalition to take us through this panel.

>> JEREMY GRANT: Great. Thanks, Dustin, and welcome, everybody. Glad to have you with us.

So the title of this panel is "Why Don't We Have Better Digital Identity? And What Could We Do If We Did?"

I'm joined by a great panel, senior counselor for strategic policy and innovation, US Department of Treasury, Ann Wallwork. And Pam dingle with Microsoft and Patrick Kinsel, is CEO of Notarize. I thought it was important to talk about that the IGF conference is going on for years, but this is first time that you have all actually a panel on the topic of digital identity.

It reminded me -- so today I run the Better Identity Coalition and part of the cybersecurity team at Venable.

Ten years ago, I was working at NIST, the National Institute of Standards and Technology, leading the newly launched program office for the National Strategy for Trusted Identities In Cyberspace. Such as we are just getting to identity here this year within IGF, I had a meeting shortly after we launched the program with Vince Cerf who was talking about when they were architecting the Internet years ago, they didn't quite get around to doing.

And with it, you know, it's turned up some problems and challenges. I think that's still the case today. Identity is really important to the Internet, but it has been something that has taken us a little bit of time to, perhaps recognize its importance.

So you know, diving into things in terms of, you know, framing the discussion. You know, I talked going ten years back. I will go 28 years back to a famous cartoon, if you are interested in the Internet. You probably all remember this in some cases when it came out, but it's now been 28 years as of about two weeks ago, when Pete Stiener talked about identity and the Internet.

And there's a couple of things that I pointed out about how much time has passed. One, these dogs are dead now! Because of dog years, unfortunately. And, you know, their kids probably are as well. But the media of the cartoon has changed quite a bit over the years, in that, look when this first came out, I think I was a freshman, maybe a sophomore in college, and, you know, it was a great way to capture the novelty of going online and, you know, occasionally some of the funky things you might run into.

But these days, we're actually seeing the dogs on the internet weaponized. It's an anomaly when a major breach happens these days and identity is not providing the attack factor. More recently started in 2016, we started seeing some other countries who are not so friendly to the US actually looking to weaponize dogs on the Internet and how, you know, easy it could be to, you know, be anonymous or synonymous. While the dogs might be long gone, the problem with the dogs is more acute than ever.

And it -- identity really gets into a whole bunch of different issues not just the security aspect but how do you create an identity layer for the Internet that is good for privacy that can deliver really good customer experiences, that can help different regulated industries with compliance that can do things in a way that can lower transaction costs?

And while there's all of these different facets of identity, the one thing that people keep talking about when they try to solve these issues how do build trust on the Internet. Trust is really hard to get right.

But identity, if you can do it right -- and that's been pretty hard to do can enable trust. Identity can be the great enabler, providing the foundation for digital transactions and online experiences that are more security, easier to use and can protect privacy better than what we have today.

The challenge as my old colleagues at NIST pointed out a few years ago is digital identity presents some real technical challenges. The problem often is trying to proof individuals over an open network. And these processes we use to establish digital identity provide a whole load of opportunities for impersonation and other attacks.

So our approach to date has not exactly been particularly sophisticated. So, you know, other than bringing a whole, you know, new meaning, if you or your family somehow picked up a pandemic puppy during the events of the last year and a half.

The whole focus on questions here has proven to be really practical. Sometimes with security questions maybe you change your mind. Maybe you forget and then you get thrown into the pit of despair, also known as the account recovery process. We have these knowledge-based questions be used for security when the adversaries we are trying no block with these sorts of things already know the answer.

And the authentication side this has not worked particularly well. Any time you are coming one all of these criteria. Nobody can manage this for one password or 20 or 30 or 200 or 300. There's such thing as a strong password in 2021. Even a 64-character password that meets all of these criteria is still susceptible to phishing, password reuse, given how many people reuse passwords across sites. When you put these things in place it makes your employees and customers hate you. They do everything they can to get around it, like just reuse the same password and put an exclamation point at the end.

The idea that passwords can be secure, that ship has sailed. And the cost of bad identity solutions, this is a chart that we actually had from three years ago when we released our policy blueprint and the Better Identity Coalition. In fact, tomorrow is the three-year anniversary of that. But it starts to show you some of the numbers that we were seeing back then in terms of nearly 17 million victims of identity fraud, nearly 17 billion stolen. Massive increase year over year of data breaches and, again, identity is, providing the attack factor for a lot of it. In the idea of dogs on the Internet has been growing into something that has some real numbers and some real problems behind it.

Synthetic identity fraud online has also been on the rise. This is a chart from a publication that the Federal Reserve published about a year, year and a half ago where they have been doing a series of papers looking at -- it's the fastest type of crime where you see criminals create a digital Frankenstein, leveraging a real Social Security number that the credit system has not seen from my 10-year-old, pairing it with fake information and then tricking the banks and the credit bureaus into thinking that somebody is actually real.

Of course, this all just got worse thanks to an awful pandemic that, you know, in addition to sadly killing a lot of people and making a lot of other people very sick, also made it basically impossible to engage in any in-person transactions for the last year and a half. And, you know, the numbers of identity fraud we have seen, the labor department has estimated just from state unemployment benefits, organized crime stole more than $63 billion of federal governments given to the states to help people out of work and they think that number may top $100 billion by the time this whole thing is over. This is one example of the challenges we have seen the last year, and the doors it's opened up for criminals thanks to having weak identity infrastructure in the US.

So why is has all of this been so hard to solve? We will talk about this in our panel, and I promise I will get to everybody in a minute. I talk about this from the perspective of the problem we have that I call the identity gap which is -- it's not that we don't have nationally recognized, authoritative identity system, we have the Social Security, and passport, and the driver's license, and global entry for a small group of people but everything we have is stuck in the paper and plastic world, where transactions are moving increasingly online.

A lot of the challenges we have, had ever since those dogs on the Internet first appeared is figuring out ways to close this gap between the authoritative systems the government has today, and the types of transactions everybody is engaging on which are increasingly digital.

And, you know, if you ever had a knowledge-based question, applying for a credit card, well this was an attempt to get around the identity gap. This is industry responding to a -- probably more of an unconscious decision by government than a conscious decision to not create digital systems that went beyond the paper and plastic ones.

So, you know, industry needed something to enable trusted digital commerce and these solutions that are generally called knowledge-based solutions. Challenge is like that with many security tools, the attackers catch up. And these out of wallet questions are not as secret as they used to be. This is a problem for quite some time. These are from 2015, six years after the IRS had a major breach when they were allowing people with some pretty weak knowledge-based verification to get access to their tax transcript online, which had a whole bunch of sensitive personal information and data.

And as the article pointed out at the bottom being the hackers already had the keys and we had so many breaches that a lot of these answers are known these to the point where if somebody answered the knowledge-based quizzes, too quickly there's a sign of fraud. The average human probably gets one wrong and probably has to take some time to look it up like their monthly mortgage payment because they might not know it offhand.

I want to jump into the question today, having set the stage here, you know, why don't we have better digital identity? And what could we do if we did? And I will stop sharing my slides at this point so we can see our fantastic panel a little bit more clearly, but let me actually just start going down the line. I will ask Anne and then Pam and Patrick to introduce yourselves and, you know, provide a little bit of opening thoughts and then we will dig into some questions.

>> ANNE WALLWORK: Thank you, Jeremy. Let me first of all, I'm delighted to be here with everyone --

>> JEREMY GRANT: We can't quite hear you. I'm not sure if your microphone --

>> ANNE WALLWORK: No.

>> JEREMY GRANT: It's better if you get closer.

>> ANNE WALLWORK: No, I can't do anything with volume. Does that work?

>> JEREMY GRANT: Decent, yes.

>> ANNE WALLWORK: Sorry about that. Let me give the first US government disclaimer, the views I express here are my personal views only and do not represent the position of the Department of the Treasury or any other part of the US government.

As Jeremy said, I'm senior counselor for strategic policy in and innovation in the US department of the treasury's office of terrorist financing and finance crimes, TFFC write focus on innovative technologies in the financial sector, including particularly these days the digital identity.

I help identify and develop policies and strategies to address potential illicit finance and other risks related to innovation, but also to identify the benefits and develop policies and strategies to leverage responsible innovation, to support financial inclusion, and efficiency. I work closely with other US government departments and agencies, bilateral, foreign countries, and also international partners, including the financial action task force, which is the intergovernmental global standard setting body for any money laundering counterterrorist financing and counter-proliferation financing.

TFFC leads, and I had the privilege to cochair and lead drafter, which encourages a risk-based approach, leveraging technical standards and frameworks like the NIST 800-63 suite which was issued in March of 2020.

>> JEREMY GRANT: Thanks, Ann. Pam over to you. Quick introduction.

>> PAMELA DINGLE: That's an impressive introduction. I don't know how to follow that in those shoes. My name is Pamela Dingle. I work for Microsoft. There probably is a Microsoft standard disclaimer. I just don't know what it is. But in general, I work in -- I am the director of identity standards. So I work within the identity and network access division at Microsoft. We work a lot with the standards bodies and my background is as a 25-year veteran of identity management.

I have lots of experience and opinions on what the best practices are and should be around identity engagement.

>> JEREMY GRANT: Thanks. And Pat?

>> PATRICK KINSEL: Pat Kinsel, founder of Notarize. We are a smaller organization and my views do represent those of the company. And Jeremy, your introduction was. And I have my McLovin driver's license. Notarize, we are an online notary service. We started the company to solve that pain point for consumers and for industry. I think what's interesting for us as it relates to identity, though, is we have had to solve the practical problems of working with regulators to meet the standards to actually have transactions move forward.

Which is no small challenge in something that is state regulated, and also has to meet, you know, federal or, you know, GSE or whatnot, policies.

So we have been advocating for legislation across the country, helped pass 34 state laws, numerous approvals from different federal agencies and whatnot really to solve the practical problem of whatever the standards are, ensuring that they can serve customers meeting SLAs, solving issues of access, where people might not have what's required for transactions to move forward. At the end of the day, the conversation is about provenience. It's about tying identity to the actual creation of an object which I think is a sort of second side of the coin that industry and government needs to solve for and I'm excited to be here today and I appreciate the chance to participate.

>> JEREMY GRANT: Thanks, Patrick. Let me follow-up on that point to ask sort of a basic point for everyone, what do we mean when we talk about identity? Is it a credential? Is it just data or attributes about ourselves? Is it something in between? You know, how do each of you define it? And, you know, how should that sort of frame our conversation?

>> PATRICK KINSEL: I'm happy to go first. So for us, identity means something that's legally validated. So the person exists but has to be a standard, you know to a level that meets the, you know, requirements of that industry.

I think notarization is interesting because notarization touches real property, mortgage and finance, the legal industry, powers of attorney, different state requirements around witnesses and whatnot and so it's right sort of in the center of that Gordian knot. And so for me, identity means it not -- it is a practical identification of the consumer. It has to be all the way to the point of meeting the standard, and I think for us, as a company, what is so critical, it's not just that I can prove that someone exists named Jeremy in the world. It's that I can prove that that person Jeremy was actually physically present and personally took an action, and I think that is the core problem that we as a company are trying to solve. I understand there's many other definitions but that's the one that I'm dedicated to solving.

>> JEREMY GRANT: Thanks, Pam or Anne.

>> ANNE WALLWORK: Yes, when I think of identity in the context primarily, it's primarily in the context of customer identification and verification, regulatory requirements to the financial sector, for example, to open a bank account or access certain other financial services or to obtain government benefits or other government payments.

And in that context, we're talking about official identity, which is distinct from concepts of personal identity that may be relevant for unofficial purposes like buying unregulated commercial goods or services on the Internet or social interactions on media.

And so I like the FATF guidance of official identity which it is the specification of a unique natural person that is based on characteristics, which in the identity space, we call attributes or identifiers of the person that established the person's uniqueness in the population or the -- the relevant context and this is the kicker, is recognized by the government for regulatory and other official purposes. Proof of official identity can be digital or a combination of boat, but it -- at least at this point in time, depends on some form of government provided or issued registration documentation, certification. Such as the kinds of things that Jeremy was pointing to, for certificate identity card, the core identity attributes.

With we talk about identity solutions, we are talking about kind of -- we have a comprehensive view that includes all of the components addressed by the technical standards of the NIST identity proofing and enrollment, authentication, and credential life management and when it's relevant federation or other architecture that enables portability of digital identity.

>> JEREMY GRANT: Thanks, Anne and Pam?

>> PAMELA DINGLE: I think I would take a more metaphorical view of this. You know, everyone -- so the only sure thing about identity is that everyone has a different view of what identity means.

>> ANNE WALLWORK: True.

>> PAMELA DINGLE: This is literally the only absolute. The way I think of identity is a clothesline. And when you think of the different ways that you interact with the people in your life, the relationships you have in your life, those things are, you know, clotheslines on which you can hang events

and conversations and credentials and other things.

As an example of this, when you look at identity and access management, from a corporate IT perspective, right, it is very -- it's really cool that Patrick, you and I are on this call because we have very different views of this. In an IT perspective, the clothesline is the person's relationship with the person. It's identity-proofing events. You hang them on the clothesline and then you assign credentials, right to that relationship. And you start to assign access and entitlements to that relationship, right? And the whole time, time is moving on. And so you are accumulating -- you are accumulating good things like entitlements. You are accumulating data, right, organizations are collecting data about you and accumulating that.

Events are happening like job changes, you know, and you can think of that entire clothesline as the timeline of an interaction that represents your relationship with somebody, and so, you know, thinking of identity as that, as this set of clotheslines that emanate from you, as a human being right, and interact with other parties is the best metaphor I have found to talk about identity concepts.

>> JEREMY GRANT: I like and I have not used that one before.

Let me, you know, digging into some of the elements, you know, NIST sort of breaks it out into three things with identity. It's one, identity proofing which is hey, I'm trying to on an account for the first time or prove that I'm really Jeremy Grant and a particular Jeremy Grant, and what are the things you need to do. And the second is authentication. How do you log in? How does Microsoft or treasury department know it's me once I established an account. And then the third is federation. I have already gone through this process to get a trusted credential one place, how can another party decide to trust it?

Any thoughts on what parts are easier to solve these days or where the biggest challenges are?

>> ANNE WALLWORK: Well, I will jump in. And flag remote identity proofing as a challenge because as you pointed out, the most -- most of the underlying infrastructure in this country, such as digitalized state driver's licenses or US, state and local databases that -- or registries at this point, that either private sector identity providers or government-relying parties could ping against to verify identity attributes haven't been developed yet.

And I would also flag that too many people have difficulty obtaining or producing, if they once had them, they may have lost them, the government issued identity evidence that is required to establish official identity under either industry practices, financial sector or understandings of what is appropriate, and regulatory requirements, or under the overarching real ID act standards for identity-proofing.

>> JEREMY GRANT: Thanks. Pam or Pat any perspectives.

>> PAMELA DINGLE: I would say they are all hard. None of them are easy by any value of easy, but they are very different. You know, the blessing of federation, for example, is that it is essentially stateless, for the most part. Right?

You can -- you know, if you think of federation as a secure introduction, across domains on the Internet, right, you are kind of pinning a letter to the chest of the small child and sending them across the park, right, to introduce them to somebody if you will.

That -- that statelessness is valuable because it reduces cost. But what's happening right now is that authentication used to be stateless. So when you think of where we came from, we came from a world where everyone had a stream that was a password and essentially all you had to do to enable your application to use passwords as to check the string and then get the person ever asked, right? You would just test a password to see if it matches and then forget. And what's happened in authentication is that that has been obliterated and so blown into 50 million pieces because attackers are using that forgetfulness, that statelessness in authentication to attack.

And so you know with authentication, the challenge is now that we need that state. We need state in sessions. We need state -- you know, we need to be able to remember who is -- who is failing authentications just as much as who is succeeding at them being right?

And that state fullness is bleeding over. It's bleeding into federation as well, because what we are finding is that forgetfulness across domains is as dangerous as forgetfulness within them.

So for me those are the exciting ones and the ones I know best and I would probably call them the hardest.

>> PATRICK KINSEL: If I would chime in, I think we as a company, you know, we're not the government. We're not a massive, you know, multinational corporation with all of these use cases. We have the advantage of focuses on use cases, right? The mortgage closing experience and online auto sale, and that allows us to really try to understand exactly what is, you know, standard we need to meet. So for us, we don't see proofing as a challenge. You know, we're confident we meet the requirements that we need to meet, you know. Solving that on a global basis, I think is an exceptional challenge and I think it's really something that government needs to step in and I know we will talk about that later and provide better services.

For us, I agree with your expression Pam around the statelessness or statefulness for authentication. I think one of the things as industries move digital, I think the real goal is how do you have all the benefits of secure identity and all the benefits of frictionless online commerce, right? And those can be at odds and so, you know, for example, we may be able to meet the requirements for our industries, but those requirements may require a unique proofing event in coordination with whatever we're trying to do. And that's not a palatable experience for a lot of consumers.

There is an expectation, I will do this once and when I come back, I won't have to do this again which gets into the concept of, you know, the statefulness of the proofing that you have accomplished.

I think a lot of people think of this as a gate as a long-running service or benefit. You can't do those things until you have statefulness and you have a lasting identity, you know with the consumer. And I think a lot, they are all very hard. I think the other thing to add quickly, notaries in the legal context are considered proofing agents. And I think that's one of the interesting things I didn't appreciate when I started the company and it's given a lot of ways to move in this space.

A lot of experiences it's not natural to introduce a human to the process. The classic, something you have, something you have, something you know, I think that, you know, giving people a digital credential, possession of the credential is not sufficient, right? You still have to know that the person actually has the right to possess the credential, right? And the online, you know, notary interaction is -- it's been an interesting place for us to try to move out from.

>> JEREMY GRANT: I think that's an interesting point, Pat, in that, you know, my next question was, you know, why is the US struggled to develop and implement digital identity infrastructure. You make the point that the notary is a physical structure. It's a special category of professional, recognized under law that allows they are able to attest someone is who they claim to be.

You have a start-up company that you and a couple of peers have almost dragged an entire set of government and industry players -- I don't know if kicking and screaming is the right word, but it's taken, you know, firms like yours to say we will ought to be able to do this online as well and I know in some cases you had to engage on a state-by-state basis to change laws or regulations.

Why is it -- and I want to throw this to others as well -- has struggled to implement a digital identity infrastructure? Let me throw that back to you. Anne, I realize this may be a tough one for you in government.

>> PATRICK KINSEL: There's a lot in that one. Given our experience, I think it's a very, very, very complicated set of issues for people to understand. And I think that especially notary law, it's -- it was largely settled, you know, for a long period of time. So the people that would be the regulators are not actively engaged in the subject matter, right? And they are not actively engaged in issues of identity and whatnot.

You have to create knowledge and shared language and vocabulary and just address the issues to have momentum. I think what you are seeing now going from two states to 34 and soon to be 38. There's the council of state governments, you know, all of these organizations that have done the work and created infrastructure for people to have good dialogue. I think the other thing is that culturally, I think as a country and I would say at the federal level, we have to make some philosophical decisions about what we prioritize. And I think about, you know, the notions of KBA and whatnot, it's frankly in my view -- and I say this with all due respect, it's a way to have our cake and eat it too as a country. We push the responsibility on to private industry to manage credit profiles. And then talk about the issues with that, but then the only authoritative source is government.

But then do you move into biometrics? What methods of authentication and we have to make some really big decisions, I think, culturally what we prioritize in order to move -- to move these things forward. I think our position as a company is we will make due with the infrastructure that's in place today, right, because I think that there's areas where we can move forward and make progress, but it's super, super complicated and right at the heart of privacy and the right to anonymity, and biometrics. These are cultural foundational issues in our country.

>> JEREMY GRANT: Thanks.

Pam, any perspectives on your side?

>> ANNE WALLWORK: Yeah, I think that there's also -- (no audio).

>> JEREMY GRANT: Anne, we are losing you again.

>> ANNE WALLWORK: Oh, sorry, I will take a moment afterwards to try to just phone in so we can use that. But -- so when I disappear to go get my phone, please give me.

But can you hear me at all now?

>> JEREMY GRANT: Much better when you are closer.

>> ANNE WALLWORK: Okay so I think that the fact that we haven't really fully both in the private sector and in government recognized a kind of consensus level that digital identity infrastructure has become critical financial sector infrastructure for both efficiency, antifraud, combatting money laundering, terrorist financing and that also makes it national security infrastructure.

We have been looking at cybersecurity and funding it increasingly without fully looking at how digital identity, both the identity proofing and then linking that identity to trustworthy credentials is a part of the cybersecurity, but it's addressed very separately both in terms of financial institutions that separate AML customer identification from antifraud measures even though antifraud measures are using the most incredibly sophisticated, in some cases, forms of -- of digital tools from cybersecurity and -- and data privacy.

And I think we need both a whole of government and of public/private initiative to really recognize that if we're talking about losing $100 billion a year to fraud, and granted that we don't really have good statistics on the total amount of identity-related fraud either on the government or in the private sector which itself is an issue that I personally think needs to be addressed, we need to look at this as something that's urgent, just as we're looking at the incursions on our private -- our critical private sector infrastructure and our government systems, but to understand that digital identity is part of that infrastructure and we can't solve the issues that we are focusing on without looking at this issue more holistically. And I -- I'm going to stop now because I probably shouldn't comment on existing legislation, et cetera. So --

>> PAMELA DINGLE: Yeah, I will only add that this is also a people problem and a systems problem.

>> ANNE WALLWORK: I will be right back.

>> PAMELA DINGLE: Every single one of these things under some sense bubbles, that have existed for a long time, that have people in them, with habits and with -- who understand where the boundaries are. And what we're doing is we are pushing people beyond those boundaries, right?

So you have whole systems of people who understand how documents work. They -- you know, they understand their place in the system, right? And then we ask them to change those systems and it's really easy for people to rebuff that, for people to just constantly revert to what they know, right?

And so, you know, the beauty of a top down mandate is that you force people to go beyond their boundaries, but, you know, in the US, that isn't -- it is not how we work, right? We work essentially, I think on -- almost on a viral adoption program, where you have to get enough viral momentum to push past a boundary that would otherwise just rappel people back into their comfort zones. That's where we are now, trying to push those boundaries.

>> JEREMY GRANT: In terms of what government can do. This will be a loaded question given the role I play in the Better Identity Coalition. What could government be doing more to address this challenge that you all see out there?

>> PATRICK KINSEL: Well, I don't want to always go first,

but I will take the -- I will take the arrows.

You know, when we started the company timing-wise, it was 2015, and just to give one example, in 2012, the CFTB had compiled a study around electronic mortgage, they wanted to digitize and why haven't they? There were many issues but two critical issues that jumped out of me, and one was lack of access to digital notarization and lack of legal clarity. And the legal clarity challenge that I don't think people recognize, and I agree with the comment about viral adoption. Things have to get to a critical mass. You have to have industry adopting and you have to prove the efficacy. And you have to get to the second order problems when systems are in scale at a place and functioning, right?

And so, you know, in my mind, there's a lot of places in the country where there is either gray or opposed policy between, you know, agencies and I think that when you think about changing policy, we need to have an approach of what is the problem that we are trying to solve for and what are all the places that this actually touches, you know, in government, you know, wherever it may be at the state and federal level. I think what ends up happening, you have large industries that are choosing not to move forward because the issues are so complex.

I think about some of our conversations, around NIST, I will have the conversation with five different people, and I will get five different answers. The question is do you comply or do you not? So for me, it's just the work of engagement, of consensus, of getting clarity on these issues.

Even if it's too hard and too ambitious for us to solve the high order issue of proving identity on the Internet, we can make progress so the industries can move forward.

I think the other thing I would add is I often run into what I call frontier tech, right, in these areas. And there are companies who push the idea that if you jump up and down five times, I will know that you are Jeremy. And there are people who grab on to that and it's a theoretical state, the notion that you can -- I'm not going to get into -- and cast aspersions, but I think the real challenge is the bridge, right?

And access and the industries that we have in this country that have federal regulations that they have to follow about not treating customers differently, right, and not everyone has the world's greatest iPhone.

And as a country, it's not just a top down mandate, we need a bridge strategy to bring everyone into this, you know, new era and ensure people have access to the critical services which are increasingly being digitized and that's a hard conversation to have as well.

>> JEREMY GRANT: Other perspectives on the government side, I'm happy to jump in.

>> ANNE WALLWORK: No, I will take the bait. So I think that more -- and, again, speaking personally, I think that more robust certification against technical standards and audit, so that both the government agencies at state, local, and federal level can understand what solutions meet their needs given the risks they face, and -- and efforts to work maybe through the kinds of public/private partnerships that the FDIC has just proposed for exactly that sort of voluntary certification in the digital identity space would be -- as well as in other innovation as it impacts various sectors would be really helpful.

I know that Jeremy has been doing identity work not only with the financial sector, but also -- sorry, also with healthcare, and I think both in terms of what the government can do there, looking at where there are similar needs for technology solutions, and -- and then trying to use government's economy of scale as customers and in that regard, I would say we haven't been asleep at the wheel.

The GSA has a cross government, cross agency digital identity strategy to develop the kind of institutional structures for promoting a modular risk-based digital identity procurement use and feedback type of system that does have -- in creating the structures for that, it's not only US government has advisory -- it will have advisory structures that pull in the private sector as well.

I think going ahead and implementing that at whatever level is necessary to actually get it done and to actually implement the updated ICANN strategy which calls for just that sort of leveraging of private sector or government solutions, but coordinating in a way that -- that is privacy preserving, consent-based, cyber secure, and having an ability, for instance, through gov ramp to have those products certified.

So I think that's one thing that both is happening but that may need higher level impetus.

>> PAMELA DINGLE: I will just add one quick think, which, you know, having been in this game for quite a while now, I have seen successful public/private collaborations and failed ones, but the one thing that I think has worked incredibly well, if I would choose a poster is the NIST 800-63 work that has been done. Specifically that work is living. Like, it's -- not a case where you have created, you know, ten Draconian rules and you are now going to stick to those rules for the next 20 years. You know, specification is really -- it personifies the industry best practices that are at the forefront and they are, you know -- and it is just such a leadership position for the US government specifically to have taken.

So my recommendation would be to look at how you can do more things in that 800-63 vain. For those of you who don't know what 800-63, is it's around how authentication methods can be governed to give you greater and greater levels of assurance.

>> JEREMY GRANT: We're two weeks from legislation being introduced, the bipartisan bill in the house, called the digital identity act. It will be heard in the topic, that I

will be testifying at, if you want to have another couple of hours of virtual discussions.

It approaches to how the Better Identity Coalitions have talked about it. They are tuck in the paper and the plastic world. How can we come up with a model where anybody could ask an agency who issued them something in paper and plastic to vouch for them online?

And, you know that is a model around the identify of government validation services, that at least sitting here in Washington, DC, is you know, I think we're getting more buy-in into that concept as a way to bridge some of the gap between physical and digital. That then to the point that Pam made or, to the point that Patrick has made or Anne provides stronger evidence directly from the truth bureau, the authoritative source that issued it which can potentially take some of the doubt out, you know, involved with of the other tools that are out there.

Although, the role of government here, of course, then, you know, starts to raise questions around, well, what role is too much? And I actually want to jump ahead a little bit to my question and actually reach into some of the Q&A that's opened right now in the Zoom. Because we have got a couple of questions around privacy. You know, one person says is there some way you can stratify my identity information to make sure the supermarket may not get to know my mobile phone number just because I'm presenting a credential.

Mike Nelson talked about, you know, I would like to have a privacy enhancing identity service so I can verify maybe two or three of my attributes but not all of them.

What is the art of the possible with that these days and where is that going?

>> PAMELA DINGLE: I can jump in if that works for everyone.

>> JEREMY GRANT: In fact, I think I was going to point you to you first, the standard works that you are doing is

relevant, Pam.

>> PAMELA DINGLE: There's some interesting work. In some ways it's really innovative and in some ways it's very much building on standing on the shoulder of giants when it comes to this.

You know, this -- the best, most awesome option here, if you will, at this point, you know is what we would call selective disclosure, right? So when you talk about, you know, ideally what you could do is have a credential, for example, from your driver's bureau that contains your, you know, for example, your age of content and you should be able to prove to the supermarket that you are over the age of consent to buy a cigarette out disclosing all of the other pieces of information in your driver's license. That's the holy grail.

The digital equivalent, the way we do that is with cryptography, and the goal is to be able to cryptographically limit what gets disclosed. Now, there's obviously user experience challenges to that. Explaining, you know, having folks understand what they are disclosing and when they are not and then there are -- you know there is a zero knowledge proof. There are other ways to do selective disclosure. You can, for example, go back and get a new credential, right, get a credential that contains only the information necessary for this realtime transaction. Right? That's a perfectly valid way to do this too and that is a more historical way to have this happen. A lot of attribute exchange services work in this way as well.

But the promise of a zero knowledge proof is this idea that it can be ad hoc, right? That the supermarket does not have to have a relationship with your identity authority in order no be able to consume that super simple proof. And so that -- you know that would be my -- you know, the shining light that is on the horizon right now would be zero knowledge proofs.

>> JEREMY GRANT: From the perspective from the private

front?

>> PATRICK KINSEL: Interestingly, I worked at Microsoft for a number of years. In 2008, pre-Microsoft, I was the author of called the Internet users bill of rights and it was about exactly these issues. And then when I was at Microsoft, I worked with Facebook on what they called granular data provisions the idea that exactly like this, in their central repository, people could only access -- I believe that's absolutely where the Internet needs to get to and if it doesn't get there, at some point, I have a feeling that Pam will be very, very disappointed. I will as well.

It's absolutely in the future state. I think the challenge is how do we get there? And who are the organizations that have to adopt it to make that real? And I think that's where -- I don't know anywhere near as much as Pam but if there's not real engagement from the large institutions of the government, that won't happen. And if it doesn't flow through from the policies and all of this other stuff, there's no purpose to it.

I would say more broadly with the consumer privacy, I really, really hope that we make progress on that issue because I think it's important first and foremost and secondly, I think it's a hindrance to a lot of other regulatory innovation. I will tell you for us at the state level, the number one issue with advancing ours is that it becomes mired in a larger consumer privacy discussion and debate, but it's the same as the healthcare bill, and the same as the digital identity bill. It's the same conversation being inserted into what are our use case our industry specific issues. In California we comply -- you can comply when you know what they are. And I hope there's broader progress on privacy issues so issues can be delated in isolation.

I'm optimistic. There's a lot of debate and discussion that's happening but it touches everything.

>> JEREMY GRANT: And let me shift a bit in that, you know,

while there's plenty of other countries struggling with these issues, there are some that have blazed ahead. You know, it's -- whether you look at very different approaches between India, Estonia, Europe, Singapore, what do each of you think we can learn from other countries here in the US, and also what -- what do we want to replicate? What might a distinctly American approach to digital be like that's different from what we have today.

>> PATRICK KINSEL: I --

>> ANNE WALLWORK: I was just going to say that, I think unless I'm mistaken, and maybe things will change or have changed, and the pulse needs to be read again, but we do not have a central national digital or other identity system that's comprehensive in this country, and I don't think that we want one. But that -- that said, it gives us an advantage of having a very open marketplace in digital identity solutions where you may have government departments and agencies providing identity solutions, but also a really robust role for the private sector.

And I think that's a very good thing, in terms of security, cybersecurity, not having a central honeypot, protecting us against abuse, and the potential for abuse for inappropriate access that -- that could occur in some countries with national ID systems that could be used for surveillance or bias against vulnerable groups.

And I also think that our system will be technology neutral, that -- that zero knowledge proofs are really exciting and we need to work really aggressively together to resolve the -- I think to me personally, the tension between transparency and the illicit finance protections versus privacy and what we are seeing in terms of data localization in some countries, et cetera, that can be resolved. I don't think it's pie in the sky. It can be resolved by innovative technology and I think we can get there as soon as possible, and have the privacy authorities and -- and frankly advocates whether they are in the private sector or -- or government authorities and the financial sector integrity and efficiency officials and -- and interest groups really work together on that. And I would like to just note that the financial action task force is doing exactly that by reaching out to governmental privacy authorities and advocacy groups and bringing them into the digital identity work stream at the FATF, where the fundamental mission is, financial sector integrity.

>> JEREMY GRANT: Other perspectives on things from across the globe? Pam, I know you are engaged quite a bit globally in the standards space?

>> PAMELA DINGLE: Yeah, there are some great examples. There are good features and bad features of what lots of these places have gone through. I mean, I think the United States does not have the luxury of considering a monolithic approach. I don't think it's even possible.

And I'm -- I'm actually happy with that. I think that the best option here is to define domains of control that are, you know, legally and technologically separable but that have known standardized relationships between them. So you know, an example of this would be on the biometrics front, I saw some comments on the biometrics, right? There are reasons sometimes to do centralized biometrics and there's valid reasons, especially in government, for deduplication reasons for benefits.

The one thing I would suggest we not do is -- you know, I suggest we constrain that use to where it's appropriate, and look at where biometrics can be used in other use cases in a much different format. So, for example, in authentication, you know, the best practice in authentication is that your biometrics should not leave your device, right? Those biometrics should be locally stored and, that is a pattern that is important and no one pattern is correct. We just have to get the right patterns applied to the right part of our segmented world.

>> JEREMY GRANT: Thanks. And I will add the Estonian side, I mean I feel like this comes up time and time again in that the Estonians really have created -- if there's a platonic idea of what you could do with a national ID card that's sitting in a cave somewhere, it's certainly what the Estonians have done. I think as you point out, that's not a model that will work in the US. I often have noted Estonia is impressive. It's also a country with a population that's smaller than Fairfax County, that's just outside of the district.

I think a lot of times what is lost, a lot of what has motivated the very impressive investment in digital ID in Estonia, they were not a country for years while they were absorbed by the Soviets and so much of what they have invested in is also driven by this fear of this existential threat that remains immediately to their east in Russia and one day they might invade and they want to be able to reason a government in exile that you can only do digitally.

That's a fascinating set of motivators that are really different than what we deal with here in the US and, you know, I think as you start to pick those part, it makes clear some other types of solutions might be needed.

I wanted to pivot a little bit to the issue of inclusion and identity, which I think is rightfully getting much more attention in that it turns out it's not so hard to get an ID in the US in many cases. Where are their challenges? Where do some of our systems fall short? And what's the impact on those who might be excluded?

>> PATRICK KINSEL: I think a lot about this, and I think that there's a lot of issues. A think that -- we'll start with mortgage. Mortgage documents are generated in English. You have to take a picture of the front and back of a credential that has to pass a software-based forensic analysis. Not everyone has a camera sufficient to do those things.

People who speak foreign languages are subject of notorious fraud which is that people galvanizing as immigration attorneys and they are not. And so we force people through processes that they may not have the capacity, you know, if you think about a video session, you know, physical impairments, the equipment. You know, I can go on and on and on, right?

And yet, you know, the future that we are all creating here, you know, people are getting better service. They might be getting discounted pricing, right and those issues and that is not -- that's not cool. And so these are very, very real issues that we have to solve for. And I think, you know that's why your comment, Anne, about risk-based approach, and alternative means for validation, that's the world that we live in, right? A.

And so I don't know what the solution is there, but we're very diligently working on these issues.

>> ANNE WALLWORK: Well, I think you point to a couple of factors, one is that it's important that digital transition not result in further exclusion from either civil society or from financial healthcare or education. And we have seen that during the pandemic.

So I think that we need to have -- and I think the administration certainly does have and is trying to implement an expansive view of what critical infrastructure is for a digital world that includes access devices, and -- and programs to expand the Internet broadband, but they need to be really looked at very hard and funded appropriately.

I think another challenge is, you know, we talk about the digitalization of the financial sector, and move to eGovernment. But in this country, our foundational government issued identity starts with a birth certificate, and that is either -- that is, I believe, local registry, and other -- other sources of information are state level. Even the driver's licenses, the information that they get, it's, at this point as Jeremy notes, is documentary. You do have to come in in person. I think that may continue to be appropriate in terms of the higher levels of security that we need for under the real ID act and for certain kinds of regulated financial activities or accessing healthcare information, et cetera.

But, we don't pay much attention to digitalize and support the digitalization in a trustworthy way of those basic databases for verifying identity, and we really haven't to date, funded the transition in the states to mobile driver's licenses which I really do believe can be a game changer.

And we are seeing incremental moves, both by some states moving ahead to do that transition, and also by -- under the Dodd-Frank amendments, the requirement of the Social Security Administration open up an app for pinging against to -- in a privacy preserving, yes/no way to verify that a -- a person with a given name, address, and Social Security -- no, I guess it's name, date of birth and Social Security number exists but there's no credentialing that ties that data to an individual, that that individual or private sector identity solutions, et cetera, can leverage.

So I think we need to really value our federal system, but we need to look at how we need to help the components of it state, local, as well as federal departments and agencies move forward in a way with digitalization that is secure, and privacy preserving and safe as, again, a matter of national security infrastructure.

So --

>> JEREMY GRANT: Other perspectives on the inclusion side?

>> PAMELA DINGLE: There's so many angles to this. So, so many angles being right? There's the questions about our aging population, and how we can help our aging population. There's questions about, you know, access to technology at all, even having access to technology, like Anne talked about.

I think to look on the bright side of this and to look at the opportunities that we, have while still respecting that we can't leave people behind, I think is -- you know, we do have some really interesting opportunities, for example, you know, I mean the idea of user experience reform in a forms-based world is a pretty tough thing to talk about, right?

But if we can find a digital paradigm that will work for folks, we really do have the opportunity to iterate, right, to really study the user experience to be able to create trends, you know, of who is falling off? Like, you know, it's very difficult to know who doesn't finish a form, I think. I mean, not that I'm an expert here.

But, you know, it's much easier to know watt dropoff rates are digitally. So, I do hope that whatever we create, we then can apply all of this science and user experience, digital user experience to try to help those folks to have a greater experience online.

>> ANNE WALLWORK: Yeah, and I would also kind of add that programs whether they are private sector or government to identify identity gaps that are particularly pertinent to disadvantaged or vulnerable groups, and then help them get the access to the identity evidence that they currently need is very important for inclusion.

But so is a risk-based approach. And I would like to kind of -- kind of promote a reading of the FATF's digital identity guidelines -- guidance, rather, because I think it really lays it out for the lay reader how you can look at using digital identity solutions in the financial sector, for example, and -- and calibrate the level of, say, identity proofing or authentication both to the risk but also to the way -- to other ways of mitigating those risks.

So, for instance, the FATF recognizes that in low-risk situations, you may have simplified customer due diligence, and low risk situations can be created not just based on a customer profile, but also on limiting the functionality of a given financial product.

So if they have transaction number limits per, you know, in a given period or volume limits or value limits, you -- you may be able to have more flexible ways of identifying and using the attributes.

And I think that that guide -- the guidance also points out that, you know, there are different ways that governments in establishing what the processes and attributes for official identity are, can approach that. And if one is a very rules oriented, you must have this, this, this and you must, in terms of attributes you many have, that, that, that, in terms of evidence, that's challenging in a digital framework, in terms of leveraging evolving technologies.

And if you have regulatory frameworks that are risk-based and that are outcomes or principles based, for instance, the BSA says that a financial institution should have a reasonable belief that it knows who each of its customers is. That is an example of -- of a kind of outcomes and principled-based approach.

So, you know, I think -- I think that understanding and then leveraging the flexibility that could be there to promote financial inclusion is really important. It's an issue that we see a lot in our engagement with the development community, that still tends to see transparency and integrity controls, AML requirements, in opposition to financial inclusion; whereas, we certainly see them as mutually reinforcing. We are very interested, and the reason why I have financial innovation as part of my portfolio and look at it from an inclusion perspective, is because the more people we can bring into the regulated financial sector, the more those financial transactions are subject to not only AML/CFT projections but also consumer protections, and privacy protections.

So, I think that I would encourage everyone to think hard about what flexibility and ways of looking at different technologies in the regulatory contexts is.

And in that regard, I think it would be really very helpful if both the private sector and NIST could work on dynamic authentication, standards in the context of identity. You know, we see that in a very robust level being used for antifraud measures, where it's the financial institution's ox that gets gored, that's not being used for identity proofing at this point. I think we need to understand, you know, what level of trustworthiness and technologies deliver given levels of assurance with respect to dynamic authentication and then see how we can use that on the front end for onboarding customers in a way that addresses risk that is more inclusive.

Again, speaking personally.

>> JEREMY GRANT: And I will say on the inclusion side too, I think an issue that gets overlooked a lot is if you are poor, how hard it is to get an ID. If you have been recently evicted and, you know, your Social Security card and birth certificate were left in a soggy heap of a cardboard box on the side of the road, if you are fleeing a domestic abuse situation or you just got out of prison, you know, in fact -- Anne, you participated with Pastor Ben Roberts from Foundry Methodist Church, that is the ID ministry that focuses on charitable donations and volunteers helping people work through this process, because it's something that certainly in DC and most states as well, they don't have those services.

As we talk about going from physical to digital ID, perhaps based off of those foundational identity documents. We only have a couple minutes left. We have one more question that I wanted to ask. So for closing thoughts and, you know, maybe pivot into where we go next. There was a common thread here that says the US government will never have a single identity solution. So what are some of the reasons driving this conclusion? And then I would add to that as a closing question, what do we end up with instead?

So 30 seconds each person.

Pat, I will start with you.

>> PATRICK KINSEL: I mean, how do the roll out of enhanced driver's licenses go? We pushed that back how many years? How is the vaccine rollout going, you know, across the country in different states? I'm a fundamental believer in states rights. Notarizations are governed by the secretary of state. Everyone

has the right to impose their own policies on process. So the way that the organization market works is a good precursor. Every state has their own policy. There's reciprocity between states, and then what we're seeking now through a federal bill called the Secure Act is a minimal federal standard.

If you have a system, I think the other missing component is the audit component to ensure you meet the minimum standards. You can have multiple different players and they meet a minimum statement and they have reciprocity and interoperability and standards between systems and I think the other thing in my mind that's crucial is that the biometric or whatever it is, you know, the credential is stored on consumer's device and they have possession of it.

By the way, that's exactly how the iPhone works, it's not a cloud-based service. There are patterns out here to follow. Going back to answer -- you gave me 30 seconds. International. We need reciprocity between nations. The systems and rules we put in place. There are not credit systems in other countries how do you ask identity challenge questions? So this is a much larger issue. And there's model called NAP plus C it's out of the Hague. I can go on and on.

I think this is not a design challenge. This is an implementation and a buy-in challenge.

>> JEREMY GRANT: Next, Pam. 30 seconds.

>> PAMELA DINGLE: So I would say permeable boundaries. We absolutely have to have permeable boundaries. You need to identify people within domains and areas and you need ways to relate those areas together but you need rules to protect privacy between those areas.

Right?

So otherwise we end up in a world and we may inbound this world right now, where the people who were best qualified to correlate us are the ad tech people and, you know, we need to decide who should correlate and why, and then help everyone be successful in defining those rules and enforcing them.

>> JEREMY GRANT: Thanks. Anne. Wrap us up. 30 seconds.

>> ANNE WALLWORK: Okay. Well, I agree very much with what both Pam and Pat said. And I think in that regard, we need not only national standards, such as the NIST, but also mapping exercises between national standards that also can lead to global digital identity standards that support interoperable trust frameworks in different countries. And so the ISO-type of work, I think, needs to really be accelerated and linked to the digital identity workstream in the ISO, versus other very relevant work streams that you see the kind of siloing there in global technical standards of the sort that we have been that you canning about, we need to overcome in a regulatory and policy framework in each country.

So I think global standards and certification body is, such as FIDO alliance, for various types of elements are really important and most of all, I think public/private partnerships in this country are critical for driving the development of the infrastructure that we -- and then the solutions built on top of it, that both the private sector and government at all levels urgently, urgently needs.

>> JEREMY GRANT: Great. Thanks. We are a couple of minutes over time. I will just say thanks to all of you, Pam, Anne, Pat, thank you so much for taking the time. It's been a great discussion. And IGF USA, thanks for having us. And Dustin, let me hand things back to you. Thanks.

>> DUSTIN LOUP: Thanks, everyone, for putting a digital identity firmly in the IGF USA radar. I appreciate that, and so look forward to hopefully building on these conversations moving forward.

This is bringing us into our longer break of the day. So you all have until 2:45 to get lunch, network, do whatever you need to do, and we'll see you back after the break. Just a reminder that we do have the networking rooms open. So if you would like to chat with other attendees, then you can use the link that's in the chat. It's also in the agenda, but if not, we'll look forward to seeing you back for our discussion on 100% online how to close the Internet access gap once and for all after the break.