NEAL R. GROSS & CO., INC.

RPTS SHIPLE

HIF334020

IDENTITY VERIFICATION IN A POST-BREACH WORLD

THURSDAY, NOVEMBER 30, 2017

House of Representatives

Subcommittee on Oversight and Investigations

Committee on Energy and Commerce

Washington, D.C.

The subcommittee met, pursuant to call, at 10:15 a.m., in Room 2322 Rayburn House Office Building, Hon. Greg Walden [chairman of the subcommittee] presiding.

Members present: Representatives Walden (ex officio), Griffith, Brooks, Collins, Walberg, Costello, Carter, Schakowsky, Castor, Tonko, Clarke, Ruiz, and Pallone (ex officio).

Staff present: Jennifer Barblan, Chief Counsel, Oversight & Investigations; Samantha Bopp, Staff Assistant; Adam Fromm, Director of Outreach and Coalitions; Ali Fulling, Legislative Clerk, Oversight & Investigations, Digital Commerce and Consumer

Protection; Elena Hernandez, Press Secretary; Paul Jackson, Professional Staff, Digital Commerce and Consumer Protection; Bijan Koohmaraie, Counsel, Digital Commerce and Consumer Protection; Alex Miller, Video Production Aide and Press Assistant; John Ohly, Professional Staff, Oversight & Investigations; Hamlin Wade, Special Advisor, External Affairs; Jessica Wilkerson, Professional Staff, Oversight & Investigations; Greg Zerzan, Counsel, Digital Commerce and Consumer Protection; Julie Babayan, Minority Counsel; Jeff Carroll, Minority Staff Director; Chris Knauer, Minority Oversight Staff Director; Miles Lichtman, Minority Policy Analyst; Dino Papanastasiou, Minority GAO Detailee; and C.J. Young, Minority Press Secretary.

Mr. Griffith. We will go ahead and get started.

Welcome to this meeting of the O&I Subcommittee of Energy and Commerce. So that everybody knows, there are a lot of folks who are at another hearing downstairs and will be drifting in and out.

Also, I would like to take a point of personal privilege and recognize Allie Gilmer and Olivia Smoot who are here visiting today from my district at Auburn High School in Riner, Virginia.

They are too young to remember this but I started representing the Riner area in 1994 in the state legislature. So it's good to --

Ms. Castor. Do you want to stand up?

Mr. Griffith. Yes, stand up. Be recognized. Thank you.

Thank you again. Welcome. Glad you're here with us today.

That being said, let's get started with our business here today and other folks will join us as we go forward on this very important issue.

We are here today to talk about a very important topic, identity verification in a post-breach world. This hearing is especially timely, given several events that have taken place since the hearing itself was announced last week, including three newly-discovered data breaches that comprised an additional 58.7 million records as well as two major shopping days -- Black Friday and Cyber Monday.

With consumers rushing to take advantage of holiday sales

both in stores and online, the questions and challenges around modern identity verification become even more pressing.

Data breaches have been increasingly -- have been an increasing problem over the last several years. In fact, it is likely that everyone in this room has had their information included in a recent breach.

Between the 57 million accounts comprised in Uber's recent disclosed 2016 breach, the 145 million accounts compromised in Equifax's breach, or the 22 million accounts compromised in the OPM breach as well as many others, I would argue that it would be difficult to find an American whose information has not been compromised.

While these breaches themselves are troubling enough, they also raise a subtle more complicated series of questions and issues around the ways in which organizations including government agencies, banks, health care organizations, and retail companies perform identity verification of their citizens and their customers.

It is a well understood concept that, to quote the famous cartoon on the internet, nobody knows you're a dog when you're in the internet.

This anonymity has many advantages and it is important to many aspects of the modern internet.

However, as the global economy has become more and more digital and an increasing amount of commerce takes place online,

it also creates significant challenges for organizations attempting to ensure that they provide information and services only to authorized individuals.

Because these interactions usually take place on opposite ends of an internet connection with participants rarely if ever meeting face to face, the ability of organizations to remotely verify individuals has been a constant struggle.

As a result, for years many organizations have relied on a type of identity verification known as knowledge-based authentication, or KBA. We are all familiar with this process even if we don't quite know it.

For example, some online accounts ask consumers to provide answers to security questions such as their mother's maiden name, the make and model of their first car, or the street on which they grew up on.

Similarly, when consumers attempt to open new credit lines they are often asked a series of multiple choice questions that may ask who provided a consumer loan and in what year.

These are all examples of KBA. The effectiveness of KBA depends on a very important assumption -- that information such as birthdays, mothers' maiden names, addresses, work histories and other KBA attributes remain relatively secret.

In today's post-breach world, this is a tenuous assumption. Add the wealth of personal information consumers voluntarily share about their lives through social media and this assumption

appears almost laughable.

So what do we do? If modern commerce and many other services including government services rely on KBA for identity verification and that verification is no longer as secure or reliable as it was in the past, we need new strategies and new technologies to ensure that consumers are protected and economic growth continues and we need them quickly.

With the exponential growth of connected devices and services, it is likely that we will see more data breaches more often, not less.

Luckily, we are not starting from scratch. In the public sector, the National Institute for Standards in Technology -- NIST -- spent the past several years developing strategies and frameworks for identity verification under their Trusted Identities Group -- TIG.

As a part of this work, NIST's TIG has provided funding to pilot programs looking to develop, implement, and leverage innovative new technologies that move organizations beyond KBA.

Similarly, in the private sector, many companies and organizations from a wide variety of sectors have come together to create the Fast Identities Online, or FIDO, Alliance.

The FIDO Alliance provides a forum for collaboration and cooperation around the development of standards-based interoperable technologies. These standards are freely available and already deployed in the products of companies like

Google and PayPal.

Our witnesses today will not only help us understand the cumulative impact of the dozens of data breaches that have occurred in recent years go also assess how current practices can and should be improved to protect consumers and their information and how it's been breached.

Today's hearing is the start of what I expect will be a much longer conversation. But it's a necessary conversation to have as our world becomes ever more connected. Identity verification is a challenge that will only continue to grow.

Thank you, and I yield back and now recognize Ms. Castor of Florida for an opening statement.

Ms. Castor. Well, thank you, Mr. Chairman, and thank you for calling this hearing.

Mr. Chairman, data breaches are compromising the personal information of millions of Americans. The Equifax breach earlier this year, for example, exposed the personal information including names, Social Security numbers, birth dates, addresses, and other sensitive data of as many as 145 million Americans.

And there have been many more -- Yahoo, JPMorgan Chase, eBay, Uber. We simply cannot accept this as standard operating procedure. When companies like Equifax, Yahoo, and Uber fail to protect the vast information they collect about consumers, it poses very serious risks.

It's not limited to private corporations. Governmental

entities have also failed to adequately protect personal private data.

But with each data breach after each data breach, compromising more and more of consumers' personal information, we have got to ask how do we ensure an online identity can be verified only by the person in question.

I also think it's important that we not forget that companies should be held accountable when they fail to protect our data.

The Equifax breach exposed the personal information of nearly half of the American population and it could have been prevented by applying basic security standards.

So what is the recourse? What is the appropriate recourse? I know that experts are working to develop methods to better protect online identities and I would like to hear what your recommended solutions are.

Under President Obama, the White House released the National Strategy for Trusted Identities in Cyberspace. It's a framework for public and private collaboration on protecting digital identities and improving online transactions.

So building on that effort, companies have begun experimenting with ways to improve identity verification and authentication.

I would like to hear about some of these solutions as well as what we can do to protect consumers' privacy. As more and more of our lives are online, it is equally important that we ensure

that these systems are secure and that the ways in which we access these systems are protected.

I would like to thank our witnesses -- Mr. Jeremy Grant, Mr. Troy Hunt, Mr. Ed Mierzwinski -- for coming today to discuss the principles and various challenges in verifying online identities.

Each of you brings a wealth of knowledge and experience to this hearing and it's a pleasure to have you here today. Thank you, and I yield back.

Mr. Griffith. I thank the gentlelady.

I now recognize the chairman of the full committee, Mr. Walden of Oregon.

The Chairman. I thank the chairman, and we appreciate your leadership on this and so many other issues, and we want to thank the witnesses for being here today.

We have another hearing going on downstairs on the anniversary of the 21st Century Cures legislation so I am bouncing back and forth today.

Today's hearing is about the future of digital commerce, as we all know, and it's about the future of how we ensure the person on the other end of an online transaction is in fact the person they claim to be. What a concept.

For years, we have relied on user names, passwords, and knowledge-based questions to confirm a user's identity. It's not a particularly sophisticated process. Your mother's maiden name or the make and model of your first car aren't exactly reliable

forms of verification.

Regardless, this process was suitable for a period of time in the evolution of our connected world but that time has long since passed, as we all know.

As noted by one of our witnesses today, it was almost a decade ago that the 2008 Commission on Cybersecurity for the 44th presidency highlighted identity as a frequent attack vector for cyberattacks.

This prompted the previous administration to launch the National Strategy for Trusted Identities in Cyberspace, or NSTIC.

As we will hear today, this high-level federal attention encouraged the progress but we still have a long ways to go.

How far? Well, according to Verizon's annual data breach investigation report, about 80 percent of breaches last year used identity as a point of compromise -- 80 percent.

What has changed to make existing identity management practices so ineffectual and vulnerable to attack? There are a number of factors at play but the underlying answer is fairly simple.

Today, the information necessary to compromise identity is readily available to those who wish to find it. We live in a post-breach world. Just look at the massive breaches that have occurred over the last several from Target and Home Depot to Yahoo, Anthem OPM, Equifax and, most recently, Uber, to name a few.

I would be surprised if anyone in this room has not had at

least some portion of their personal details stolen in the last two years, let alone their digital lifetime.

I remember a former colleague from Michigan who chaired the Intelligence Committee, Mike Rogers, used to say there are two types of companies in America -- those that know they've been breached and those that don't.

It is not, however, just stolen data that undermines current identity verification practices. The explosion of social media is also a factor.

Every day, consumers voluntarily post, tweet, and share details about their lives, adding to the rich data set of information available to malicious actors.

One of our witnesses, Mr. Hunt, is a global expert on these issues and that's why your testimony is so very valuable to our work, especially on how bad actors can compromise identity through the collection of personal information and data that already exists in the digital universe.

He endured a 27-hour journey to be here, I am told, and I suspect his testimony will be illuminating for all of us. I thought I had a long trip back and forth to the West coast every week.

We can no longer ignore the current reality. Whether through theft or voluntary disclosure, our information is out there and this is not likely to change.

Social media will continue to grow. Social, cultural, and

economic benefits are just too great for it not to. Likewise, digital commerce and online transactions are integral to our economic prosperity both now and in the future.

As our lives become increasingly entwined in the digital -- with the digital space, this must come with an acceptance that our information will always be at risk.

Such is the nature of the cyber threat we face and there is no perfect security in the connected world. But that makes it even more important that we find ways to reduce vulnerabilities in our digital ecosystem.

Clearly, identity is one of those weaknesses. So therefore, I look forward to the work this committee is doing and the testimony you all have submitted to us and the policies that will develop, moving forward.

With that, Mr. Chairman, I yield back the balance of my time and, again, thank your witnesses for being here and, as I said, I've got a couple of these I have to bounce between. But we appreciate the work you're doing.

Mr. Griffith. Thank you, Mr. Chairman. I appreciate that.

I will tell you that Mr. Hunt not only sacrificed with the 27-hour flight to get here but also put on a suit and tie for us where he normally wears jeans and a black t-shirt, according, at least to his comments on the internet.

[Laughter.]

Mr. Griffith. But anyway --

The Chairman. I was starting to wonder if it's actually him or a stolen identity before that. But I don't know. Thank you.

Mr. Griffith. Anyway, thank you, Mr. Chairman.

At this point, I would ask -- oh, I would recognize Mr. Pallone of New Jersey for an opening statement. Glad you made it. Thank you.

Mr. Pallone. Thank you, Mr. Chairman.

I want to -- I have actually got the wrong statement here from the other committee.

Mr. Griffith. We will give you a minute. We have explained to everybody that we have two hearings going on at the same time and that folks are having to bounce back and forth so --

Mr. Pallone. All right.

So let me, again, thank you, Mr. Chairman.

So much of our lives today is linked to what we do online and companies in virtually every sector of the economy collect vast amounts of personal data about consumers, and these companies know they are targets for malicious attacks and all too often they fail to protect the valuable consumer information they collect and store.

For example, recently the ride service company Uber revealed that it had been hacked more than a year ago, and this breach reportedly exposed the personal information of 57 million riders and drivers.

This security breach is yet another example of a company that

failed to protect the data of its customers and then failed to come clean about their security breach, in this case for more than a year.

Then there was the Equifax data breach which compromised the personal data of more than 145 million Americans, and what's worse, the Equifax breach compromised personal data like Social Security numbers and birth dates that are difficult or impossible to change.

And consumers affected by the Equifax breach are vulnerable, particularly because these identity verifiers can give someone access to other sensitive information.

The committee is still waiting for answers to questions we asked Equifax both before and after our hearing on the breach and, obviously, that's unacceptable so, hopefully, we will get answers.

It's also unacceptable to the American people because when companies fail to protect consumer data consumers pay the price, sometimes years after a breach.

So as data breaches continue to compromise our personal information, it's important that we explore how consumers and the holders of consumer information can verify that individuals are who they say they are online.

For example, how many times has each of us been asked to provide the last four digits of our Social Security number to get access to other information?

But how do we protect consumers' digital identities, especially after the Equifax data breach exposed the Social Security numbers of nearly half the U.S. population.

And as companies suggest that they may move to behavioral and biometric verifiers, are we comfortable with how much more personal information will be collected and used?

Are we comfortable with trusting that companies will keep this data secure? And these are important questions now facing the world of digital commerce.

According to the Identity Theft Resource Center, as many as 1,190 data breaches have occurred so far this year. Any data breach exacerbates the issues the public is facing in verifying their identities and authenticating access online.

Hackers and other malicious actors erode the trust we have online by using the data they've been able to glean about each and every one of us, and that's not good for business and it's certainly not good for consumers.

So, again, I just want to thank our witnesses for being here today to discuss the latest in identity verification and the challenges of protecting people's data and I believe that unless we act and pass meaningful legislation we will continue to see more data breaches and the unfortunate ripple effects that result from them.

I don't know if -- you don't want to add anything? All right. I yield back, Mr. Chairman.

Mr. Griffith. Thank you very much for yielding back. I appreciate that, Ranking Member.

With that being said, I would now ask for unanimous consent that the members' written opening statements be made a part of the record. Without objection, they will be so entered.

I would now like to introduce our panel of witnesses for today's hearing and appreciate all of you being here.

First, we have Mr. Troy Hunt, the information security author and instructor for Pluralsight. Next is Mr. Jeremy Grant, who serves as the managing director of Technology Business Strategy at Venable. And finally, we have Mr. Ed Mierzwinski, who is the consumer program director at U.S. PIRG, or PIRG.

Thank you all for being here today and I look forward to your testimony and we appreciate you providing that testimony. We look forward to the opportunity to discuss identity verification with you all.

As you all are aware, the committee is holding an investigative hearing and when doing so it is the practice of this committee -- this subcommittee of taking that testimony under oath.

Do any of you have an objection to testifying under oath?

Seeing none, the chair then advises you that under the rules of the House and the rules of this committee, you are entitled to be accompanied by counsel.

Do any of you desire to be accompanied by counsel during your

testimony today?

Seeing no request for counsel, in that case would you please rise and raise your right hand, and I will swear you in.

[Witnesses were sworn.]

Seeing affirmative answers from all, you are now under oath and subject to the penalties set forth in Title 18 Section 1001 of the United States Code.

You may now give a five-minute summary of your written statement and we will begin with you, Mr. Hunt.

Thank you so much for being here. You have five minutes.

STATEMENTS OF TROY HUNT, INFORMATION SECURITY AUTHOR AND INSTRUCTOR, PLURALSIGHT; JEREMY A. GRANT, MANAGING DIRECTOR, TECHNOLOGY BUSINESS STRATEGY, VENABLE, LLP; ED MIERZWINSKI, CONSUMER PROGRAM DIRECTOR, U.S. PIRG

STATEMENT OF MR. HUNT

Mr. Hunt. Vice Chairman Griffith, Ms. Castor, and distinguished members of the House Energy and Commerce Committee, thank you for the opportunity to testify today.

My name is Troy Hunt. I am an independent information security author and instructor for Pluralsight. I am also the creator of data breach notification service known as Have I Been Pwned.

In my time running this service, I've analyzed hundreds of individual data breaches containing many billions of records and I've observed first hand both the alarming increase in incidents and, indeed, the impact they are having on people's lives.

This testimony draws on my experiences running the service and describes the challenges we are now facing in a time where data breaches have become the new normal.

When we talk about data breaches, we are really talking about a range of different types of events that can lead to the exposure of their personal information.

We typically think of malicious actors exploiting vulnerabilities and protected systems and, indeed, that's an

enormous prevalent and alarming situation.

But increasingly we also see data breaches occur as a result of simple human error. For example, accidentally publishing data to an unprotected publicly-facing server where it's then discovered by intended parties.

We have a perfect storm of factors that are causing both the frequency and scale of these incidents to accelerate. Cloud services have made it easier than ever to publish data publicly, and that has helped to drive the expansion of other online services, which have in turn increased the overall attack surface of the internet.

At the same time, we have the rapidly growing internet of things, collecting classes of data we simply never had digitized in the past and, increasingly, we are seeing that information appear in data breaches, too.

Organizational attitudes to our personal information lead to data maximization. That is a desire to collect as much of it as possible, often well beyond the scope of what is actually needed by the service it's being provided to.

Frequently, this is without informed consent, particular by the likes of data aggregators and, indeed, we have seen them suffer data breaches, too, both here in the U.S. and overseas.

Now, data is viewed as an asset yet organizations fail to recognize that it is also a liability. Exacerbating exposure of data is a rampant trading scene. Data is not only sold for profit

but regularly exchanged by individuals building personal collections.

I liken it to kids exchanging baseball cards, except that unlike trading a physical commodity, the exchange of data breaches is more like making a photocopy, as the original version still exists.

Once it enters circulation, it is impossible to contain it. The data breach genie is out of the bottle. We are also learning how much we don't know as significant data breaches that occurred years ago come to light.

We have no idea how many more unknown incidents are out there, and not only do we not know which organizations have lost their data and are unaware of it themselves, we don't know which ones are deliberately concealing data breaches.

There is a lack of accountability when a breach does occur. We know this because very little changes in the industry afterwards.

We constantly see large data breaches and people ask, will this be the watershed moment where we start taking these breaches more seriously.

Yet, nothing changes and we merely repeat the same discussion after the next incident. We are also disclosing large amounts of personal data of our own free will, such as our date of birth, by social media.

We think nothing of it because a growing proportion of the

population has never known a time where we didn't do this. They are the internet natives that have grown up in an environment of personal information sharing.

Consider the impact on knowledge-based authentication, the very premise that there is information that you know that is sufficient to prove your identity.

Mr. Griffith. All right. Mr. Hunt, I apologize to knocking you off but we have gotten word from our technical folks that the microphone is not close enough to your mouth and we need that.

I can hear you fine but apparently the folks recording this for later cannot. So --

Mr. Hunt. I will continue from here, a little bit closer.

Mr. Griffith. Thank you, sir.

Mr. Hunt. Consider the impact on knowledge-based authentication, the very premise that there is information that you know that is sufficient to prove your identity. That same information is increasingly public.

My dad recently had some help setting up a new broadband connection, and after calling up the provider the first thing they asked him was his date of birth. That's the same personal attribute I had exposed after I donated blood and that subsequently appeared in a data breach.

And that is really the challenge we have today, the premise of authenticating one's self with information that only they should know, yet is increasingly in the public domain.

That worked years ago when information was contained in a small number of silos but that's not the world we live in today. And consequently, our assumption about who knows what has to change accordingly in the age of the data breach.

Thank you very much.

[The prepared statement of Mr. Hunt follows:]

**********INSERT 1**********

Mr. Griffith. Thank you. I appreciate that, and now recognize Mr. Grant. Yes, got to turn on the mic.

Mr. Grant. Let's me try that again.

Mr. Griffith. There you go.

STATEMENT OF MR. GRANT

Mr. Grant. Good morning, Vice Chairman Griffith, Ms. Castor, members of the committee. Thank you for the opportunity to discuss identity with you today.

As background, I've worked for more than 20 years in both industry and government at the intersection of identity and cybersecurity.

In 2011, I was selected to lead the National Strategy for Trusted Identities in Cyberspace, or NSTIC, which was a White House initiative focused on improving security, privacy, choice, and innovation online for better approaches to digital identity.

In that role, I built out what is now the Trusted Identities Group at the National Institute of Standards and Technology and also served as NIST's senior executive advisory for identity management.

I left government in 2015 and now lead the Technology Business Strategy practice at Venable, a law firm with the country's leading privacy and cybersecurity practice, though I should note today my testimony represents my views alone.

So let me say up front I'm quite grateful to the committee for calling this hearing today. Identity is a topic that impacts every American but it's only recently that identity has started to get proper attention from policy makers in the U.S., and at a high level the way that we handle identity in America impacts

our security, our privacy, and our liberty.

From an economic standpoint, particularly as we start to move high-value transactions into the digital world, identity can be the great enabler, providing the foundation for digital transactions and online experiences that are more secure, more enjoyable for the user and, ideally, more respectful with their privacy.

When we don't get identity right we enable a great set of attack points for criminals and other adversaries looking to execute attacks in cyberspace and, unfortunately, we have not been doing very well here.

Last year, a whopping 81 percent of hacking attacks were executed by taking advantage of weak or stolen passwords. Eighty-one percent is an enormous number.

It means that it is an anomaly when a breach happens and identity does not provide the attack factors and, as my colleague, Troy, will probably discuss today with his website, Have I Been Pwned, there is now billions of compromised usernames and passwords that are out there in the marketplace. It is high time we find a way to kill the password.

Outside of passwords, we have seen adversaries go after massive datasets of Americans in large part so they have an easier time compromising the questions used in identity verification tools like KBA.

This was illustrated quite vividly by the 2015 hack of the

IRS' Get My Transcript application where more than 700,000 Americans had sensitive tax data compromised.

A key takeaway for this committee to understand today is that attackers have caught up with many of the first generation tools that we have used to protect and verify identity.

The recent Equifax breach might have driven this point home but the reality is that these tools have been vulnerable for quite some time.

There are many reasons for this and there is certainly blame to allocate. But the most important question at this point is what should government and industry do about it now.

As I lay out today, I believe the government is going to need to step up and play a bigger role to help address critical vulnerabilities in our digital identity fabric.

There are five primary areas where government, working together with the private sector, can help address the weaknesses of first generation identity verification and authentication tools and deliver next-generation solutions that are not only more secure but also better for privacy and consumer experiences.

First, when talking about the future of the Social Security number and whether it needs to be replaced, it is essential for folks to understand the difference between SSN's role as an identifier and its use as an authenticator.

SSN should no longer be used as authenticators but that does not mean we need to replace them as identifiers. Instead, let's

just try treating like the widely available numbers that they are.

That means that as a country we stop pretending that knowledge of somebody's Social Security number can actually be used to prove that they are who they claim to be.

Second, along with the SSN let's just recognize how useless passwords have become as a security tool. There is no such thing as a strong password in 2017 and we should stop trying to pretend otherwise.

Third, recognize that it's not all bad news out there. Government and industry have recognized the problem with old authenticators like passwords and SSNs and they've actually been working together the last few years to make strong authentication easier.

Multi stakeholder efforts like the FIDO Alliance, which Vice Chairman Griffith mentioned earlier, have developed standards for next-generation authentication that are now being embedded in most devices, operating systems, and browsers in a way that enhances security, privacy, and user experience. The government can play a role in helping to drive user adoption.

Fourth, while authentication is getting easier, identity proofing is getting harder as attackers have caught up to first-generation solutions like static KBA.

This might actually be the most impactful area where the government can help, by allowing consumers to ask agencies that already have their personal information and have validated it,

in many cases with an in-person process, to then vouch for them for -- with other parties that they seek to do business with.

The Social Security Administration and State Department and Motor Vehicles have the most to offer here, and this is actually a concept that was embraced in the 2016 report from the bipartisan Commission on Enhancing National cybersecurity.

Here, the federal government should work to develop a framework of standards and rules to make sure this is done in a secure privacy-enhancing way and look at funding work to get it started.

Finally, technology can help solve the problem but better standards will be needed for companies and agencies to apply it. Further investments in government research and standards work can go a long way toward making it easier for any party in the public or private sector to implement stronger identity solutions.

I appreciate the opportunity to testify today and look forward to answering your questions.

[The prepared statement of Mr. Grant follows:]

**********INSERT 2**********

Mr. Griffith. I thank the gentleman and now recognize Mr. Mierzwinski for five minutes.

STATEMENT OF MR. MIERZWINSKI

Mr. Mierzwinski. Thank you, Vice Chairman and Representative Castor and members of the committee.

The Equifax breach was an epic fail in a lot of different ways. I know that this full committee has held hearings on it.

Mr. Walden, the chairman of the full committee, used an excellent line when he said, "I can't fix stupid," when he was talking about Equifax's many problems.

I agree with the chairman on that but I want to point out a few other points about Equifax that may not have been pointed out in that hearing.

First of all, I think everybody sees them as a credit bureau, and that is true -- they are one of the big three credit bureaus that collect information and sell it for the purpose of employment and credit and insurance decisions.

They are gatekeepers to our financial and economic opportunity. So it's very important that they do a better job. In fact, that's their only job is buying and selling data. So you can't blame Target or even OPM the same way you can blame Equifax for their many, many epic fails in that -- in that debacle.

But I want to point out also -- and the Federal Trade Commission has issued several reports on this -- Equifax is not only a credit bureau. It is a data broker, and data brokers, unlike credit bureaus, are ubiquitous in society and they are

virtually unregulated and they buy and sell information every day that's very similar to credit reports but unregulated. So we need to take a look at the data broker system and figure out a way to regulate it more closely.

Second, I think we need to go back to first principles. Mr. Hunt referred to data maximization. The code of fair information practices says data minimization should be a goal and the code of fair information practices is embedded in a number of our laws, including the U.S. Privacy Act of 1974.

So we can't just protect all information. We've got to start collecting less information and keeping it for shorter periods of time.

We have already heard from several witnesses and members of the committee about the problem of SSNs as identifiers and authenticators.

But I want to point out that our credit reporting system, how we obtain credit in society, a bad guy doesn't try to get your credit report. That's very hard to do.

A bad guy gets your Social Security number and goes to a creditor, and a creditor, being a trusted partner to the credit bureaus, gets your credit report and gives credit to the imposter. That's a very flawed system that needs to be fixed.

The principal thing that I think Congress should do in response to Equifax, and I think it's bipartisan, is make credit freezes free.

Credit freezes are the best way to protect your identify from financial identity theft. But, unfortunately, they cost money in most states.

The problem of KBA authentication has already been discussed. I want to point out it's so obsolete it's pathetic and it also upset -- it's not only bad because imposters can do one-second searches on the internet and obtain answers to the questions.

Sometimes consumers don't know the answers to the questions. My colleague was asked how much credit her -- you know, her family member Chester had. Chester was her dog. He died years ago. She was five years old. Why is Chester a security question? What is the name of your first student loan company? Was it Sallie Mae or was it Navient? They keep changing the names of all of these companies. It's all ludicrous.

On multi factor identification, I think it's a real positive step. But I do want to point out that biometrics, the third general multi factor authentication -- something you know, something you have, and something you are -- privacy groups are very concerned about databases of biometric information posing privacy and civil liberties threats.

But on the other hand, if my fingerprint is only stored in my phone, perhaps that's a better solution. I'm very encouraged by the work that the other witnesses have talked about.

The FIDO Alliance and the NIST program have been open source

open standard multi stakeholder investigations of how to improve our privacy and authentication mechanisms.

On the other hand, I contrast that to the credit card PCS standards that have been imposed on merchants. The Target and the Home Depot, the Michael's, et cetera -- all the merchant breaches -- you can't blame the merchants for having to use an obsolete credit card with a magnetic stripe.

And now the -- now the first have gone to a chip card, which is a type of tokenization, and that is good but they could have gone further. They could have gone to chip and PIN. They could have gone to best available technology.

So we have made some progress but a lot more needs to be done. Thank you very much for the time.

[The prepared statement of Mr. Mierzwinski follows:]

**********INSERT 3**********

Mr. Griffith. Thank you. Appreciate that, and we will now begin the questioning and I will start with questions.

Mr. Hunt, in your testimony you talk about the exposure of data due to accidental misconfigurations of cloud services. You were certainly spot on.

One such misconfiguration was discovered in the federal government this week and it has been reported that this is the fifth time the government has suffered a similar accidental exposure this year.

Indeed, many companies, including Uber, have suffered information compromises because of these kinds of misconfigurations.

Why does this keep happening? Is it really that easy to accidentally share your cloud services with the world?

Mr. Hunt. Well, the easy answer to the last question is yes, it is that easy. It's very often just a simple misconfiguration, and the difference between, let's say, a storage account within Amazon being protected and needed credentials in order to access it and being wide open is literally one configuration that can take seconds to make.

So in terms of why it's that easy or how come this keeps happening so frequently, very often this is a competency problem. So people have access to resources such as cloud services that aren't sufficiently skilled in order to figure out how to configure them securely. Sometimes it can just be a simple

oversight and there's not enough backup controls to identify when something like this is exposed publicly.

It is also very difficult for organizations because when cloud services are used they tend to very frequently sit outside their known address base.

So, traditionally, an organization could say these are our IP addresses, this is the range of our scope of assets and then you can go onto the cloud and you can put things in totally outside that construct.

And then compounding that as well we have this -- this, I guess, construct called Shadow IT and for the longest time we have had the concern of Shadow IT -- people working outside the formal constructs of the way the IT department and organization should run.

And today, it is very simple for someone in an organization to go to the likes of Amazon and say, look, I would like a storage account -- I am going to publish data there, and the IT department never even knows about it.

So there's a number of factors leading to the prevalence of what is now becoming a very common event.

Mr. Griffith. Now, are any of the data breaches included in your service from such a misconfiguration?

Mr. Hunt. From which, sir?

Mr. Griffith. From -- from your service.

Mr. Hunt. Oh, from misconfiguration?

Mr. Griffith. Yes.

Mr. Hunt. Yes, many of them. So we are seeing many incidents. The perfect example that comes to mind, earlier this year we had an OIT device called a CloudPet.

It is literally a teddy bear with a listening device that talks to the internet. Their data was left publicly exposed in a database facing the worldwide web without a password. And, again, that is just a simple misconfiguration on their behalf.

Mr. Griffith. Wow. What can companies do to decrease the likelihood of this kind of a misconfiguration?

Mr. Hunt. It's a combination of things. To me, many of these incidents, whether it be misconfiguration or flaws in software, come back to education, and this is the sort of thing we are trying to do with Pluralsight.

Let's try and get education out there to the people that are building these systems and standing them up. Because so frequently it is just such a simple little thing and had the person understood what the ramifications of the configuration change they're making or the code change they're making was, it wouldn't have happened. So I would love to see more education.

Mr. Griffith. And what are the consequences? I mean, we can all think of some. But what are the consequences of companies exposing this kind of data?

Mr. Hunt. Really depends on the data. I mean, at the -- at the sort of the least end of the scale very often we are seeing

large amounts of email addresses and passwords.

Now, that then often becomes a skeleton key into other things because we know that people reuse their passwords.

So that -- I almost hesitate to say that's the best that could happen. But when we think about the worst that could happen, well, now we start to talk about large amounts of very personal data.

So we have been speaking about the impact of things like the Equifax incident. South Africa just recently had an incident which was data exposed as a backup on a publicly-facing server that had information about the entire country and this included their national identifier, so think about a Social Security number, which within there also includes date of birth and gender, and now we have got a whole country saying we literally had all of its data published on the internet and we know that it had been obtained by other unauthorized parties and redistributed.

But what do we do? And to me, that's sort of the worst case scenario because now you got a whole country saying, how are we going to do knowledge-based authentication when the knowledge about the whole country has gone public?

Mr. Griffith. Now, from what I understand, when folks go back and analyse many security instances like data breaches, they find that somewhere along the line someone in the organization chose convenience such as the ability to check their personal email from their work computer, for example, over security. Have

you found that to be true as well, in your work?

Mr. Hunt. Absolutely. I mean, the concern with convenience -- I will give you a really good analogy -- is very often I will say to people, look, we might see an application talking to a database that has effectively server admin rights -- the most privileged user you could possibly have -- and I will say to people, why would that happen. And they say, well, it was easy -- it was much easier to give access to everything than to start implementing fine-grained permissions. And they are right, it is much easier. But that then leads to the problems we have got here.

Mr. Griffith. And, sir, how do we make it easier to protect things -- protect that data?

Mr. Hunt. Well, again, I go back to that education side. This is people making mistakes unknowingly, and when we see these happen over and over again and we look at the behaviors of the individuals, very often it is because they've never been taught what are the ramifications of setting this configuration or writing code that way.

Mr. Griffith. Yes. I do think we all choose convenience from time to time when we know in our hearts we ought not.

With that, I have to yield back because my time is up and now recognize Ms. Castor of Florida for five minutes of questions.

Ms. Castor. Well, thank you, Mr. Chairman.

As the Equifax breach made all too clear, there's an

astounding amount of data that is collected by companies and especially credit bureaus.

The Equifax breach, for example, exposed the personal information including names, Social Security numbers, birth dates, addresses, other sensitive data of almost 150 million Americans.

Mr. Grant, if this data is out there, should companies no longer use this information as a component of identity verification online?

Mr. Grant. I wouldn't say that they shouldn't use the information anymore but they should be smart about the ways in which they use it and I think there needs to be a recognition, you know, across government and industry that these first-generation systems that we were using the attackers have caught up with them.

So let's figure out where it can be valuable in a process to establish identity or authenticate identity and where it can't be. I think there are still tools that are out there that are using some of this data that could be -- you know, I often talk about, you know, you have an arrow with multiple quivers in terms of, you know, the tools that you're using.

There still may be some value. But I think we need to recognize that it is been greatly diminished and we need to focus on next-generation solutions.

Ms. Castor. So, Mr. Mierzwinski, a similar question. In

your testimony, you stated in reference to Social Security numbers that, quote, "you cannot authenticate with a number that is also an identifier," especially one that anyone can obtain, thanks to the data breach world that we live in.

This seems like a good reason to prevent companies from using the Social Security number as an authenticator. Is that right?

Mr. Mierzwinski. Well, I think you're absolutely right, Congresswoman, and many people don't know that the Social Security number was invented so long ago it doesn't even have a correct check sum number.

When you type your credit card number and make a mistake in an online form, it knows instantly. Your Social Security number can be completely garbled and it wouldn't know.

The first five digits actually aren't really about you. They're about when you were born and where you got your number more than unique. So it is a very big mistake.

I am encouraged that some of my banks know that when I've logged on from a new machine or even a new place. But others of my banks and other companies that I do business with don't ask me extra questions or don't want to send me a text.

So it is uneven how companies are doing better authentication and, to me, you have also got to penalize them when they make a mistake.

I realize Equifax and other firms will be penalized by the market. However, I wonder whether regulators need more authority

to penalize companies that lose our info.

Ms. Castor. So let's talk about that especially. You mentioned the data brokers. Even outside of data breaches, internet-connected datasets contained vast information.

A University of North Carolina study showed that data brokers can obtain almost anything from demographic data to financial data to travel data.

In your opinion, are there adequate safeguards in place to limit what information data brokers collect, store, and sell about us? It seemed in your testimony you said no, it is kind of the --

Mr. Mierzwinski. No, despite -- and you can find many items on the record from me criticizing the credit bureaus and the Fair Credit Reporting Act for being too weak. It actually is one of our stronger privacy laws. There are virtually no laws that apply to data brokers and they are out there in a Wild West ecosystem of digital collection and selling of information about consumers in real time, and as I believe the vice chairman pointed out in his opening statement, a lot more information is being collected into their databases.

Your locational information is, for one, a new piece that should be protected that isn't protected under many laws.

Ms. Castor. So are there any incentives currently in place for companies to minimize the data they collect and store?

Mr. Mierzwinski. Unfortunately, I don't know that there are

enough and there -- public shaming helps but regulatory accountability would help even more, and companies just feel that we are not their customers.

Consumers are not Equifax's customer. Mr. Smith, the ex-CEO, said that before numerous committees over the last month. Business is their customer. We are their product. We need to get them to think about taking care of us, and they haven't.

Ms. Castor. Mr. Grant, thank you for all of your work on the National Strategy for Trusted Identities. The identity ecosystem adheres to fair information practice principles, one of which is data minimization.

This is the idea that organizations should collect only information that is directly relevant and necessary to accomplish the specified purpose. Is that right?

Mr. Grant. Yes.

Ms. Castor. So now it seemed to me, in this day and age, companies want to know everything about you. I am going to ask you the same question. What incentives are currently in place for companies to minimize the data they collect and store?

Mr. Grant. Well, I will say concerns both about regulatory enforcement as well as liability that they might face by having too much data.

You know, Mr. Hunt talked before about data maximization. When I was running the NSTIC program there was a term one of our staffers coined, which was data promiscuity -- the practice that,

you know, companies are just quite open in terms of collecting and sharing gobs of data.

And I do think one thing you're starting to see now, particularly when some of that data is exposed in a massive breach, is other companies take a look at it and say, do we actually want to have all of this data.

And so, you know, now that I am in the private sector I spend a lot of time working with companies, advising companies on how to minimize their risk, and I would say there are some companies that still want to hoard data and there are some that are realizing that it might be a liability and are actually trying to put proactive measures in place to reduce the footprint of data that they have on their customers and really focus only on what they need.

So I do think a mix of regulation and liability does have an impact in the marketplace. You know, certainly, if you look across the ocean to what's happening in Europe right now with the impending implementation of Europe's general data protection regulation -- GDPR -- there's a lot of companies here in the U.S. that are still going to be impacted by that and that's also causing some firms to wake up and reevaluate in some cases what data they collect, how they store it, how they use it.

Ms. Castor. Thank you.

Mr. Griffith. I thank the gentlelady for yielding back.

Now recognize the gentleman from New York, Mr. Collins, for

five minutes of questions.

Mr. Collins. Thank you, Mr. Chairman.

And Mr. Hunt, I guess it is 3:00 a.m. right now so I am hoping you got some sleep on the flight coming up from Down Under.

I want to try to put today's hearing maybe in context just for the everyday person. So many of us -- you know, every three months one of our credit cards is accessed in some way. Usually we find out because we get a notification -- a fraud alert from American Express or Master Card. They've actually got some algorithm somewhere that says, this looks unusual, or something.

So I want to make sure I understand. That's a little -- people doing that, grabbing our credit report and stealing our numbers is perhaps different than the data breach area, or not?

Mr. Hunt. Where it probably differs to credit cards is there are a lot of different places where credit cards are exposed which may not be as a result of a data breach.

I've had my wife's card compromised several different times now and, as you say, you hear from American Express --

Mr. Collins. Because I am sure she uses it daily.

[Laughter.]

Mr. Hunt. Well, she does appear to use it regularly, evidently. When this happens, she will, as you say, get fraud alerts from the bank.

Now, that could have been anything from -- we might have been in a taxi in a particular location and they scribbled down the

number when they had physical access to it. You give it to someone at a restaurant -- that guy behind the counter. It could have happened in an incident like that. It could have been that a single merchant resold the data after purchasing something online.

Now, that's not necessarily the same as someone who was a malicious party came along, found a vulnerability in software, and sucked out a million different records in one go.

Mr. Collins. Yes. So I wanted to kind of make -- because I think sometimes we confuse the two and I think most of us are impacted by somebody grabbing our credit card more than not.

Then we got to go to the inconvenience -- getting a new card, set up on autopay. You know, I probably have to do that three, four times a year even.

So here we are talking about data breach. So now it begs the question, when someone is getting that, and I certainly understand someone, if they had enough, could try to apply for, I don't know, a mortgage, a something.

But that probably doesn't impact too many Americans as much as somebody stealing their credit cards.

So it kind of begs the question, these data brokers, as we call them -- it sounds like a business because there's guys -- and it sounds like they're -- are they continuing to try to fill out, you know, for, you know, myself, you know, there's people with my same name, so I don't know.

Are they sorting by my last name? My first name? My middle initial? As they find out that I, you know, just went to the SPCA and got a new cat, you know, what's the cat's name.

You know, how are they sorting this? By Social Security number? By address, in multiple ways, and as you said, trading baseball cards -- are they doing this for fun? And then once they have it, and they're just out there selling it, why can't we catch these guys?

If somebody -- I think of Raymond Reddington on "The Black List," you know. He'd be the guy buying this stuff. Why can't we find them, shut them down? And so that kind of general questions. What would you add to that?

Mr. Hunt. I would say one point to maybe sort of disambiguify here is when I made the comment about trading baseball cards what I am talking about is there are a lot of individuals out there who obtain access to data breaches and then they redistribute them between peers -- not necessarily commercial legal entities like data brokers such as Equifax but individuals, in many cases children, sitting in their bedroom going, hey, I've got a data breach -- you have got this one -- let's swap and we'll build up these personal collections.

Now, that is not necessarily with malicious intent but it does lead to the redistribution and the growth of the amount of data that's out there.

And then in terms of the data brokers, in terms of the legally

operating entities, very often they refer to data enrichment, which is like let's just get as much data as we can about the individuals, refine it so that we have very, very clear pictures because that makes the product that they offer that much more valuable.

And then whether they saw it by your Social Security number or your name or your job title, whatever it may be, that got significant amounts of data that they can offer people, whatever sort of sorting or filtering mechanism they like.

Mr. Collins. So in this case, you're referring to a data broker as a legal entity --

Mr. Hunt. Correct.

Mr. Collins. -- not a blacklister that's out there selling it?

Mr. Hunt. That's right.

Mr. Collins. All right. So the folks that are out there selling it on the darknet or whatever, just walk us through -- we don't have a lot of time -- how are they finding their customers, verifying it is not an FBI or somebody under cover?

Mr. Hunt. Well, they don't always get that right.

[Laughter.]

So how are they selling it? Well, very often we see data breaches being traded on the same sorts of marketplaces that are trading things like drugs.

So we have seeing very prominent darkweb websites -- the Silk

Road, Hansa Market, AlphaBay. Now, many of those services have now been shut down but others have emerged in their place and they operate on Tor hidden services on the darkweb, which does make it very difficult many times to actually track them down. So they operate illegal marketplaces and data breaches are another commodity like heroin.

Mr. Collins. Well, I appreciate all your comments. My time is up. I yield back, and thank you for coming up from Australia.

Mr. Griffith. I thank the gentleman for yielding back.

I now recognize Mr. Tonko of New York for five minutes for questions.

Mr. Tonko. Thank you, Mr. Chair.

In recent years, as breaches have become more common, companies and technology have not kept pace to protect consumers. As more breaches occur, more consumers are at risk for identity theft and other crimes.

While progress has been made, we must do much more to, obviously, protect consumers. Many ongoing concerns were brought to the forefront once again with the Equifax breach. More than 8 million New Yorkers were affected by the Equifax breach including many of my constituents.

One constituent, who I will label as Lee from Albany, asked Equifax, why are you using this gross misconduct to turn your victims into customers for a paid monitoring service that you will profit from.

Mr. Mierzwinski, can you speak to Lee's concerns that companies are profiting off these breaches?

Mr. Mierzwinski. We think it is outrageous and we wish it would stop. The companies have turned consumers into cash cows.

They're responsible for keeping our information safe and keeping it accurate. They don't, and so instead they say, you better buy this credit monitoring service at $19.95 a month, and the marketing of these services is extremely deceptive. Several banks have been fined by the bureau and several of the credit bureaus have been fined by the FTC.

A third party company, Lifelock, has been fined by the FTC and numerous state attorneys general. After it violated the terms of its settlement order, it was fined an additional $100 million for contempt.

So the marketing of credit monitoring is unfair, and you don't need credit monitoring either because you can get your credit report for free under federal law. In seven states, you can get a second credit report for free from each of the three companies.

If you file a fraud alert -- a 90-day fraud alert -- after you have been a victim of a breach, you could get an additional free credit report, get them every three months, and you have got your own free credit monitoring.

But Equifax should not be profiting. We'd like to put a stop to it and we'd like them to not charge consumers for freezing.

Mr. Tonko. Thank you.

And Mr. Mierzwinski, again, you discussed the privacy risks that come along with biometrics. Can you elaborate on these risks?

Mr. Mierzwinski. Well, very simply, I think that as we put our biometric information into databases, it becomes another commodity in the cloud.

It becomes another way that you can steal information about a consumer, if you steal my fingerprints or my retina scan, it's -- you could clone yourself as me in a lot of different ways.

I am not an expert on whether that is being done yet today, but we are very concerned and also concerned about the civil liberties aspects of government agencies getting access to the information in the databases without warrants, et cetera.

Mr. Tonko. Mm-hmm. I thank you for that.

And a 2017 New York Times article described the nightmare that Americans face when confronted with identity theft. The article referenced a study on identity theft and pointed out that, and I quote, "Last year, 15.4 million American victims of identity theft lost $16 billion."

The article continues, describing cases where Americans were denied the ability to refinance their mortgages or tax refunds were fraudulently sent to hackers and other similar cases.

So Mr. Mierzwinski, many companies use certain information to verify someone's identity like a full name, home address, and

Social Security number. Now with the data for nearly half of Americans stolen, is it true that malicious actors could retrieve those identifiers?

Mr. Mierzwinski. Absolutely malicious actors can retrieve your information in a variety of ways. They can even retrieve more information if they've only obtained some.

So the Yahoo breach largely obtained for the bad guys phone numbers and email addresses. That's the way that you can then conduct phishing and spear phishing exploits to get more information from consumers or even call them on the phone and say, "I've got your Social Security number. I am going to read part of it to you. You read the rest of it to me" -- those kinds of gimmicks -- social engineering. It is easier than hacking, actually.

Mr. Tonko. Mm-hmm. The article also makes the case that we shouldn't necessarily get rid of using Social Security numbers to identify someone but that we should stop using it as an authenticating factor.

Mr. Grant, do you agree with that?

Mr. Grant. Yes. I wrote an op-ed that was published in The Hill about a month ago that made that same point. I think we need to understand how Social Security numbers are both an identifier and an authenticator and essentially stop recognizing them for use of the latter. If I call my credit card company and they ask for the last four of my Social Security number, my answer should

be, "Why in the world would you think that me knowing that actually proves that I am me?" My information has been stolen several times over. It could be anybody who's calling in making that claim.

But as an identifier, look, identifiers are needed in the modern economy. The government needs a way to track how much money I am making from both my job and my bank accounts. You know, individual companies need an identifier as well.

Let's just treat it as something that's widely available and I think once we acknowledge that it is not something that is a secret, then we can start to focus on what comes next, which are better solutions for identity verification, better solutions for authentication that don't have the weaknesses that the ones that we are using today have.

Mr. Tonko. Thank you.

And with that, I yield back, Mr. Chair.

Mr. Griffith. I thank the gentleman, and now recognize Mr. Costello of Pennsylvania for five minutes for questioning.

Mr. Costello. Thank you, Mr. Chairman. I am going to try this with my voice.

To all three of you, I am just going to read through a series of questions and ask that you weigh in as appropriate.

You talked -- you spoke in your testimony about the role of Social Security numbers both as they are used now and as they should be used in the future.

In particular, you're both adamant about the need that we

don't need to replace Social Security numbers as some have suggested we need to.

Instead, you have said that using them or the need to change them from using them as identifiers and authenticators to using them solely as identifiers.

My questions are oriented in this fashion. Are there barriers to moving away from Social Security numbers as both identifiers and authenticators? For example, are there government regulations that require them in certain instances?

Are there private sector standards that recommend or require their collection? And how will these organizations begin making the change you suggested?

How expensive both in terms of time and resources would this change be and are there any potential down sides, and if so, what are they?

Mr. Grant. So I am happy to jump in with that first.

I think one point you raised is there are a lot of entities that are required to collect my Social Security number.

I started a new job at Venable five months ago. They needed to know my SSN. Any bank account that I open they need to know my SSN. And that's for the purpose of an identifier and I don't know that there are any real issues there with them continuing to use that.

There are issues that are out there in terms of, you know, particularly when opening financial accounts. I mean, one big

problem we have in this country is what, you know, many people refer to as synthetic identity fraud -- when you'll see fraudsters try and combine a real name and a real Social Security number that don't match and then start throwing it into the system in an attempt to establish credit, and that's, you know, one way that, you know, organizations are then defrauded or people are defrauded.

I mean, so, you know, I think there's good reasons to keep using the SSN as an identifier but we could also use better systems to verify.

One of the things I talked about in my opening statement was what government could actually do as a provider of identity verification services themselves.

The Social Security Administration knows that there's a Jeremy Grant that has my Social Security number that matches but if I go to open a new account at a bank today or a mobile network operator or anybody else who's collecting it, there's no way to electronically verify that with Social Security that that really matches up.

There's a paper-based system that requires a wet signature. It was a great thing 20 years ago. It is 2017 now. I think you could actually help cut down on fraud in new account opening if there was an electronic way for Social Security to validate those numbers if queried.

I think where there's going to be bigger issues -- you were

asking about barriers and costs and things like that -- is where we replace the Social Security numbers and authenticator.

So I can make fun of the credit card company I called last week who asked for the last four of my Social Security number and, obviously, there's no security value to that in 2017.

But their next question is, well, then how do I authenticate you when I am talking to you on the phone, and that's a much harder question. I think there's some interesting products. There's new standards that are emerging. There's -- there are ways that you can do it. But there tends to be -- the pace of adoption tends to lag the creation of new technology.

And so I think this is actually an area where I would love to see government partnering with industry focus more is how can we identify where those are -- where there are promising technologies that could replace the first-generation tools that have, you know, started to fail and accelerate the pace of adoption everyplace.

Mr. Mierzwinski. I agree.

Mr. Costello. That's a good answer.

Mr. Mierzwinski. Yes. Try to keep some of your time for you.

Mr. Costello. Very good. I will yield back, Mr. Chair.

Mr. Griffith. I thank the gentleman for yielding back.

I now recognize Ms. Clarke of New York for five minutes for questions.

Ms. Clarke. I thank you, Mr. Chairman. I thank our ranking member. I thank our panellists for their expert testimony here today.

And I wanted to bring up the national strategy for trusted identities in cyberspace. Under President Obama, the White House released this strategy and this spurred the public and private sectors to collaborate on issues related to identities and online transactions.

Mr. Grant, is it accurate that this strategy laid the framework for privacy-enhancing technology as well as identity solutions that must be secure and cost effective?

Mr. Grant. Well, I would say it helped. I think where NSTIC really helped was throwing down a marker in 2011 for an industry that, you know, hadn't really started to think about this yet, and when I look at the impact several years later, you know -- I talked about this in my written statement -- companies that liked it came in and said, hey, this is a great idea -- how can we actually work with you to come up with solutions that align with it.

Even companies that didn't like the fact that the government had thrown down a marker still had to pay attention to it because their customers were focussing on it.

So when I look at where the market is today, look, we still have plenty of problems in the identity space. We wouldn't be having this hearing if it wasn't the case. But I think the strategy helped and some of the specific activities that we --

that we sponsored and funded out of NIST during the time that there was a national program office implementing NSTIC really helped to move the market along at a point much faster than it would have gone otherwise and, you know, also pointed the way to, you know, create the -- you know, just pointing out basic things like security doesn't have to be at odds with privacy.

Security doesn't have to be at odds with user experience. Those are concepts -- it is not a radical statement to make but there were some vendors in the space who seemed to think that they were going to be at odds and this helped -- helped to show that there could be other ways.

Ms. Clarke. So what -- can you elaborate a little bit more as to what a privacy-enhancing solution may look like in the age of data breaches?

Mr. Grant. Sure. So, you know, the concept of privacy enhancing it is, you know, how does -- how do you create solutions that can actually give people more control over their personal information -- have more choice in terms of what attributes they choose to share about themselves when they go online.

And, you know, it is a catch-all term. But in terms of practical application, I think it is, you know, something you see today. Let's say you're logging in to a website with a social provider and they now give you radio buttons that, you know, let you choose -- do I just share my name?

Do I log in anonymously or do I share -- let's say it is using

Facebook Connect -- a whole bunch of information about me with that site. That's, you know, one example of giving consumers choice in a way that's also pretty easy to select, you know, with radio buttons, for example, that you can click on or off. That is something that we didn't have in the marketplace before.

I think there's other interesting approaches. You know, people can get -- we could really go down the rabbit hole in terms of talking about privacy-enhancing encryption, which is an area that I will say there's been a ton of R&D done but I would say we still have barriers in the marketplace in terms of coming up with systems that can scale.

I know there's really a commercial -- a need for. We, you know, funded a lot of research there as well and NIST continues to do good work there today. That's probably some of the next generation work, I think, in terms of where the market focus is next.

Ms. Clarke. So can you tell us the benefits of a universal two-factor authentication or similar types of technologies that secure a user's identity?

Mr. Grant. Well, it is a universal two factor. Whether it is universal or whether you're just using two-factor authentication everywhere. You know, I mentioned in my opening statement 81 percent of breaches last year were caused by exploiting passwords.

There is a reason for that. The password is really easy to

compromise and the notion that there's such a thing as a secure password just doesn't make sense. You know, a lot of the attacks we see these days are speak phishing attacks where you get something that looks like a normal login to your email provider or your bank but it is not. It is somebody who's inside trying to phish your user name and password.

If you have unphishable two-factor authentication behind it, that attack doesn't work anymore. Although one problem we are actually seeing in the marketplace is some of the first-generation tools that we have seen for two-factor authentication -- things like getting a code through SMS or, you know, through an app on your phone.

That is phishable as well. And so, you know, I keep making the point we had solutions that were good for a while and now the attackers have caught up with them.

Moving to unphishable authentication -- you know, we have talked in this hearing about, you know, standards bodies like the FIDO Alliance that are coming up with solutions based on public key crypto, which is unphishable. That, I think, is where, you know, we need to focus there.

Ms. Clarke. Where we need to go. Okay.

And just sort of in closing, you know, I am glad that we somewhat have a roadmap to improve the security of our online identities but it seems that more efforts are needed to implement these effective solutions and we need to continue to evolve, as

you have stated, because we sort of get static after a while and, of course, there are those who are out there constantly working at how to phish and break through.

So thank you for your response today. Hopefully, we will heed what you have shared with us today.

I yield back, Mr. Chairman.

Mr. Griffith. I thank the gentlelady for yielding back.

I now recognize Mr. Walberg of Michigan for five minutes of questions.

Mr. Walberg. Thank you, Mr. Chairman, and thanks to the panel for being here.

Mr. Hunt, I appreciate you coming all that distance. In fact, I've often had some sinister thoughts of sending some of these hackers, et cetera, back to Darwin, Australia, and let them confront some of the wildlife there in that beautiful but dangerous part of your great country. But I won't suggest that.

One of the reasons that we are having this hearing today is to shine a light on a problem that we think is getting worse, namely, that there is so much data available on individuals from these various breaches that malicious actors can package or enrich data to create very robust profiles of almost any given person.

Is that something that you have seen or heard about and if so is it a growing problem?

Mr. Hunt. Yes. Look, it is certainly a concerning thing because, obviously, the more personal attributes you can gather

about an individual the richer the picture you have.

And then when it then comes to things like knowledge-based authentication you start to build up many different attributes. And in my written testimony I talk about the concern of aggregating from multiple services, and they're not always data breaches either.

So someone might take certain attributes from one data breach -- let's say a name and a birth date. They'll go to another data breach and they may get gender and home address.

And then they'll go to open source intelligence sources such as LinkedIn, Facebook, Twitter, and aggregate further data attributes from there -- your profile photo, your social connections. And the real concern I have there is that even beyond just data breaches alone there are so many sources of information that we literally willing publish ourselves publicly that we now have to start to work on this assumption that so many known attributes about ourselves, which we did previously consider to be personal attributes, are now public and that's the concern I have. There's just so many different sources and it is not just data breaches.

Mr. Walberg. And that's what makes it so valuable then, that --

Mr. Hunt. Oh, absolutely, and I can see why the likes of legally operating data aggregators are running great businesses these days because there is so much data that they can obtain from

us.

Mr. Walberg. Yes.

Mr. Grant, as former head of NSTIC, is -- this is likely an issue that you're familiar with as well. Did NSTIC look at this kind of problem and, if so, what were its conclusions and recommendations?

Mr. Grant. So I would say we spend a lot of time looking at it in the Trusted Identities Group and NIST continues to focus on this.

You know, I think probably the most -- well, there's a lot of things that NIST has done in this space that's been Impactful.

But one that I would point to are the updated digital identity guidelines. One of the NIST special publications, 800-63-3, is the title or the code that was put out this past summer, which was an effort led by my old office to basically take a look at what is the modern state of solutions in terms of what we can use for identity verification and authentication in the marketplace and also recognize where some of the attackers have caught up with some of the old technologies.

And so they published new guidance this past summer which I think -- you know, what's been nice about it is not just in government but also a number of entities in industry have looked at this and said, this is fantastic -- this is a guidebook that we can use as we are building solutions for the private sector to make sure that we are, you know, both taking into account new

technologies and new standards that are emerging -- things like FIDO as well as make sure that we are not using some of the legacy solutions that just aren't as good anymore.

So, you know, certainly, in the topic of identity verification, one of the things that the new guidelines did was diminish the role of KBA in terms of how much you can trust it for identity proofing.

It establishes that there's still a role for it in the process of identity resolution, you know, trying to figure out whether I am the Jeremy Grant who's actually applying for an account but says you cannot use it alone for, you know, full-blown identity verification. That was a big change from what we've seen in the past.

So, you know, one thing I mentioned in my written testimony some of the budget for NIST work in this area has been proposed for a cut in 2018 at a time when everybody's looking at, you know, where we can actually take some actions after events like the Equifax breach. I think we, you know, are going to continue to need more funding for research and standards in this area, both to help government implement better solutions as well as the private sector.

Mr. Walberg. What updated standards are you talking about there?

Mr. Grant. There is updated -- well, I think there's other work to be done still. So I think NIST has put out digital

identity guidelines.

I would say two things. One, attackers are always evolving and technology is always evolving and so it is something that should be updated I would say, you know, on a regular basis rather than, you know, a cycle that's every five or 10 years, which is often how NIST tackles the special publications.

Beyond that, I think there's other research for areas. You know, for example, one of the questions that Mr. Hunt was asked before was about the security of cloud services and how entities are getting into that.

And often, again, the attack vector there when you're guarding against big enterprise class data breaches is through identity.

I think NIST could do a lot more work looking at enterprise identity and how you actually manage administration, authentication, authorization, analytics, and audit -- what I call the five A's of the identity life cycle.

There is not great guidance out there anywhere in the world and NIST is really well poised to help enterprises apply better identity security.

Mr. Walberg. Thank you. My time has expired.

I yield back.

Mr. Griffith. I thank the gentleman for yielding back and now recognize Representative Jan Schakowsky of Illinois. The gentlelady is recognized for five minutes.

Ms. Schakowsky. Thank you so much.

As we talk about consumer protection, which has really kind of been my bailiwick for a very long time, I have to mention what's going on right now at the Consumer Financial Protection Bureau.

OMB Director Mick Mulvaney is serving now as acting director as his appointment continues to be challenged in the -- in the courts and Mr. Mulvaney has been pretty much a longtime opponent of the CFPB and no friend of consumer protection regulations.

He has already put a hiring freeze and a regulatory freeze in place at the agency. So Mr. Mierzwinski, I wondered if you could just share your thoughts on what is currently going on at the CFPB and perhaps how it relates now to this issue also of data protection, et cetera.

Mr. Mierzwinski. Well, thank you, Congresswoman, and of course, the Consumer Bureau was created after the big collapse of the economy and it was designed to be independent of the political process that has corrupted a lot of the control of how we protect consumers in the financial system.

By appointing -- by suggesting that the head of the OMB, a deeply political agency of the White House, could also at the same time be the director of the independent Consumer Bureau, we just don't think that computes and we support Director Cordray's appointment of Leandra English as acting director.

We truly recognize the president has the authority to eventually nominate and get someone confirmed by the Senate. But

we hope that person is qualified as a consumer advocate and is not someone who has attacked the bureau and called it a sick, sad joke, as the current acting director has.

The Consumer Bureau, in just six years of existence, has recovered over $12 billion -- about $12 billion for 29 million Americans and has restored confidence in the financial system.

So we like -- we'd like to protect it. Going forward, you have pointed out one issue that is in conflict there is actually data security. Interestingly, the Consumer Bureau gained authority over Equifax when it sells credit reports through the Fair Credit Reporting Act.

But the Gramm-Leach-Bliley Act under the Federal Trade Commission still controls on data security for a number of nonbanks including the credit bureaus. That's a real problem.

Ms. Schakowsky. Yes, although before he left, Chairman Cordray said that he thought that there ought to be embedded regulators at Equifax and companies -- and the other companies.

Mr. Mierzwinski. Well, actually, he does have the authority or he did have. The bureau still retains the authority to supervise Equifax in the same manner that bank regulators including the bureau supervise banks, meaning the ability to be there in an embedded basis and look for problems before they get bad and also to look at the toxic -- not the toxic but the secret sauce that the company uses to generate its credit scores.

There are a lot of things that the bureau can and should do.

But there is this one little piece of Gramm-Leach-Bliley that says the Federal Trade Commission is still the regulator for when you have a breach, when you have to notify.

The Federal Trade Commission rule still has not created a notification standard at the federal level and this is something people may not be aware of. The Federal Trade Commission under Gramm-Leach-Bliley cannot impose a penalty for the first violation of the data security rules.

The bureau can and any bank regulator can impose a penalty for any first violation by companies they regulate. The Federal Trade Commission cannot.

Ms. Schakowsky. So regardless of how big the breach is, how many people are affected, they do not have the authority?

Mr. Mierzwinski. Not under their statute and not under their regulations. They've never done it so I don't believe they have the authority and it is been confirmed to me by former staff there.

Ms. Schakowsky. Oh, I see. Do I have time?

Well, let me see if I can get to one last question and that is about credit freezes. So the long-term risk from data breaches underscores the need for strong data security and breach notification legislation such as the -- I have a bill called the Secure and Protect America's Data Act that I introduced with Ranking Member Pallone, several other members of this committee.

So, again, Mr. Mierzwinski, when a company fails to protect

consumers' data, then where does that leave the consumer? And let me just add also in the wake of the Equifax breach you have talked about making credit freezes free for consumers. How would that help?

Mr. Mierzwinski. Well, how -- making credit freezes free would give us control of our own data, and by the way, that has almost become a bipartisan issue.

The next step is to make credit freezes the default on switch. Make the consumer information always protected until the consumer agrees to turn it on.

Ms. Schakowsky. So the --

Mr. Mierzwinski. The opposite of the current situation.

Ms. Schakowsky. Okay. Thank you so much. I yield back.

Mr. Mierzwinski. Thank you.

Mr. Griffith. Appreciate it. The gentlelady yields back.

I now recognize the gentlelady from Indiana, Mrs. Brooks.

Mrs. Brooks. Thank you, Mr. Chairman, and thank you to all of our witnesses for being here.

I am a former federal prosecutor -- former U.S. attorney that worked on and prosecuted identity theft cases between 2001 and 2007. So this is certainly not something new.

I haven't heard very much, quite frankly though, about going after the bad guys, and we are talking about the hackers and I want to learn a little bit more.

And Mr. Hunt, when you talked about the analogy of it is like

shopping for heroin or so forth on the darknet and so forth, could you please talk with me a little bit more? Because I haven't been in that world, quite frankly, since '07 and really want to learn a little bit more about the buyers, the sellers, and how do they purchase it, select their buyers and sellers.

Do they earn reputations on the darknet? Can you tell us a little bit, and then for yourself and maybe Mr. Grant a little bit about what kind of cooperation you have engaged in with law enforcement.

Mr. Hunt?

Mr. Hunt. I think we can sort of speak to the last part of the question first, which is around reputation, so how do people establish a reputation.

One of the quite intriguing things when you do see these dark market marketplaces or darkweb marketplaces is that in many ways they look very familiar.

They look like an eBay, for example, and there are buyers and sellers on there that have a reputation that they gain over a series of trades. Now, of course, the difference is they're not buying iPhones or consumer electronics. It is, literally, drugs, data breaches, and so on.

So that's sort of the first part of the answer. The establish a reputation. In terms of then identifying who those parties are, one of the difficulties we have with privacy and anonymity tools is whilst they're very good for maintaining

privacy and anonymity for people that want to do good things, they're also very good at maintaining privacy and anonymity for people doing bad things.

Now, we have seen a number of these marketplaces taken down over time but, obviously, they are much harder to track down.

I guess to the other points, one of the things that sort of concerns us is that there is a thriving marketplace for this data and there are, I guess, various shades of gray in terms of who finds this data attractive.

That's, clearly, criminals -- those who literally want to go out and mount identity theft attacks. They find this data attractive.

One of the things that worries me a little bit more is that it is also an attractive piece of information for more mainstream legitimate organizations who are looking to gain access to this data so that they can figure out which of their customers are protected.

So we are now seeing very mainstream online web properties that many of us know and use on a daily basis that will tell people when they have appeared in a data breach and some of these are actually purchasing information in order to gain access to that to protect their customers.

And, frankly, that -- I am a little bit torn with that because I understand the desire to protect their consumers but I also worry about the incentives that provides those who are breaking into

systems.

Mrs. Brooks. Mr. Grant, anything you want to add?

Mr. Grant. Not too much. I mean, my -- look, law enforcement is quite important. It is -- I think as Mr. Hunt pointed out, it is becoming quite hard to attract people down in part because of the international nature of, you know, many of the criminal rings that are actually running all of these, you know, marketplaces and what not.

I would agree in terms of what, you know, Mr. Hunt said as well in terms of the same tools that can protect us and keep us anonymous can also be protecting them. So there are definitely challenges there.

Mrs. Brooks. Has there also been evidence that nation-states besides entities, individuals, criminal organizations are involved in this as well?

Mr. Grant. Absolutely. I mean, that's something we haven't talked about much. I am sure most of us in this room were victims of the OPM breach, which I guess I appreciate that the government is giving me credit monitoring services for this.

I don't think that the government of China is looking to establish credit in my name. They're interested in looking through the 75 pages or so of my SF-86 and figuring out if they can compromise me because I have a top secret clearance.

But this is certainly something that has been quite interesting to other nation states who are looking to execute

attacks, you know, both for those purposes as well as just for, you know, getting into basic accounts.

Again, if we are protecting access to an account with only something like static KBA and they've now stolen the answers to those questions, well, then you can get into them and do things with them.

You know, likewise, Mr. Mierzwinski talked before about, you know, some of the risks of biometrics. All of my fingerprints are now sitting in another country somewhere because of the OPM breach, which means I wouldn't feel particularly comfortable using anything that's doing remote match fingerprint to secure anything that I care about.

That said, I am really comfortable with using a fingerprint on my phone because you have to come get my device out of my hands first before you can compromise it.

Mrs. Brooks. Mr. Mierzwinski mentioned that the credit monitoring services maybe have been not very honest in their practices.

Do you agree that when we receive these requests after we've been a target of a breach that people should or should not be accepting those services by the company?

Mr. Grant. You know, I don't think it hurts to accept them. Whether you pay for them is another question that I think --

Mrs. Brooks. Right.

Mr. Grant. -- you know, folks are asking right now. Look,

I think they are helpful because it is good to know if something is happening. It is good to be able to monitor your account.

Whether you need to pay for it is another question. From, you know, the government perspective as a victim of the OPM breach I don't know what value it offers me other than it is nice thing to have to be able to keep close watch on my credit.

So it -- you know, value in the service, yes. Whether, you know, I want to pay for it as a consumer that's another question.

Mrs. Brooks. Thank you. Thank you all for your work.

Yield back.

Mr. Griffith. I now -- thank you.

I know recognize the gentleman from Georgia, Mr. Carter, for five minutes of questioning.

Mr. Carter. Thank you, Mr. Chairman, and thank all of you for being here and for your efforts to get here. Appreciate it very much.

This is, obviously, very, very important to all of us. I want to start with you, Mr. Grant, and just ask you if you can, and please dumb it down for me, if you will, what are trust marks? Can you just explain that to me?

Mr. Grant. Trust marks -- sure. Best example of a trust mark is the Visa logo that's on two credit cards in my wallet.

So that if I go down to the cafeteria here afterwards and have lunch with Troy or Ed, the cafeteria doesn't really care which credit card I pay with. I got one issued by Capital One and one

issued by Chase.

Because it is got that Visa trust mark on it, which stands for a bunch of standards and operating rules that govern everything from how that card's authenticated at the point of sale terminal, what security is in place, how long it takes for my bank to pay the cafeteria for my lunch, what transaction rate that they're actually going to pay in terms of, you know, the fee for processing that, and some would argue most importantly if -- let's say Chairman -- Vice Chairman Griffith steals my credit card and buys lunch for the committee and I contest that with my bank, what am I liable for and what's the merchant liable for.

So the trust mark is essentially something that represents all those standards and operating rules that in the credit card network everybody who's an issuing bank has to follow and everybody else has to follow.

In the identity space, one argument -- this was a lot of the focus of NSTIC is that we need to create something similar to the Visa network before identity, which is that I could have the issuer be my state DMV or the Social Security Administration, my bank, my mobile network operator.

It could be an advocacy group like the NRA or the ACLU or U.S. PIRG, who all could validate my identity a certain way, issue me a credential that I could use everywhere and the reason it would be trusted is because it has that trust mark.

Mr. Carter. Well, that's really what I am getting at because

as I understand it, the Trusted Identities Group has actually farmed out, if you will, pilot projects and the Georgia Tech Research Institute has actually come up with the emphasis on the machine-readable trust marks, and it is been very successful and the results have been positive, particularly when it was -- when it was over a trusted framework and that would encourage greater trust.

How can this be implemented in industry? How can we use this?

Mr. Grant. So I don't think -- you know, a little bit of background on the GTRI pilot that was one of the ones that I selected for funding when I was, you know, running the NSTIC program and the idea was, you know, how can you do something for identity that's, you know, similar to what you see in financial services.

I would say, you know, where it has gone as a pilot, it was a great -- look, it is a pilot. It is a proof of concept, basically. It isn't something that's been picked up yet by industry.

What I can say, though, is that work is being looked at by -- I don't want to break confidentiality with anybody I am, you know, doing work with now.

Mr. Carter. Right. Right.

Mr. Grant. But some bigger players that matter in the ecosystem who are actually looking at taking that similar concept

and actually developing a, you know, broader federated identity system that could be led by the private sector for making it easier for consumers to identify themselves.

The idea would be to basically leverage work that's being done there already with I can actually say some financial services.

Since banks know you, thanks to the Know Your Customer rules that they go through and you might trust your bank -- not everybody does but some might -- how could they vouch for you other places when you're looking to open up a new account.

Mr. Carter. Right. But do you agree that this is kind of the route we ought to be going?

Mr. Grant. I think -- yes, I think it is a big part of the solution. I don't know that trust marks are going to solve everything. You know, look, so we did some good things with NSTIC.

One of the things we didn't do is solve all the problems and it is because it is really complicated and there's a whole bunch of, you know, whether it is legal barriers, technical barriers, how do you create something that's really easy for consumers to use. There's issues that are out there.

For as much as everybody loves to beat up on KBA and what the credit bureaus do, there's a reason it is been used so much in the market for years because that for many people it is work.

Mr. Carter. Right.

Mr. Grant. I am applying for a new credit card. I can do something instantly. When I went to lease a new car for my wife a year ago, I was able to get quick credit.

So I don't want to suggest we throw the baby out with the bath water because there's problems. It is more realizing where attackers have caught up and how do we develop better solutions.

Mr. Carter. Okay.

Mr. Hunt, any -- any comments on trust marks and how it can be implemented into the private sector?

Mr. Hunt. I think I would probably defer back to Mr. Grant as the expert on trust marks there.

Mr. Carter. Right. Right.

Were there any other new technologies that you find interesting and perhaps that have some potential?

Mr. Hunt. I think ultimately we are going to see an augmentation of different practices. I mean, many people, for example, say, well look, is the answer biometrics or is the answer physical tokens.

And where we are getting to now is I think an acknowledgement that we can't rely on one single knowledge-based authentication attribute, for example -- that we do have many other things available to us now that we didn't have, say, two, decades ago.

We have ubiquitous mobile devices with internet connectivity. We have SMS. We have other forms of identifiers like physical YubiKey tokens, for example. And I think the right

strategy moving forward is going to be the right augmentation of those under the right scenarios, depending on the trust level that you need to establish.

Mr. Carter. Great. Thank you all again, and I yield back.

Mr. Griffith. I thank the gentleman for yielding back. I do have a couple of follow-up questions just to try to clarify some things. Staff did a nice job, as they always do, in educating me beforehand. But, Mr. Grant, you used the term public encrypto.

Mr. Grant. No, public key crypto.

Mr. Griffith. Oh. And what does that mean?

Mr. Grant. Well, so there's -- we can get really geeky talking about cryptography now -- there's essentially two ways you can manage cryptographic keys.

One is called symmetric-key, which is when I got a key and you know the key, and I have to present the key to you for it to match. It is a lot -- similar to the way passwords work.

The other is what's commonly known as asymmetric public key cryptography, or PKI for public key infrastructure. It is what the Defense Department as well as the federal government had been using for years, in many cases in lieu of passwords, in order to, you know, come up with unphishable authentication to protect federal networks and systems.

At the end of the day, the concept is rather than each entity having the same key, I get a key pair, and the public key is known to everybody but the private key is only residing with me.

It can be in my mobile phone. It could be in my computer. It can be on a device like the YubiKey, which is -- that Mr. Hunt mentioned which is a FIDO standard token, and when I am logging in someplace, I am basically asked to sign a cryptographic challenge where my public key is presented but the only way I can get in is if I have the corresponding private key with me physically.

And so the -- we could really go into the details of it in ways that would make everybody's head explode. It is not -- this is actually one of the problems with -- about the adoption of technology, by the way.

It has been very complicated. But I think the most important point to keep in mind is it is a way to deliver unphishable authentication. It is not based on shared secrets.

And when I talk about how attackers have caught up not only to passwords but also things like SMS codes or other one-time passwords that are only good for 30 seconds, you know, that 30 seconds is still enough for a moderately skilled attacker to phish my authentication code.

Asymmetric public key crypto is where we should be building authentication solutions in the future so that we don't have phishable authentication.

Mr. Griffith. All right. I appreciate that.

Mr. Hunt, you travelled a long way. Is there anything that you had a burning desire to tell us that you haven't had an

opportunity already to do so?

Mr. Hunt. I think that the other thing I would add, obviously, I am very interested in how do we stem the flood of data breaches that we are seeing. And, you know, the things that really come to my mind that I would love to see implemented I mentioned education.

So we are making lots of fundamental little mistakes. Another thing that's very important is making the disclosure of these incidents much easier.

So I myself have been in this situation many times where someone has sent me data from an organization and just the ability to disclose it to the company, to find the right person who will listen, who will take it seriously, is enormously difficult.

So I am very supportive of some of the initiatives we are seeing like bug bounties. So, for example, companies like BugCrowd are running many bug bounties where you as an organization can say if someone finds something wrong with my systems, I would like to know about it and I will likely pay a reward for that. And it is done legally, ethically, and it encourages the right behaviors.

And I guess, finally, we'd also like to see more in the way of penalties because at the moment there's not enough accountability when things do go wrong, and I think we are all very curious to see how things like GDPR, which Mr. Grant mentioned earlier, how that plays out when it comes into effect in Europe

in May where potentially an organization can be fined up to 4 percent of their annual gross revenue.

Now, that starts to sting and we really hope that that actually drives more positive behaviors in the industry.

Mr. Griffith. All right. I appreciate that.

Mr. Tonko? Ms. Castor?

Appreciate you all being here. This has been very informative. I suspect it'll be one of the more popular reruns on CSPAN, for those folks who are really into this, and I have learned so much.

Thank you all for your time today and I appreciate it.

And with that, got to go to my script so I don't leave anything out. I would remind members that they have 10 business days to submit questions for the record and I ask that the witnesses all agree to respond promptly to those questions.

Do I need to say anything else? All right. Got all that business -- housekeeping taken care of.

With that, the subcommittee is adjourned. Thank you.

[Whereupon, at 11:47 a.m., the committee was adjourned.]