This is a preliminary transcript of a Committee hearing. It has not yet been subject to a review process to ensure that the statements within are appropriately attributed to the witness or member of Congress who made them, to determine whether there are any inconsistencies between the statement within and what was actually said at the proceeding, or to make any other corrections to ensure the accuracy of the record.

{York Stenographic Services, Inc.}

RPTS BURDETTE

HIF027.170

WHAT ARE THE ELEMENTS OF SOUND DATA BREACH LEGISLATION?

TUESDAY, JANUARY 27, 2015

House of Representatives,

Subcommittee on Commerce, Manufacturing, and Trade

Committee on Energy and Commerce

Washington, D.C.

The subcommittee met, pursuant to call, at 11:01 a.m., in Room 2123 of the Rayburn House Office Building, Hon. Michael Burgess [Chairman of the Subcommittee] presiding.

Members present: Representatives Burgess, Lance, Blackburn, Harper, Guthrie, Olson, Kinzinger, Bilirakis, Mullin, Upton (ex officio), Schakowsky, Clarke, Kennedy, Cardenas, Rush, Butterfield, Welch, and Pallone (ex officio).

Staff present: Charlotte Baker, Deputy Communications Director; Leighton Brown, Press Assistant; Graham Dufault,

Counsel, Commerce, Manufacturing, and Trade; Melissa Froelich, Counsel, Commerce, Manufacturing, and Trade; Kirby Howard, Legislative Clerk; Paul Nagle, Chief Counsel, Commerce, Manufacturing, and Trade; and Olivia Trusty, Counsel, Commerce, Manufacturing, and Trade; Michelle Ash, Democratic Counsel, Commerce, Manufacturing, and Trade; Jeff Carroll, Democratic Staff Director; Lisa Goldman, Democratic Counsel, Commerce, Manufacturing, and Trade; Tiffany Guarascio, Democratic Deputy Staff Director; and Ashley Jones, Democratic Director of Outreach and Member Services.

Mr. {Burgess.} Well, good morning, everyone. Before we begin our first subcommittee meeting of the 114th Congress, the ranking member and I would like to briefly recognize new members of the subcommittee. For the benefit of the ranking member, I am not a new member. I was on this subcommittee several terms ago. So I am back on the subcommittee. For that I am grateful, but on the majority side--I don't believe she has joined us yet. We have Ms. Brooks representing the 5th District of Indiana and Mr. Markwayne Mullin representing Oklahoma's 2nd District. Welcome to the committee, welcome to the subcommittee. We are grateful and excited to have you on board. For the minority, subcommittee Ranking Member Schakowsky will introduce her new members.

Ms. {Schakowsky.} Thank you, Mr. Chairman, for just letting me say how much I look forward to working with you on this subcommittee. New members include Yvette Clarke. She represents New York's 9th Congressional District as a proud Brooklyn native with strong roots planted in her Jamaican heritage. She is an outspoken advocate for district, always working to champion the middle class and those who aspire to reach it. Her district has become a center of innovation for healthcare and includes some of the best hospitals, trade associations, and businesses in the industry. I look forward

to her bringing her tenacity, deep knowledge, and enthusiasm to this subcommittee.

Next to her is Joe Kennedy who serves the people of Massachusetts' 4th, has dedicated his life to public service, and brings with him a firm commitment to social justice and economic opportunity. Joe has previously served in the Peace Corps, worked as an International Development Analyst for the United Nations' Millennium Project, and as an anti-poverty consultant abroad. I know that he will bring that passion for public service and economic growth to everything he does on the subcommittee. And not here now but also a new member of the subcommittee is Tony Cardenas representing California's 29th Congressional District. He has made a name for himself by always advocating strongly on behalf of his constituents on issues like juvenile justice, immigration, higher education, and economic improvement. He has brought hard work and dedication to his 16 years of public service on behalf of the people of the Northeast San Fernando Valley. As a former small business owner, an engineer, head of the California Budget Committee, and as a leader in environmental progress in the City of Los Angeles, I am certain Tony will be able to lead his expertise to our subcommittee's progress. Thank you, Mr. Chairman.

Mr. {Burgess.} Thank you, Ranking Member Schakowsky.

We welcome all members of the subcommittee back and look forward to working with each and every one of you in the 114th Congress.

Before I get started, I also want to recognize a visiting delegation of the legislative staff from the Parliaments of Georgia, Kosovo, Macedonia, and Nepal through the House Democracy Partnership. They are in town for a seminar on strengthening committee operations and are observing today's hearing as part of the program. I hope they are able to learn a great deal, both today and during their tenure here the rest of the week.

Ms. {Schakowsky.} Mr. Chairman, could they acknowledge themselves so we can all see who they are. Great. Thank you.

Mr. {Burgess.} Welcome. Thank you for coming. I am glad you were able to make it here with the weather.

The Subcommittee on Commerce, Manufacturing, and Trade will now come to order. I will recognize myself for 5 minutes for the purposes of an opening statement.

The purpose of today's hearing is to move one step closer to a single, federal standard on data security and breach notification. Increasingly, our personal details, which we need to verify financial transactions, are converted into data and uploaded to networks of servers, and not always

can those servers be protected with a simple lock and key. We benefit immensely from the quick access and command this system gives us. Global commerce is literally at our fingertips on a daily basis.

And yet such a dynamic environment brings with it dynamic, evolving risks. As our options multiply, so must our defensive measures. Those defensive measures must adapt quickly. As several commentators have noted in testimony before this subcommittee, it is no longer a matter of if a breach occurs. It is when and what happens when.

Even so, questions remain as to whether businesses are doing enough to prevent security breaches. That is why I believe federal legislation should include a single but flexible data security requirement. Now, about 12 states have already implemented such a requirement on commercial actors that are not banks or health care providers.

A single requirement across the states would give companies some confidence that their methods are sound in handling electronic data, an inherently interstate activity. Moreover, it would put all companies on notice that if you fail to keep up with other companies, if you aren’t learning from other breaches, you will be subject to federal enforcement.

Indeed, too many resources are spent trying to

understand the legal obligations involved with data security and breach notification. Certainty would allow those resources to be spent on actual security measures and notifications and their affected consumers.

As we discuss the necessary elements of a data breach bill, there are a few considerations that I want to mention. First, there is a limited window for us to act. Criminal data breaches have grabbed the headlines for about a decade, but a consensus solution has thus far eluded federal legislators. This Committee is calling for action, the President asked for legislation with national breach notification, and the Senate has legislation in front of it with a national standard.

But most importantly, it is our consumers who are calling for legislation, thus giving us the time to act.

Second, this legislation is limited to this Committee's jurisdiction. The surest way to deny consumers the benefits of federal data security legislation is to go into areas beyond our jurisdiction. Specifically, the health care and the financial sectors have their own regimes. If we aim to rewrite rules for those sectors, then it will be years, perhaps decades, before a bill is signed into law. That is not to say that we will ignore those issues. But they may need to be taken up separately.

Third, our aspiration at this point is that legislation comes forward with bipartisan support, and do sincerely believe that that is an achievable goal.

With this hearing, I aim to understand the policy points where stakeholder compromise is possible. We are seeking to find agreement not only between the two sides of the dais but also between stakeholders with divergent interests. The sooner we understand the most important principles, the smoother negotiations will go over the next several months.

[The prepared statement of Mr. Burgess follows:]

********** COMMITTEE INSERT **********

|

Mr. {Burgess.} With that, I do want to thank our witnesses for the testimonies that they have provided us and representing their interests candidly in the spirit of compromise. And I would like to recognize the Vice-Chair of the Subcommittee, Mr. Leonard Lance, of New Jersey.

Mr. {Lance.} Thank you, Mr. Chairman, and it is an honor to serve under your leadership as the new chair of the subcommittee, and I am sure you will do a superb job.

Well, the debate over data breach legislation has continued for several years. The issue has been brought to the forefront by unfortunate, high-profile breaches recently, and of course, the most recent is the Sony Pictures hack at the end of last year.

The question of how to proceed on data breach reform has wide implications for both businesses and consumers alike. Today businesses that attempt to report a breach must navigate through a complex labyrinth of 47 State laws which are not all the same. Each State has answered the following questions in its own way: What is defined as an event trigger? What is the appropriate timeframe by which companies must notify consumers that their identifiable information has been breached? Who is responsible for notifying affected consumers?

The lack of certainty of these regulations places an undue burden on businesses trying to report a breach properly and an undue burden on consumers. Federal law will streamline regulations, give certainty to businesses resulting in greater compliance and also to consumers who suffer a data breach.

However, it is my belief that it will only be effective if it preempts the patchwork of 47 State laws. The debate over federal data breach legislation has continued over the span of several Congresses. It is my hope that we can pass effective, bipartisan data breach legislation this year.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Lance follows:]

********** COMMITTEE INSERT **********

|

Mr. {Burgess.} The chair thanks the gentleman. The chair now recognizes the Subcommittee Ranking Member, Ms. Schakowsky, for 5 minutes for the purpose of an opening statement.

Ms. {Schakowsky.} Thank you, Mr. Chairman, for holding today's important hearing on what to include in federal legislative approach to the challenges of data security and breach notification.

I look forward to our work together in the 114th Congress, and this is a great issue to open up with.

The data security is one of the most important issues that this subcommittee will consider this year. In the State of the Union last week, the President urged us to pass legislation that will better protect against cyber attacks and identity theft. I look forward to working with the White House and my colleagues on both sides of the aisle to meet that goal.

Since 2005, over 900 million records with personally identifiable information have been compromised. The recent uptick in high-profile data breaches including those of Target, Home Depot, Neiman Marcus, and Michael's prove two important points: One, just about every retailer and many non-retailers that we engage with are collecting and storing

our personal information, credit card numbers, contact information, and much more. And two, hackers are growing in number and becoming more sophisticated in their attempts to access that personal information, and they are having more success. From programming home security systems and thermostats from hundreds of miles away, to remembering shopping preferences and account information, to connecting with friends over the internet, Americans benefit in many ways from an increasingly data-driven world. But that doesn't mean we should sacrifice our right to have our personal information appropriately protected or our right to know if and when that data has been compromised.

There are a variety of State laws regarding data security standards and breach notification requirements. However, there is no comprehensive federal standard for appropriate protection of personally identifiable information, nor are there federal requirements in place to report data breaches to those whose personal information has been exposed. And I firmly believe that legislation to address that data breach threat must include those two safeguards.

It is important to say that no legislation to require data security standards and breach notification will completely eliminate the threat of data breach. That being

said, entities that collect and store personal information must take reasonable steps to protect data, and consumers must be informed promptly in the event of a breach.

And while I clearly believe that the Federal Government should have a role in data breach--that is what we have been working toward--I also believe that there have been many important protections that are at the State level that we don't want to eliminate when we do federal legislation, perhaps even eliminating rights and protections that would not be guaranteed under federal statute. We have to be sure that we don't weaken protections that consumers expect and deserve. If we include federal preemption of some of those things or if we don't include those good things in federal legislation, then I think that would be a serious mistake at this point.

I also believe that if we include federal preemption, we must ensure that State Attorneys General are able to enforce the law, something my Attorney General has made very, very clear.

So I think we can achieve all these goals working together, get a good, strong federal bill that makes consumers feel confident that we have taken the appropriate steps.

[The prepared statement of Ms. Schakowsky follows:]

267 ********** COMMITTEE INSERT **********

|

Ms. {Schakowsky.} And let me with my remaining time yield to Peter Welch for his comments.

Mr. {Welch.} Thank you very much. Mr. Chairman and Ranking Member, you both nailed it with your description of what we are doing. It is pretty astonishing that with the use of computers, two things still have not been done at the federal level: one, to provide data breach security, and number two, to provide notice to consumers. Consumers receive notice when they have been harmed, but they don't need notice just to scare them. And we have bipartisan momentum here, thanks to Chairman Upton and my colleague Marsha Blackburn, who I have been working with, and Congressman Rush has been working on this for a long time. So we have got a foundation here.

The practical challenges, those are the ones we have to resolve. What do we do about a national standard? What do we do about having enforcement at the AG level, something I agree with Ms. Schakowsky on. What is the notice standard? When should consumers be notified? How do you give some time for a company that has been breached to do law enforcement, investigation, and inquiry into what the scope of the breach was? These are more or less practical issues. And I think the chairman has set a good tone here where we have a common

objective, and we don’t have ideological differences. We have practical differences. And the hope I think of all of us with the foundation that has been laid by my predecessors is to find some common-sense, legitimate balancing of the interests so that at the end of the day we do protect consumers with data breach security, we give some reasonable certainty to our companies, and we have a standard that is robust and strong. I yield back.

[The prepared statement of Mr. Welch follows:]

********** COMMITTEE INSERT **********

|

Mr. {Burgess.} I thank the gentleman. The gentleman yields back. The chair now recognizes the Chairman of the Full Committee, Mr. Upton, for 5 minutes for an opening statement.

The {Chairman.} Thank you, Mr. Chairman, and it has been noted this committee does have a strong tradition of bipartisan cooperation and problem solving. In this spirit, today we continue our focus on the key elements to pass a federal data breach law, a priority that the President identified in his State of the Union address just last week. I look forward to working with the White House, Dr. Burgess, and members of this committee on both sides of the aisle to accomplish that goal.

Criminal cyber hacking presents a serious risk of economic harm to consumers and businesses alike. From small mom-and-pop shops in my district in Southwest Michigan to global Fortune 100 companies, the unfortunate reality is that companies of all sizes are at risk of having information hacked.

This committee will be examining a series of issues relating to cybersecurity in this Congress. Where the conversation begins today is with a data breach bill, and I want to encourage all members and the public to focus on

getting that issue right before we try to tackle some of the other concerns. There are significant privacy issues in an online economy, and some of those will have to be addressed separately.

Let us also be clear that this isn't a financial services bill. We cannot let data breach legislation be sunk by extraneous issues.

Today's hearing will examine two discrete issues related to the complex effects of cybercrime, commercial data security and breach notification to consumers. There is a real opportunity this Congress to set a single, national standard for data security and breach notification. I personally believe that a single, federal standard is the key to passing a solution. The trade-off is that it has to be a strong, consumer-friendly law, one that has real protections and real enforcement. Both the FTC and State AGs have shown that this is an area that they would police very effectively. Our role is to strike the right balance on when notification is required, how timely it needs to be, and what information leads to identity theft.

Setting a national standard benefits consumers by ensuring that every business must look at their activities and make certain that they are taking reasonable security measures. A national standard allows businesses to focus on

securing information and systems instead of trying to figure out how to comply with a host of different State laws with their team of lawyers. Consumers benefit from consistency as well.

We are particularly concerned with the impact that these criminal acts have on consumer confidence, economic growth, and job creation. So let us get to work. A data breach bill is the first step in securing that future.

[The prepared statement of Mr. Upton follows:]

********** COMMITTEE INSERT **********

|

The {Chairman.} I yield the balance of my time to the Vice-Chair of the Full Committee, Marsha Blackburn.

Mrs. {Blackburn.} Thank you, Mr. Chairman, and I want to thank the chairman of the subcommittee for calling the hearing, and I want to welcome all of our witnesses today. We are indeed looking forward to hearing what you have to say.

As has been referenced by Mr. Welch, we have spent a couple of years working on the issues of privacy and data security. We have done this in a working group or a task force and drilling down, making certain that we have a good understanding of defining the problem and then looking at the opportunities for addressing that. So we come to you from that basis of work. And Ms. Schakowsky, Mr. Olson, both served on this task force with us.

Last October Director Comey from the FBI said there are two kinds of big companies in the United States: those that know they have been hacked by the Chinese and those that don’t know they have been hacked by the Chinese. That is pretty apropos, and we know that it applies to all sizes of companies, as Chairman Upton just said.

Because of that, we understand that there are a few things that we need to look at: preemption and making

certain that we have the standard, that this is easily communicated, that our constituents and the citizens understand what is the toolbox that they have for protecting, as I define it, the virtual you, whether that virtual you is they themselves individually, they themselves the small business person, or the corporate entity that is looking to protect its product and its name.

Now, I come from Nashville. We have a lot of entertainment, healthcare, and financial services that are watching this issue closely. They want to make certain that we get this right the first time.

[The prepared statement of Mrs. Blackburn follows:]

********** COMMITTEE INSERT **********

|

Mrs. {Blackburn.} With that, I yield back the balance of my time.

Mr. {Burgess.} The gentlelady yields back. The chair now recognizes the Ranking Member of the Full Committee, 5 minutes for an opening statement, Mr. Pallone from New Jersey.

Mr. {Pallone.} Thank you, Mr. Chairman. I first wanted to congratulate Dr. Burgess on his appointment as the chairman. I will say, though, that having spent last evening with you on rules, I am not going to congratulate you on continuing on rules because I don't know what possible reason you could have for continuing to stay there. But everyone makes their own decisions around here.

I do look forward to working with you on many issues, starting with the issue of today's hearing, data security and breach notification. I also wanted to thank Ms. Schakowsky for her continued service as the Democratic Ranking Member.

The title of this hearing, What are the Elements of Sound Data Breach Legislation?, assumes that legislation is needed, and I agree that it is time to legislate but only if the result is a strong bill that puts consumers in a better place than they are today. Right now millions of consumers are being hit with endless waves of breaches. Criminal

hackers will always target our communities, and while we cannot expect to eliminate data breaches, we can work harder to reduce the number of breaches and better protect consumers' information. Just as we expect a bank to lock its vaults of money, we should expect that companies lock and secure personal consumer information. Unfortunately, that is not happening. According to the Online Trust Alliance, over 90 percent of data breaches in the first half of 2014 could have been prevented had businesses implemented security best practices. Firms must do a better job of protecting information they demand of consumers, and preventing breaches is not just best for the consumer, in the long run it is cheaper for companies as well.

And I believe that we should also expect companies to notify consumers in the event of a breach. During this hearing we will hear the often-repeated statistic that 47 States plus Washington, D.C., Guam, Puerto Rico, and the Virgin Islands already have data breach notification laws on the books. While no one on either side of the aisle wants to unnecessarily burden businesses with duplicative or overlapping requirements, these State laws provide baseline breach notification to most Americans. In addition, businesses that operate nationally often follow the strictest state laws, giving our constituents strong data security and

breach notification protections coverage regardless of what is written in any individual State law. And therefore, I can't support any proposal that supersedes strong State protections and replaces them with one weak federal standard.

So Mr. Chairman, this subcommittee has had a tradition of being bipartisan, particularly on the issue of data security, and the 111th Congress' committee passed a compromise bill on the House Floor as H.R. 2221, and that bill was shepherded by then-Subcommittee Chairman Bobby Rush and was based on a bill crafted by former Subcommittee Chairman Cliff Stearns, and Chairman Upton, Vice-Chairwoman Blackburn, and Chairman Barton were original cosponsors of these various bills.

So I just want to say I look forward to working with the subcommittee on a bipartisan basis to craft similar legislation and legislation that requires companies to have reasonable security measures in place and to provide notification to consumers once a breach has occurred.

[The prepared statement of Mr. Pallone follows:]

********** COMMITTEE INSERT **********

|

Mr. {Pallone.} I yield back, Mr. Chairman.

Mr. {Burgess.} The gentleman yields back his time. The chair would remind all members on the subcommittee that they are able to insert their written statements for the record.

And I do want to welcome our witnesses for being here this morning. I thank all of you for agreeing to testify before the committee. Our witness panel for today's hearing will include Ms. Elizabeth Hyman who is the Executive Vice President of Public Advocacy for TechAmerica, and she will be testifying on behalf of the Computing Technology Industry Association. We also have Ms. Jennifer Glasgow, the Global Privacy Officer for Acxiom Corporation; Mr. Brian Dodge, who is the Executive Vice President of Communications and Strategic Initiatives on behalf of the Retail Industry Leaders Association; and Mr. Woodrow Hartzog, an Associate Professor of Law at Samford University's Cumberland School of Law in Birmingham, Alabama.

Our first witness is Ms. Elizabeth Hyman, and you are recognized for 5 minutes.

|

^STATEMENTS OF ELIZABETH HYMAN, EXECUTIVE VICE PRESIDENT, PUBLIC POLICY, TECH AMERICA; BRIAN DODGE, EXECUTIVE VICE PRESIDENT, COMMUNICATIONS AND STRATEGIC INITIATIVES, RETAIL INDUSTRY LEADERS ASSOCIATION; JENNIFER BARRETT-GLASGOW, CHIEF PRIVACY OFFICER, ACXIOM CORPORATION; AND WOODROW HARTZOG, ASSOCIATE PROFESSOR, SAMFORD UNIVERSITY, CUMBERLAND SCHOOL OF LAW.

|

^STATEMENT OF ELIZABETH HYMAN

} Ms. {Hyman.} Thank you, Mr. Chairman.

Mr. {Burgess.} Be certain that your microphone is--

Ms. {Hyman.} Sorry about that. There we go. Fair enough. Good morning, and thank you very much for having us, Chairman Burgess, Ranking Member Schakowsky, and distinguished members of the Subcommittee on Commerce, Manufacturing, and Trade. We appreciate your convening this hearing and for giving us the opportunity to provide our insights on the important issue of consumer data breach notification.

My name as you mentioned is Elizabeth Hyman. I am the Executive Vice President of Public Advocacy for TechAmerica, the public policy department of The Computing Technology

Industry Association, CompTIA. CompTIA is headquartered in Downers Grove, Illinois, and we represent over 2,200 technology companies, a large number of which are small- and medium-sized firms.

Technology companies take their obligations to protect consumers' information very seriously. Data is the life-blood of the internet economy, and protecting consumers' information is not only a responsibility of the industry but also a crucial business practice. Failure to do so will lead to a loss in customer faith and damage to a business' reputation.

Unfortunately, as has been pointed out, criminals remain intent on stealing information. Data breaches are sadly all too common in 2015, and thus we need strong rules in place to inform consumers when a harmful breach occurs and to provide the necessary information to enable consumers to take the necessary steps to protect themselves.

As you are all well aware and has been stated, there currently is no federal standard for data breach notification. Instead, 47 different States, the District of Columbia, Puerto Rico, Guam, and the Virgin Islands, all have their own separate data breach notification laws and requirements.

Furthermore, States are regularly changing and updating

their data breach notification laws. This year we have already seen 17 bills introduced in seven States in just the first 2 weeks of State legislative sessions. With the increasingly mobile and decentralized nature of our economy, most companies are under the umbrella of multiple State laws at all times. This patchwork of state laws creates significant compliance costs with no additional protection for consumers since no two State data breach laws are exactly the same. In fact, many are in conflict with one another. A federal data breach notification standard is thus necessary to protect consumers and ensure that companies can respond quickly and effectively after a breach.

Responding to a data breach for a company of any size is difficult, especially given the need to assess whether the breach could trigger notification provisions in any one of 47 States, whether they have any consumers that live in any of those States, who to notify, how to notify, what information to include, and what the timelines are for notification.

Small- and medium-sized businesses face particularly difficult compliance challenges. To address their obligations to resolve the breach, gather information, and notify the necessary parties, these companies often rely on cyber-insurance, payment processors, or outside counsel to help implement a response plan. None of these options is

cheap.

Thus, the key to any federal data breach notification law will be finding a single standard that maintains strong requirements but allows companies to focus on the important work of protecting their customers in the wake of a breach.

In crafting a federal data breach standard, we would suggest a few key provisions that are further outlined in my statement for the record. For example, any federal data breach notification law needs to be the standard for all companies to comply with. It cannot simply just become the 48th standard that State can add to. In order to avoid the risks associated with over-notification, a federal standard should ensure that consumers only receive notification about a breach when their information has actually been accessed and only when that information is likely to be used in a harmful manner.

Adequate time should be provided for companies to conduct a risk assessment in order to best assess the scope and depth of the breach. A circumscribed set of sensitive, personally identifiable information must be the basis for determining whether any notification should occur. We should try to avoid mandating specific technologies while also exempting companies from notification requirements where data is rendered unusable. Companies should not be punished for

the criminal acts of others, and private rights of action regarding data breach notification should be explicitly banned.

In closing, I would like to thank the subcommittee for working on the issue of data breach notification. Unfortunately, our patchwork of state laws, while well-intentioned, has created a burdensome and complex compliance regime. A strong, single standard that applies throughout the country will ensure our consumers are safer and ensure our companies are well-informed about how to respond to the growing threat of data breaches.

Security and economic growth are not mutually exclusive, and I would respectfully request that the solutions you draft through this subcommittee address both through a national data breach notification standard. Thank you.

[The prepared statement of Ms. Hyman follows:]

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

|

Mr. {Burgess.} The gentlelady yields back. The chair would now recognize Mr. Brian Dodge, the Executive Vice President of the Retail Industry Leaders Association, 5 minutes for your testimony, sir. Thank you.

|

^STATEMENT OF BRIAN DODGE

} Mr. {Dodge.} Chairman Burgess, Ranking Member Schakowsky, and Members of the committee, my name is Brian Dodge, and I am an Executive Vice President with the Retail Industry Leaders Association. Thank you for the opportunity to testify today about data breach legislation and the steps that the retail industry is taking to address this important issue and to protect consumers.

RILA is the trade association of the world's largest and most innovative companies. Retailers embrace innovative technology to provide American consumers with unparalleled services and products. While technology presents great opportunity, nation states, criminal organizations, and other bad actors also are using it to attack businesses, institutions, and governments. As we have seen, no organization is immune from attacks. Retailers understand that defense against cyber attacks must be an ongoing effort.

RILA is committed to working with Congress to give government and retailers the tools necessary to thwart this unprecedented attack on the U.S. economy and bring the fight to cybercriminals around the world.

As leaders in the retail community, we are taking new

and significant steps to enhance cybersecurity throughout the industry. To that end, last year RILA formed the Retail Cyber Intelligence Sharing Center in partnership with America's most recognized retailers. The Center has opened a steady flow of information between retailers, law enforcement and other relevant stakeholders.

In addition to the topics this hearing will cover today, one area of security that needs immediate attention is payment card technology. The woefully outdated magnetic stripe technology used on cards today is the chief vulnerability in the payments ecosystem. Retailers continue to press banks and card networks to provide U.S. consumers with the same chip and PIN technology that has proven to dramatically reduce fraud when it has been deployed elsewhere around the world.

Before I discuss what RILA believes the components of sound data breach legislation are, I will briefly highlight the significant data breach and data notification laws with which retailers currently comply. As has been said, 47 States, the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands have adopted data breach notification laws. In addition to the 47-plus existing State data breach notice laws, retailers are subject to robust data security regulatory regimes as well. The Federal Trade Commission has

settled at least 50 cases against businesses that it charged with failing to maintain reasonable data security practices. These actions have created a common law of consent decrees that signal the data security standards expected of businesses. Additionally, inadequate data security measures for personal information can lead to violations of expressed State data security laws. Also, many States has so-called little FTC acts that can be used to enforce against what Attorneys General deem to be unreasonable data security practices.

Finally, retailers voluntarily and by contract follow a variety of security standards including those maintained by the payment card industry, NIST, and the International Organization of Standardization.

While retailers diligently comply with this range of data security notice and data requirements, a carefully crafted federal data breach law can clear up regulatory confusion and better protect and notify consumers.

RILA supports a federal data breach that is practical, proportional, and sets a single national standard. RILA urges the committee to consider data breach legislation that creates a single national notification standard that allows business to focus on quickly providing affected individuals with actionable information; that provides flexibility in the

method and timing of notification; that ensures that notice is required only when there is a reasonable belief that the breach has or will result in identity theft, economic loss, or harm; that ensures that the responsibility to notify is that of the entity breached but provides the flexibility for entities to contractually determine the notifying party; that establishes a precise and targeted definition for personal information; that recognizes that retailers already have robust data security obligations and that security must be able to adapt over time.

The final goal of data breach legislation should be to ensure fair, consistent, and equitable enforcement of data breach law. Enforcement of the law should be consistently applied by the FTC based on cases of actual harm. Similarly, if civil penalty authority is provided, it should be capped based on the actual harm to consumers. Also, any legislation should deny a private right of action as it would undermine consistent enforcement.

We look forward to working with the committee on specific language to address each of these above goals. I thank the Committee for considering the need for preemptive data breach legislation and look forward to answering your questions.

[The prepared statement of Mr. Dodge follows:]

688 ********** INSERT 2 **********

|

Mr. {Burgess.} The gentleman yields back. The chair would now like to recognize Jennifer Barrett-Glasgow, the Global Privacy Officer for the Acxiom Corporation. Thank you for your testimony today, 5 minutes.

|

^STATEMENT OF JENNIFER BARRETT-GLASGOW

} Ms. {Barrett-Glasgow.} Chairman Burgess, Ranking Member Schakowsky, members of the committee, thank you for holding this hearing today. I am Jennifer Barrett-Glasgow, Global Privacy Officer for Acxiom, headquartered in Little Rock, Arkansas. Acxiom has two lines of business. We offer primarily to large businesses, not-for-profit organizations, political parties, and candidates and government agencies. First, we offer computer processing services for our clients' information which includes ensuring that information is accurate, analyzing the information to help our clients understand their customers better so they can improve their offerings, and our digital reach services which enable our clients to market to audiences across all digital channels. These services represent over 80 percent of our total business in the United States.

Second, we provide a line of information products to clients in three categories: fraud management, telephone directories, and marketing. And these products support all channels of communication, offline, online, mobile, and addressable television.

Acxiom supports enacting a data security and breach

notification bill, and I would like to mention some of the provisions that we think should and should not be included. Regarding data breach notification provisions, first, the bill needs to include strong preemption for State laws. As stated earlier, 47 States and 4 territories have breach laws, and every year a number of these change. Businesses and consumers will benefit from having one recognizable standard.

Second, there should be a harm-based trigger for notification. Consumers shouldn't get meaningless notices when there is no risk of harm. Businesses will have to evaluate whether there is a reasonable risk if there are penalties for failing to notify, and we will do that responsibly without Congress needing to spell out how it should be done.

Third, legislation should also provide a reasonable timeframe for notification. Consumers do need to be notified promptly, but it is critical to understand the extent and means of the breach and to give law enforcement time to identify and hopefully even apprehend the bad guys. Fixed statutory deadlines do not accomplish these objectives.

Fourth, penalty provisions should be reasonable, and we do not believe there should be a private right of action. Companies who take reasonable precautions but who still get breached are victims, too. Regarding data security language,

just as with breach notification, having a single data security standard is more efficient for companies than multiple State standards. This is more important for some businesses and other entities than it is for Acxiom. We process data for other companies, and our security is assessed by clients upwards of 80 times a year, plus we conduct our own audit internally. So we already meet multiple client standards in addition to those set by law.

Next, because the bad guys' capabilities keep changing, legal and regulatory data security standards need to be extremely flexible to allow adaptive compliance to keep ahead of the threats.

And last, Acxiom believes that businesses have a responsibility to educate their employees about security risks and that government has a role to play in educating the general public on these topics.

Where once the purpose of passing a data security law might have been to ensure companies were thinking enough about security, today we believe Congress should think about security breach legislation more like it has thought about cybersecurity legislation. How can the industry and government and law enforcement work together to keep ahead of these threats.

Finally, a comment on what should not be included in

this legislation. Congress should keep this bill focused on data security and breach notification. There is bipartisan support for enacting a good bill into law on these issues. In the past, other issues have crept into data breach bills, and this has hurt the chances of enactment. For example, some previous bills have included provisions for data brokers, and while Acxiom would be considered a data broker under any definition, it already offers the kinds of provisions seen in past bills through our web portal, AboutTheData.com. The problem has been the definition of data brokers. It was quite broad and included many companies that don't consider themselves to be one. This has stymied enactment of these bills. We urge you to keep the bill clean so we can finally put a good consensus federal data security and breach notification law into place.

Thank you for the opportunity to testify today, and I look forward to your questions.

[The prepared statement of Ms. Barrett-Glasgow follows:]

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

|

Mr. {Burgess.} Thank you. The witness yields back. The chair now recognizes Mr. Hartzog, 5 minutes for your testimony. Thank you, sir, for being here.

|

^STATEMENT OF WOODROW HARTZOG

} Mr. {Hartzog.} Thank you. Chairman Burgess, Ranking Member Schakowsky, and Members of the Committee, thank you very much for inviting me to appear before you and provide testimony. My name is Woodrow Hartzog, and I am an associate professor of law at Samford University's Cumberland School of Law and an affiliate scholar at the Center for Internet and Society at Stanford Law School. I have spent the last 3 years researching the law and policy of data protection, data security, and responses to data breaches. My comments today will address what I have learned from this research.

In order to be sound, data breach legislation must further three fundamental goals: transparency, data protection, and remedies for affected individuals. The patchwork of existing State and federal sector-specific laws further these goals, but aggressively preemptive federal legislation risks counteracting these goals and weakening our critical data protection infrastructure. Hard-won consumer protections could be lost. In short, any data breach legislation that fails to advance these three goals will be counterproductive.

I would like to make two main points regarding the

elements of sound data breach legislation. First, sound data breach legislation should be minimally preemptive of existing State- and sector-specific data breach laws. Data breach laws are relatively new. It is not yet clear what the most effective approach to data protection and data response is or should be. We need multiple regulatory bodies to ensure the adequate resources and experimentation necessary to respond to constantly evolving threats and new vulnerabilities. Additionally, preemption threatens to water down important existing robust data breach protections. There is a real risk that preemptive federal legislation would do more harm than good. For example, federal data breach legislation would reduce the level of protection many or most Americans currently have if it narrowed existing definitions of personal information, if it mandated a showing of harm before companies were required to send notification, or if it failed to require a notice to a centralized organization, like the office of the State Attorney General.

Data breach legislation would also be counter-productive if it created gaps in protection. Federal data breach legislation that preempts all state data breach laws could fail to cover data breaches that only affect the residents of one State. Additionally, preemptive legislation that only covered digitized records would fail to cover breaches

involving paper records which remain a significant target for data thieves.

The second point I would like to make is that sound data breach legislation must also incorporate requirements for data security. While data breach notification is important, we must be sure not to ask too much of it. Under a pure data breach notification scheme, providing reasonable data security would be voluntary. The law should require not just encourage that companies reasonably secure their personal data. If people cannot trust that the entities that collect and store our personal information, the commerce, innovation, public health, our personal relationships, and our culture will all suffer. Ensuring that companies must provide reasonable data security will ensure that fewer breach notifications need to be sent at all.

One important way to fortify data security would be to give the Federal Trade Commission rule-making authority. Specific authority for data security would help the FTC further clarify data security standards, require data security from non-profit entities such as educational institutions, and issue civil penalties.

Federal legislation should also preserve the regulation of data security by States and sector-specific agencies. The numerous federal agencies that require data security are not

redundant. Rather, they can and do coexist with unique expertise and regulatory authority. Even agencies with overlapping jurisdiction contribute valuable resources and have relatively harmonized approaches to data security.

Finally, data breach legislation must preserve the ability of States to regulate data security. Data security is both a national and a local issue sometimes affecting small but significant groups of State residents. Even in the case of large national breaches, residents of some States are hit harder than others. States are nimble and capable of continued experimentation regarding the best approach to regulating data security. They are also closer to those whose data was compromised and provide additional resources to alleviate the strain and cost to enforcement on federal agencies.

The modern threat to personal data is still relatively new. The concept of data breach legislation is newer still. It is too early to start rolling back protections and consolidating agencies to cut costs. Instead, sound data breach legislation should reinforce the current trajectory of data breach law which involves multiple approaches and constantly evolving robust consumer protection. Thank you very much, and I look forward to your questions.

[The prepared statement of Mr. Hartzog follows:]

879 ********** INSERT 4 **********

|

Mr. {Burgess.} The gentleman yields back, and I thank all the witnesses for their testimony and participating in today's hearing. We will now move into the question-and-answer portion of the hearing, and for that purpose, I will recognize myself for 5 minutes. And I do again thank you all for being here.

Let me just ask a general question to the entire panel, and we will start with Ms. Hyman and work our way down to Ms. Hartzog. Reading through the testimony and listening to you this morning, it is clear that most of the panelists agree on--I guess I could say three out of four panelists agree on preemption, that it is necessary for a successful piece of legislation on data security and breach notification. The question is why is it important to have a single standard rather than allowing new requirements to be developed in State courts on top of a federal law? Ms. Hyman, let us start with you.

Ms. {Hyman.} Thank you, Chairman Burgess. It is important because right now we have all these different laws, many of which are in conflict with one another. Many of our member companies are small- and medium-sized IT firms, and they are trying to do business across State lines. They don't necessarily have the in-house resources to cover all

the different State requirements. So having a more simplified federal standard, strong but a federal standard, would allow these companies to do business across State lines with confidence that they are serving their consumers.

The only other thing I would point out is, and I mentioned this in my opening remarks, this is a very unsettled area. As I mentioned just in the last couple of weeks, we have seen a number of bills introduced in State legislatures, and again, if there is some way that we can come up with a strong, appropriate federal standard, I think it would alleviate a fair amount of ambiguity for both the consumer and for the business.

Mr. {Burgess.} Thank you. Mr. Dodge?

Mr. {Dodge.} So I would say the States deserve a lot of credit for acting in the place where the Federal Government hasn't yet. But if Congress intends to or chooses to pass a federal standard, we believe it should be preemptive because first, it will allow consumers to have a clear set of expectations regardless of where they live about what kind of notification they will get, at what time post-breach. We think that is important. Consumers need to know what to expect in the wake of a breach. And also for a breach of institution or business, they want to put all of their energy towards making sure they are quickly communicating actionable

information to the consumers. And a national standard would allow them to do that instead of the complexity of complying with 47-plus different laws.

Mr. {Burgess.} Ms. Glasgow?

Ms. {Barrett-Glasgow.} Breach notification laws that are in place today in the States vary widely as has been said, and in some instances, we don't even have a security requirement in certain State laws. So enacting a federal law that includes both a security requirement and a breach notification requirement will raise the level across the country. And I think if you study those laws to any great degree, you will find that there are very few exceptions that would make a state regime more protective from any consumers.

Secondarily, from a consumer perspective, we don't live in one State all our lives often. I grew up in Texas and moved to Arkansas. And different States with different regimes with different requirements for the types of notices that need to be given create inconsistency for the consumer if they happen to have received a notice in one State and then receive a different notice in another State. As I said in my testimony, I hope that we will look at much more cooperation between law enforcement and companies to educate consumers about the risks that are out there so that they can help in protecting themselves and not rely solely on

companies or government notifying them when there has been a problem.

Mr. {Burgess.} Thank you. Mr. Hartzog?

Mr. {Hartzog.} So I think that preemption on a very limited scale could actually be useful. I think the important thing to remember is that preemption is not an all-or-nothing game, right? So we can preempt minimally or we can have aggressive preemption. So one of the reasons I recommend minimal preemption is so we can move closer towards having a national standard but then preserve some of the hard-won consumer protections and also make sure that federal legislation doesn't create gaps that things that were protected are no longer protected, so for example, solely interstate, intrastate data breaches. And I think that as far as the differences between the 47 different pieces of legislation, they do vary, but I think that maybe sometimes the differences can be overstated possibly. I mean, I think that sometimes it is compared so that it is apples to oranges, which I don't think is true. I think the more appropriate metaphor might be Fuji to red delicious apples, and the idea that it is very burdensome to comply with all 47 State laws, I think that is also possibly, potentially an overstated claim in the sense that (a) businesses comply with 50 different State laws all the time, and (b) a very robust

support network exists to provide companies of all sizes with the adequate help they need to respond to data breach requirements.

Mr. {Burgess.} I thank the gentleman. The chair now recognizes Ms. Schakowsky, 5 minutes for the purposes of questions.

Ms. {Schakowsky.} Thank you. Professor, I wanted to direct my question to you. Authors of some State laws and some federal legislative proposals have chosen to require notification to consumers to be determined by a standard in which notification is dependent on the presence of a risk of harm or actual financial harm to consumers. And I am just wondering if you are concerned about harms beyond identity theft, fraud, or other economic loss, and if so, if you could give us some examples that might narrow too much the definition of risk.

Mr. {Hartzog.} Sure. Thank you very much. I think that the harm trigger as it has been described, the idea that you only have to notify if there is some kind of finding of harm, is a dubious proposition in several different ways, mainly because the concept of harm within privacy law is hotly contested, and to limit the idea of harm to something like financial harm I think is really constraining because there are lots of different harm that can result from data

breaches. So fraud and identity theft are not the only two. When health data gets stolen, you risk things like discrimination, adverse employment decisions, emotional distress. The Sony hack made it very clear that sometimes when information is breached, it is not used to commit financial harm. It is posted online for everyone to see.

And so that brings me to my next point which is the harm trigger is dubious mainly because it is very difficult to draw a line of causation between a breach that occurred and likely harm that can happen sometime in the future. So it is not as though data gets stolen and it is a one-to-one that harm occurs as a result of it. Oftentimes data gets flooded downstream and aggregated with other pieces of data, and it can be extremely difficult to meet the burden of proof that harm is actually likely in any one particular instance. And when you mandate a harm trigger in notification, then what that means is if you don’t have enough information to prove some kind of likelihood of harm, which is often the case in many different kinds of data breaches, then the harm doesn’t go out. So as a matter of default, the notification isn’t extended.

And so I think that it is important to remember the many different ways in which harm can occur and the many different ways in which harm is a relatively dubious concept within

data breach law, not the least of which is that we haven't even talked about the ways in which information can be used against people, not just to harm you for identity theft purposes but to trick you into revealing more information. This is a common phishing attack, right, which is what they call where they use your own personal information into tricking you into think this is a communication from a trusted source. You click on it, then disclose more personal information. And this is more than just a threat to the individual who is tricked. One of the most common ways to hack into companies is through exploiting human vulnerabilities, and one of the ways in which we do that is we take information about people and use that to trick them into revealing more information.

Ms. {Schakowsky.} Answer a question then. Is there a way to identify harm or define harm that would include everything you are talking about? Or are you saying that a harm trigger itself? In other words, what you are suggesting is there needs to be notification of a breach without having to establish harm at all or are you saying we need to define harm better?

Mr. {Hartzog.} That is correct. So generally speaking, I want to caution against over-leveraging the concept of harm, and the easiest way to over-leverage the concept of

harm is to create a harm trigger. And so as a result, my recommendation would be to have the default be noticed because any definition that you use to come up with with harm is going to be--it is probably going to be pretty flawed. It is either going to be over-inclusive in which it would include every single possibility of harm we can imagine, or it is going to be under-inclusive and leave out huge chunks of things that we want to protect against.

And so as a result, my recommendation would be let us not over-leverage the concept.

Ms. {Schakowsky.} I know in the Sony breach we saw employment records, for example, that were revealed. And so, you know, that would be I think a problem for a lot of people.

So what about the--well, let me just put this on the table, and maybe others would want to answer it at some other point, the concern that there would be some sort of problem of over-notification.

Mr. {Hartzog.} The problem of over-notification is also one that I think can tend to be over-inflated. So of course you don't want consumers and people getting 45 emails a day saying, oh, hey, guess what? You know, another piece of your data has been breached. But I think we are a very long way from reaching some kind of point where consumers would just

flippantly ignore some kind of piece of advice and--

Ms. {Schakowsky.} I am going to go ahead actually and cut you off because my time has expired, but I thank you.

Mr. {Burgess.} The gentlelady yields back. The chair now recognizes the Vice-Chair of the Full Committee, Ms. Blackburn, 5 minutes for questions, please.

Mrs. {Blackburn.} Thank you so much, Mr. Chairman. I want to talk a little bit about doing a technology-neutral data security requirement, and it seems like when we talk about privacy, when we talk about data security, when we talk about entertainment delivery, more and more we are hearing, you know, don't get specific on the delivery system or don't get specific on the technology because it takes us forever, forever, to bring legislation into line with where technology is.

So we are going to start. Mr. Hartzog, I will start with you. We will go all the way down the panel, and I just want to hear your thoughts on technology-neutral or specific and how you think we are best served to approach that.

Mr. {Hartzog.} I would agree with you that we should strive to be as technology-neutral as possible. We have seen time and time again when we pass laws that are highly technically specific that they are almost outdated the moment they are passed. And so--

Mrs. {Blackburn.} They are.

Mr. {Hartzog.} --this is why things like reasonable data security standards tend to make sense, and it also is another good strong word of caution against really being overly specific in any one particular area, and if to the point where you have to be overly specific, being sure that you have enabled the definition to change where possible. So I would agree.

Mrs. {Blackburn.} Okay.

Ms. {Barrett-Glasgow.} I agree that the bill should be technology-neutral. I think a good example of language regarding security is the Gramm-Leach-Bliley security provisions which have now stood the test of 15, 16 years or so in the marketplace.

And I would also, which actually may touch on Ms. Schakowsky’s question a little bit, in the Rush bill, H.R. 2221, the definition of harm reads determination that there is no reasonable risk of identity theft, fraud, or other unlawful conduct. And I think that other unlawful conduct picks up a lot of opportunities as technology involves, as new unlawfuls occur, for us to not have to come back and revisit the language.

Mrs. {Blackburn.} Got it.

Mr. {Dodge.} So we would agree, of course, that we

should be technology-neutral. I don't think we can ever lose sight of the fact that the criminals in this space are highly sophisticated and rapidly evolving as we have seen in some of the more recent reports, sometimes backed by nation states. So allowing businesses to evolve as the threat evolves is really important, and technology is a big part of that.

Mrs. {Blackburn.} Okay.

Ms. {Hyman.} And we would agree as well, technology-neutral is an important principle. You know, we have gone from simple redaction to encryption to more sophisticated versions, and as has just been pointed out, you know, we have to keep ahead of those that wish to cause harm. And the innovation of the private sector is a great opportunity to lead on behalf of the consumers.

Mrs. {Blackburn.} Okay. Thank you. Now, Ms. Hyman, we are going to stay with you and come right back down the row. When we are talking about preemption language, I want to hear--and this is the lightning round. We have got a minute and a half left on the clock. So what language do you want to see us consider as we look at preemption?

Ms. {Hyman.} Well, as I stated previously, we want to make sure that we are not just ending up with the 48th standard--

Mrs. {Blackburn.} Okay.

Ms. {Hyman.} --that it needs to be strong enough to actually matter in terms of preemption and simplification.

Mr. {Dodge.} A strong preemption sets a single, national standard.

Mrs. {Blackburn.} Okay.

Mr. {Dodge.} Again, States deserve credit for the work they have done, but you can't create a 48th law.

Ms. {Barrett-Glasgow.} In my written testimony, I actually suggested some language that you might want to take a look at. I am not going to get into that right here.

Mrs. {Blackburn.} Thank you.

Mr. {Hartzog.} My recommendation would be preemption that served as a floor but not a ceiling and at worst would only preempt the very specific provisions listed by the federal legislation.

Mrs. {Blackburn.} Okay. Thank you all. I yield back.

Mr. {Burgess.} The gentlelady yields back. The chair now recognizes Ms. Clarke for 5 minutes for your questions, please.

Ms. {Clarke.} Thank you, Mr. Chairman, and I thank the ranking member. I would like to drill down a bit more on the breach notification issue.

Breach notification laws and legislative proposals can vary greatly in how they treat the question of when a company

affected by a breach is required to notify consumers. The Data Accountability Trust Act, H.R. 2221, affirmatively presumed a company affected by a breach would notify consumers in the breach unless it determined that there is a reasonable risk of identity theft, fraud, and other unlawful conduct. There have also been proposals with a ``negative presumption,'' in other words, that a company does not have to notify consumers unless an investigation reveals that a certain level of risk exists to the consumers whose information was breached. The burden to prove risk in this case is not on the breached holder of consumers' personal information but rather on those challenging its breach notification practices.

So Professor Hartzog, have you thought through what should be the presumption for firms to notify consumers of a breach and if so, why?

Mr. {Hartzog.} Thank you very much. I have, and my recommendation would be to a presumption of notification in terms of breach. There are some interesting options available with respect to granting a safe harbor that are still debatable. Maybe if you make information unusable, unreadable, using things like encryption standards, then that is something that States have been experimenting with. That is a positive element, although that is not free from

controversy with respect to the effectiveness of encryption. But when the presumption is that you don't have to notify unless an assessment of risk of harm proves that it is likely, then you miss out on a great deal of notifications. And it is important to remember that notifications are important not just for the individual that is being notified but also for other companies that are similarly situated so that they can know about threats that are facing them and perhaps practically respond to them, for State AGs, for the public so that they can be aware, just become more aware of the issues about data breach generally speaking.

So when the default is set and a practical effect will result in far fewer notifications, then I think that the public and other companies that--and individuals are--

Ms. {Clarke.} So that brings me back around to the question raised by Ranking Member Schakowsky. She broached this issue of over-notification with you, and one of the concerns raised about breach notification is notification fatigue or over-notification. Would a negative presumption for notification be effective in preventing over-notification?

Mr. {Hartzog.} I think that it is not so much as to whether the presumption of harm trigger would be effective in preventing over-notification. Certainly it would probably

result in fewer notifications. So then the question becomes is that a good thing or a bad thing? And I again state that we collectively lose out when notifications drop, even though there have been breaches because there is value we can get from notification. And also, over-notification is a problem not just aided by reduction in notification, but we also need to continue to experiment with the way notification is given. There is a presumption maybe that notification is just a big dense block of text that individuals would--it is very easy just to look at and throw in the trash. One of the reasons we still need to experiment, perhaps at the State law level, is that we need to focus on the way notification is actually delivered because there is a lot of opportunity there to avoid oversaturation as well.

Ms. {Clarke.} Did any of you want to weigh in on the issue of over-notification or concerns that your industries may have? Ms. Glasgow?

Ms. {Barrett-Glasgow.} Yes. I will go back to H.R. 2221, and the language that is in there I think is reasonable and good in terms of both the risk of harm as well as the presumption of notification unless it says the person shall be exempt from the requirement, meaning the notification, if certain conditions apply.

I think we have to be very careful about over-

notification. I think we have learned through not just breach notification laws that exist today but also other requirements such as Gramm-Leach-Bliley privacy notices that when consumers get repeated information about risks or about even what a bank may do with their data and there is no clear instruction as to what to do, and there may not be any recourse other than watch your accounts, that is possible, then they tend to get far more complacent about them and potentially even not read the one that really was the one that they needed to react and respond to. So I think industry in general is very sensitive to the over-notification problem.

Ms. {Clarke.} Let me just say very quickly in closing, is there something that we can learn? Is there value to proceeding with notifications simply in terms of uncovering what works best? We are really in the advent of understanding exactly what is taking place. We wanted to get a sense of whether in fact there is value. Mr. Hartzog?

Mr. {Hartzog.} One of the great benefits of breach notification statutes is it allows us to collect information and then issue reports which could then benefit not only companies but the field of data security generally because it helps us know where threats are coming from, what the response to those threats are, and how long it takes to

respond.

Mr. {Burgess.} The gentlelady's time has expired. The chair thanks the gentlelady. The chair now recognizes the Vice-Chair of the Subcommittee, Mr. Lance, for 5 minutes for questions, please.

Mr. {Lance.} Thank you, Mr. Chairman. This is a very complicated issue, and we don't want to become the 48th and yet we want strong protection. And I think it is going to be a difficult needle to thread.

Ms. Glasgow, as I understand your testimony, you believe that we threaded the needle relatively well in Gramm-Leach-Bliley, is that accurate?

Ms. {Barrett-Glasgow.} As in regards to the security rule, yes.

Mr. {Lance.} Yes. And do other distinguished members of the panel have an opinion on that and how it might relate to what we are attempting to do here? Ms. Hyman?

Ms. {Hyman.} As we think about harm and the risk of over-notification and how we should be looking at this, we want to make sure that the information that is exposed actually is significant harm. So just having for example a name or address on its own without other identifiable information like a Social Security, these things need to be seen in context, and how we thread that will be important.

Mr. {Lance.} Mr. Dodge?

Mr. {Dodge.} So I think the regulatory regimes that cover businesses should reflect the businesses themselves, but specific to notification, I believe that consumers should have a strong expectation of how they would be notified if certain information, personally identifiable information, is lost regardless of the business itself. It should be based on the data.

Mr. {Lance.} Professor Hartzog?

Mr. {Hartzog.} I think the Gramm-Leach-Bliley safeguards protections have been quite effective. They are technology-neutral and recognize data security as a process rather than just a one-time thing. So I would say that that has been very effective.

Mr. {Lance.} So this might be an area of agreement in the panel, and I think this subcommittee and then the Full Committee want to reach a point where we can report to the Floor a bipartisan bill that moves the Nation forward.

It has been a long time since I went to law school, but do we look ultimately to fundamental principles of tort law, Professor Hartzog, as to what we should be doing here?

Mr. {Hartzog.} I would caution against relying on tort law too heavily, mainly because tort law is entrenched in a harm-based mindset.

Mr. {Lance.} That is why I asked the question.

Mr. {Hartzog.} And we see that because of causation issues, because it is very difficult to prove that one piece of notification when compromised results in some kind of tangible harm on the other end--I teach tort law, and causation is one of the things you always end up getting tripped up on. And so I would actually caution away against looking to tort law and look into more general proactive regulatory principles.

Mr. {Lance.} I was taught tort law by John Wade who is the reporter of the restatement in the law school not too far from where you teach, just a little north of where you teach. How about others on the panel regarding should we look at all to tort law or is it not broad enough given our desire in a bipartisan fashion to protect the public. Mr. Dodge?

Mr. {Dodge.} I know when I am out over my skis, so I wouldn’t--

Mr. {Lance.} I see.

Mr. {Dodge.} --be able to comment on that.

Mr. {Lance.} I see. Ms. Glasgow?

Ms. {Barrett-Glasgow.} No, I am a technologist, not a lawyer so--

Mr. {Lance.} Okay. That speaks well of you. Ms. Hyman?

Ms. {Hyman.} Unfortunately, I have to join my colleagues on that.

Mr. {Lance.} I see. I won't take all of my time, but let me say that the chairman and I have discussed this at some length, and we want to be able to report a bipartisan bill. But we don't want this to be the 48th state. We want to move the Nation forward, and we want strong consumer protection. And I know the chairman is dedicated to that as am I, and I hope that we can all work together. And I see some areas of agreement. Thank you, Mr. Chairman.

Mr. {Burgess.} The chair thanks the gentleman. The gentleman yields back. The chair recognizes the gentleman from Massachusetts, Mr. Kennedy, 5 minutes for your questions, please.

Mr. {Kennedy.} Thank you, Mr. Chairman. Thank you to the witnesses for testifying today. Insightful hearing. I want to build off actually some of the comments that my colleague, Mr. Lance, just talked about and touched on and try to see if we can thread that needle a little bit.

As he indicated, 47 States, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have all enacted their own laws requiring notification of security breaches involving personal information. Some States, such as Massachusetts and California, have mandated strong

requirements. California's data breach notification law requires that a person be notified when their encrypted personal information has been or is reasonably believed to have been acquired by an unauthorized person, and the consumer has the right to know about all breaches of personal information, not just those deemed capable of doing harm.

Massachusetts law mandates that data owners provide notice of a security breach to the State's Consumer Affairs Office, State Attorney General, and the affected resident and include any steps the data-holder has taken relating to the incident.

Professor Hartzog, some legislative proposals include preemption of ``any provision of a law, rule, regulation, requirement, standard, or other provision having force and effect of law relating to either data security of personally identifiable information or notification following a breach of personal, identifiable information.'' As I understand it, that would not be limited to the 47 States' statutes but it could, building off of a comment a moment ago, also preempt tort law and contract law. Seeing as you are a tort professor, is that correct and can you just walk us through that a little bit?

Mr. {Hartzog.} Sure. So that strikes me as very broad preemptive language and the kind of which I would recommend

against, precisely because while tort law isn't our best hope, we still might actually find some hope in tort law, maybe not in the tort of negligence which is very harm based, but perhaps other theories. So some of the more successful theories at the State level with regard to data security have been promises made by companies about data security which is sort of a tort and contract mixture. And for legislation to preempt that I think would be very problematic, and I think we have to be very careful about broad preemption with respect to federal sector-specific data security law as well because there are some extremely important protections that exist throughout in various different sectors.

And so that kind of preemptive language is exactly the kind of preemptive language that would strike me as one that would ultimately end up doing more harm than good based on how significant it would seem to scale back protections for consumers.

Mr. {Kennedy.} So building off of that, Professor, as I understand it, Massachusetts data breach law has some strong data security requirements which include the authority of the Massachusetts Department of Consumer Affairs and Business Regulation to issue regulations regarding data security. Would those regulations then be preempted potentially by that language that I just referenced? We obviously, yes, don't

want to add in another layer of regulation but want to make sure that there is some strong consumer protection standards and allow States to innovate here as well.

Mr. {Hartzog.} That is correct. That language would seem to preempt the State law protections in Massachusetts as well as all the other States that have data security requirements related to it, and this is potentially problematic because while the general approach to regulating data security seems relatively consistent--we all want reasonable data security practices which is relatively tethered to industry standards--States and policymakers in general are still trying to figure out exactly the best approach to that. And it would seem to be a problem to set something in stone when we are still trying to grapple with this very important issue.

Mr. {Kennedy.} Okay. Thank you, Professor. I will yield back.

Mr. {Burgess.} The gentleman yields back. The chair recognizes the gentleman from Mississippi, Mr. Harper, 5 minutes for your questions, please.

Mr. {Harper.} Thank you, Mr. Chairman, and thanks to each of you for being here. It is a great concern as to how you protect the consumers and reduce the burden here and maybe prosecute the bad guys. So there is a lot to be done.

This affects--I don’t know of a company that is not greatly impacted and truly troubled by this.

First question would be a follow-up, Mr. Dodge. Some have suggested that consumers should receive notice from the company that was breached, even if they have never interacted with that company. Wouldn’t it be clear for a consumer if they receive notification about a breach from the company that they actually gave the information to directly?

Mr. {Dodge.} So we think that the obligation to notify creates a very important incentive to keep systems strong and protect the information that companies hold. We would urge the committee as it considers this to maintain that obligation but allow for flexibility for businesses to contractually determine the notifying party because I think there are situations that you describe where that is appropriate. But to try to contemplate all those situations would be problematic and could undermine that important incentive.

Mr. {Harper.} Is there a risk to consumers that you could create some confusion by duplicate notification from the company they gave information to and also a third party? What do you say about that?

Mr. {Dodge.} So again, I think the objective from all the parties involved would be to make sure that it was a

streamlined and clear notification. And so that is why we would argue that the value of maintaining that incentive is high, but allowing flexibility for the parties involved as you described to contractually determine who would distribute that notice.

Mr. {Harper.} And this would be a question to Ms. Hyman, you, Mr. Dodge, and Ms. Glasgow. Some States trigger notification to individuals after the company determines that there has been an unauthorized access to their information while the majority of States require notice upon a reasonable belief that the data was acquired by an unauthorized party. So the data was actually removed from the system. Is there a danger of over-notification to consumers if the duty to notify individuals is triggered by access but not acquisition?

Ms. {Hyman.} Yes, there is, and we think it is very important that companies have an opportunity to do an appropriate risk assessment to determine whether there has been actual access to the information.

Mr. {Harper.} Mr. Dodge?

Mr. {Dodge.} We believe that it has to be at the time of the confirmed breach. You want to be able to, in the wake of a breach, to define the universe of affected individuals so that the notice goes to the people who truly were or could

be impacted, rather than overly broad and catching people that perhaps weren't affected.

Mr. {Harper.} Okay. Ms. Glasgow?

Ms. {Barrett-Glasgow.} You know, the subtle difference between access and acquisition is really kind of lost I think in this debate in that if there is access and it is from an unauthorized person, you more than likely have some potential risk.

So if a company is assessing that, I think responsible companies are going to err on the side of caution.

Mr. {Harper.} And Ms. Glasgow, earlier you testified when we were talking about a national notification standard, you mentioned a harm-based standard. Who is going to determine--in your eyes, who is best able to determine if there is harm?

Ms. {Barrett-Glasgow.} Well, I think it is determined by a number of parties. First, the company is the one that is on the line to begin with to make that assessment based on their understanding of what has happened. But beyond that, there are various regulatory agencies, the FTC at the federal level and of course State AGs at the State level, that put teeth into that analysis to make sure that that assessment is done effectively and fairly for all parties.

Mr. {Harper.} Just as a comment. When you have 47

standards and you have a company, most companies are national companies. It is extremely confusing and difficult for them, and that is why as we look toward a bipartisan approach to this, it is going to be very important how we move forward.

Mr. Dodge, if I could ask you, while there are ongoing discussions on how to establish a sensible time period in which companies are required to notify consumers of a breach, I am also interested in understanding what exactly or who exactly would start the notification timeframe so there is no room for misinterpretation of when companies are required to notify consumers. I would imagine that your members would not want this left up for interpretation after the fact. What are your thoughts on when this clock should start and who should be responsible for starting it?

Mr. {Dodge.} So we believe that the trigger should be the confirmation of a breach, and at that point of course there are lots of players who would be involved from law enforcement to presumably regulators if Congress were to go down this path. I think what is important to remember that there needs to be flexibility in that timeline because there are a number of steps that need to occur in order to ensure that the notice that goes out provides actionable information. So you want to first define the universe as I said a moment ago. Then you need to train your staff because

invariably when these notices are received, it is going to lead to a number of questions. It won't be limited to the phone number or whatever the method of contact is on the notice. So you need to train staff in order to be able to respond and help consumers protect themselves.

And then there is the complex process of sending out a notice. It could be extremely large scale and making sure that notices aren't just going into junk mailboxes.

Mr. {Harper.} And not meaning to cut you off, my time is expired. Thank you, Mr. Chairman.

Mr. {Burgess.} The gentlelady yields back. The chair thanks the gentleman. The chair now recognizes the gentleman from Vermont, 5 minutes for your questions, please.

Mr. {Welch.} Thank you. I didn't know whether Mr. Rush was ahead of me or not, but he tells me he is not from Vermont. So I am okay to go. We would love to have you.

Thank you very much. This is extremely helpful. A couple of the issues we are wrestling with is, number one, is preemption, and in general, I favor non-preemption but I have been persuaded that if we can get the right standard, this is one of those situations where it really makes sense to have preemption.

Let me just go down the line like my colleague, Marsha Blackburn, did. If we have preemption, it is going to give I

think a lot more comfort to those of us who are willing to take that step if the standard is stronger, and we have got a strong standard in Illinois. We have got a strong standard in California. In my conversations with some folks in the industry, the advantage of a single standard makes them supportive of a strong standard. And I want to just get each of your views on that. In other words, if we have preemption, do you support a relatively robust standard?

Ms. {Hyman.} We have spoken out in favor of significant harm to the consumer. States are justifiably proud of the work that they have done. The chairman of our IT security group is from Massachusetts, but he, too, has shared with us the notion that the patchwork has become unworkable--

Mr. {Welch.} Right. So--

Ms. {Hyman.} --for companies such as theirs. So--

Mr. {Welch.} --you get a single standard, a strong standard is something you could support if you got preemption?

Ms. {Hyman.} Yes.

Mr. {Welch.} And how about you, Mr. Dodge?

Mr. {Dodge.} Again, based on the recognition in the case of harm or risk to consumers, yes, we totally agree, and we believe that the preemption is really, really critical.

Mr. {Welch.} Okay. Thank you. Ms. Glasgow?

Ms. {Barrett-Glasgow.} Yes, the harm-based trigger tied with federal preemption is very acceptable.

Mr. {Welch.} Okay. And Mr. Hartzog?

Mr. {Hartzog.} Well, I would say that if federal legislation is really going to move the ball forward and not actually strip away existing protections, then we should not have a harm-based trigger, and we should also, even to the extent that we should have broad definitions of things like PII which we have now, that may actually change in the future. And so we need to be sure that we can change the law--

Mr. {Welch.} If I understood your testimony, though, you had reservations about preemption, but you weren't categorically opposed to it.

Mr. {Hartzog.} That is correct. That is right.

Mr. {Welch.} Your concern is that whatever our standard is, it be robust.

Mr. {Hartzog.} That is right.

Mr. {Welch.} Correct?

Mr. {Hartzog.} So, so long as the standard is at or above what we currently have now, then I think that we can continue to move in the correct trajectory for data breach.

Mr. {Welch.} Okay. Thank you for that. The other question is if you have a single standard, can you have that

be enforceable at the local Attorney General level as well as at the federal level? And folks like Illinois, the Attorney General has been very active in this. I know Vermont has been active in local enforcement. Would there be any problem with allowing the enforcement of that standard, both at the federal and at the state level, where people would have I think more confidence that they would be heard? Let us go down the line.

Ms. {Hyman.} Sure. We understand and accept the notion that the State Attorneys General should have the opportunity to enforce or the FTC or the federal body, but we would argue that one should extinguish the other. In other words, you shouldn't have those contemporaneously.

Mr. {Welch.} I see. Okay. Mr. Dodge?

Mr. {Dodge.} Just building off that, I think we do recognize that there is an important role for the State AGs to play in this.

Mr. {Welch.} Thank you.

Ms. {Barrett-Glasgow.} Yeah, I agree, and so long as the coordination between State AGs and FTC is in place.

Mr. {Welch.} Okay. Mr. Hyman [sic]?

Mr. {Hartzog.} I would agree that enforcement of the State AGs would be desirable for a data breach.

Mr. {Welch.} Okay. The other question I want to go to

is this whole issue of tort law, and I understand that is somewhat injected into this. My understanding is, and correct me if I am wrong, the issue of tort law just applies in general across commerce and across non-commercial activity, and this committee, I am not sure--Mr. Chairman, I thought you were correct in your opening statement for acknowledging in some areas we simply don't have the jurisdiction to get involved. And I am thinking--

Mr. {Burgess.} Would the gentleman yield?

Mr. {Welch.} Yes, I will.

Mr. {Burgess.} For his purposes going forward, the chair is always correct.

Mr. {Welch.} That more or less settles it. But I see that this whole question of tort law and whether there should be some carve-out as really a separate question from the heart of this legislation. There are a lot of folks that would love to not ever have to worry about tort law, but that is across the whole spectrum of any kind of activity in society, and taking that challenge on in this legislation may be a burden that is inappropriate to bear and too great to bear.

So I just want to get your comment as to whether some tort provision in here in your mind is essential to getting some of the good things that both sides seem to be

supporting.

Ms. {Hyman.} Well, again, I will point out I am recovering lawyer. So my familiarity with tort law is a little bit obscured at this point in time. But the one thing I would say is that we need to separate out and distinguish between good actors and bad actors. And what this effort about data breach notification is about is trying to provide clear lines of responsibility between the companies and the consumer. There are always going to be people that are bad actors, and they should be punished.

Mr. {Welch.} Right.

Ms. {Hyman.} That is a different subject.

Mr. {Welch.} Okay. Mr. Dodge?

Mr. {Dodge.} I, too, am not a lawyer, so I can't speak to the details of tort law. But I would say that, you know, this whole exercise is about empowering customers, consumers, with expectations around how they would receive notice and empowering businesses to conform to a standard.

Mr. {Welch.} All right. I see my time is expired. So the last two dodged the bullet. Thank you. I yield back.

Mr. {Burgess.} The chair thanks the gentleman. The chair now recognizes the gentleman from Texas, Mr. Olson, 5 minutes for your questions, please.

Mr. {Olson.} Thank you, Mr. Chairman, and

congratulations on your first hearing of this important subcommittee, and welcome to all of our witnesses. I assure you, I went to law school, but you won't hear the word tort come out of my mouth through my questions.

Unfortunately, in today's world, data breaches are happening more and more often. Target, Home Depot, Neiman Marcus, Sony Pictures all have been attacked by very different bad actors. We have to be aggressive on account of this threat, but it is a bit but, we must craft a balanced approach that protects consumers without undue burdens upon business.

My first line of question is about notification. I want to bore down the issue a little bit. My first question to you, Ms. Hyman, is it realistic to require any company to notify consumers within a set number of days after a breach occurs?

Ms. {Hyman.} Thank you, Congressman. First of all, I just want to reiterate, businesses are incented to be responsible to the consumer. This is about trying to make sure that the consumer has information quickly and it is actionable.

There needs to be a reasonable period of time to do a risk assessment to find out, as was pointed out by my colleague, was there actual harm? You know, are there

opportunities to remedy that harm? What kind of messaging is being provided to the workforce so that they can respond to the consumer when a notice goes out? So a reasonable period of time needs to be in place for risk assessment. Thereafter, if there is an appropriate timeframe for the actual notification, that makes a lot of sense.

Mr. {Olson.} How about if they have some notification, when did this breach occur? Wouldn't we say that is where it happened, that is where the notification period starts? I mean, I am so confused when this clock starts running. Any idea when that clock starts running, ma'am?

Ms. {Hyman.} I think you are saying does the clock start--

Mr. {Olson.} Yeah, when does it start? You said it is reasonable.

Ms. {Hyman.} When there is an actual breach.

Mr. {Olson.} Okay. When does it start if it is reasonable? When do we start the clock? When has the breach occurred?

Ms. {Hyman.} As soon as there is any type of information for the company to take a look and do the risk assessment, they have to do that within a reasonable period of time.

Mr. {Olson.} Okay. Mr. Dodge, how about you, sir? How

about--is there reasonable required notification within a set number of days?

Mr. {Dodge.} So we would urge flexibility in determining what that length of time is. As we have talked about, there are a number of steps that need to occur. But in every instance, the business entity that I am aware of has a desire to communicate that quickly because they want to make sure they are limiting any exposure or risk to those affected by the breach itself.

Mr. {Olson.} Ms. Glasgow, I know you are a UT Longhorn and probably want to talk about this issue. Any concerns about requiring notification of breaches?

Ms. {Barrett-Glasgow.} Yes. I think there are two. First, any kind of deadline tends to become the norm so that--and some breaches are very simple or small breach, notification can take place in a matter of days or weeks if it is contained, a briefcase that is lost or something that is easily to investigate.

A big, complicated breach like we saw with some of the recent ones that you mentioned, take much longer. And so, you know, we run the risk of extending a simple breach to 30 days because that is the rule. But we also run the risk of not having enough information to do the assessment. And so--and the notification process may be iterative. Through an

investigation, you don't always have all the facts immediately. I mean, think about any criminal investigation that law enforcement takes. You learn something, and from that you ask more questions and from that you ask more questions. So it can very much be an interactive process of learning over a fairly extended period of time. So I think any kind of arbitrary number is inappropriate.

You know, language like we suggested in our written testimony that says without undue delay we think creates the sense of urgency but doesn't necessarily penalize the very complicated investigation.

Mr. {Olson.} And one final question about harmless breaches. We all agree that there are breaches that are harmless, yes or no? Ms. Hyman, yes or no, harmless breaches? We agree that some breaches are harmless?

Ms. {Hyman.} Yes, there are some harmless breaches because of the type of information that is accessed.

Mr. {Olson.} Mr. Dodge?

Mr. {Dodge.} Yes, of course there are situations where intrusions can occur and no information has been taken.

Mr. {Olson.} Ms. Glasgow?

Ms. {Barrett-Glasgow.} Yes. I will give another example and that is when the information that was taken is encrypted or is essentially in some form that is unusable by

the thief.

Mr. {Olson.} And Mr. Hartzog, Professor Hartzog?

Mr. {Hartzog.} I would say it depended on how you define harm. There are lots of different ways to think about it. I mean, does it result in--was the breach a result of poor security practices, even though it didn't result in financial harm? It resulted in perhaps a breach of trust. Even if it is rendered unusable, if the encryption standard--was it adequate to actually protect the data? And so I would actually hesitate from saying yes to that question simply because the way you define harm is everything and that--

Mr. {Olson.} With you leaning yes, sir. I yield back.

Mr. {Burgess.} The gentleman yields back. The chair thanks the gentleman. The chair now recognizes the former chairman of the subcommittee, my longtime friend, Bobby Rush, from Chicago.

Mr. {Rush.} Thank you. Thank you, Mr. Chairman, and I want to also congratulate you on your first hearing. It is an outstanding hearing, and I want to congratulate all your witnesses. They have provided fine testimony. And Mr. Chairman, I am going to take your pronouncement under consideration that you are always right, that you are never wrong--no, you said you are always right. And I am going to really try to process that because I am never wrong. So we

have come to some kind of mutual understanding and agreement on that, all right?

Mr. Chairman, I want to get to the matter of the day, and I want to talk Dr. Hartzog. Dr. Hartzog, I am of the opinion that somebody has got to be in charge of interpretation. Somebody has got to be in charge of implementation, all right? And I understand you call for regulation by multiple agencies in their areas of expertise. Beauty is in the eye of the beholder, and one of the issues that we are always struggling with in this place is who has got the final say? Who has got jurisdiction and what is it that they have jurisdiction over?

My question to you is, first of all, if you can kind of explain to us and clarify what do you mean by regulation by multiple agencies in their areas of expertise? Can you be a little bit more clear in regards to that? And my second question is do you believe that there should be one central agency who could be the final authority on data security for the Federal Government?

So will you try and clarify your perceptions in terms of jurisdictional issues?

Mr. {Hartzog.} Sure. So thank you for the question. I think that there should not be one entity that is in charge of data security for the entire country simply because data

security is--what constitutes good data security and reasonable data security is so highly dependent upon context and industry. And so we have already existing numerous regulatory agencies, like the Federal Communications Commission, HHS and HTSA, the FAA, many different regulatory agencies, all of which have in some form spoken and made some requirements for good data security or looking into requirements for data security. And it is imperative that we rely upon these multiple regulatory bodies because they have expertise in very specific things. So the Federal Communications Commission has well-developed expertise in regulating telecommunications companies, satellite companies, and cable companies and other intermediaries and the specific data security requirements that apply in those particular fields, which might differ than say a standard commercial enterprise.

That being said, sometimes there is overlapping jurisdiction, but what we have seen with multiple regulatory agencies is we have seen that they can coexist. They work together. Sometimes they have coordinated investigations. Sometimes they reach memorandums of understanding where they say, you know, you will handle certain kinds of data security breaches, and we will handle other kinds.

And so that is what I meant by the importance of

regulatory bodies, multiple regulatory bodies.

Mr. {Rush.} I have a second question here, and this is directed to Ms. Glasgow. The Federal Trade Commission called on Congress to enact the legislation to allow consumers with access to information held by data brokers. The Commission has also recommended that one centralized Web site be created where consumers can learn about how their data is used, correction to inaccuracies of their data, and to opt out for marketing if desired. Do you support these recommendations?

Ms. {Barrett-Glasgow.} We actually have gone so far as to implement the recommendation to have one central site where clients can come and look--or consumers, excuse me, can come and look at the data that Acxiom holds and correct it and change it. And we continue to work with industry on whether or not having a central site where everyone lists themselves and a consumer goes there, how that might be effective in terms of transparency. We certainly support the objective that the FTC has stated relative to transparency.

Mr. {Rush.} I only have a few seconds, but can you share with the committee some of your experiences? I mean, how do the consumers, how do they go about it? How do they grade their experience with Acxiom?

Ms. {Barrett-Glasgow.} Yes. The site requires the consumer to log in and identify themselves because we are

going to be sharing the data that we have about them on that site. So we have to know who they are, but once they have logged in and established an account, then they can look at all the data that we used for any of our marketing products. They can delete an element. They can change an element, or they can completely opt out of the whole process online, and it happens in real time. We would encourage you to maybe go to the site and take a look. It is called AboutTheData.com.

Mr. {Rush.} Thank you, Mr. Chairman. I yield back.

Mr. {Burgess.} The chair thanks the gentleman. The gentleman yields back. The chair now recognizes the gentleman from Florida, Mr. Bilirakis, 5 minutes for your questions.

Mr. {Bilirakis.} Thank you, Mr. Chairman. I appreciate it very much, and again, thanks for holding this very important hearing, and I really thank the panel as well. This is so important to our consumers.

Consumers must be able to trust that information they provide. They want to make sure that it is safe. They provide the information to retailers, and the digital world where sales are increasing on line, such as--you know, this trust is vital to our economy. However, I do not believe such trust will be preserved by the current patchwork of laws. We need a stable law that ensures merchants are

appropriately protecting consumers without sacrificing prosperity.

The first question is for Mr. Dodge. You mentioned in your testimony the benefits of the chip and PIN that we are transitioning to nationwide. However, my understanding is that a potential weakness exists for online transactions because the payment card is not actually present. Doesn't that mean that this technology and every other technology can be made obsolete by criminals that quickly adapt to new technologies? It seems to me that we need to ensure that what we pass into law meets the threat and is not prescriptive of one type of technology? Do you agree and what do you recommend?

Mr. {Dodge.} So just a couple of points first, specifically chip and PIN is not scheduled to be rolled out later this year. This has been a major point of tension between the merchant community and the financial services community because the expectation is the chip only is coming out. Chip and PIN has been in place around the world for many, many years and has been proven to dramatically reduce fraud. Retailers have argued for a very long time that we should be moving to this technology as quickly as possible because of its proven fraud protection and because in the context of today's hearing, that it has an important effect

and devaluing the data that businesses hold. So the information that flows through a retailers system, at the point of sale, would be rendered useless to criminals if they were able to captured, if you use the chip and PIN system. We think it is absolutely critical.

To your point about evolving technologies, that is absolutely true. It is the best technology. Chip and PIN is the best technology that is available today, and we are years behind the rest of the world in catching up to it. And as a result, we are behind. When chip and PIN was introduced in Europe, we saw fraud flow in two directions, online in Europe to you point and to the United States because it became the lowest common denominator.

As for long-term solutions, we believe the chip and PIN serves a near-term need, and we need to evolve to next generation because as you suggest, the world is moving online. E-commerce is booming on line.

Mr. {Bilirakis.} Thank you very much. The next question is for the entire panel. Some of the recent data breaches were caused by third parties, such as contractors. What recommendations would you make if any to address when these situations occur? We will start over here, if that is okay with Ms. Hyman.

Ms. {Hyman.} Well, first of all, with regard to third

parties, again, many of our member companies are solution providers, those third parties that you may be talking about. Human error continues to be one of the greatest causes of data breach, and I think doing best practices for the industry and for all companies involved on how to mitigate some of those human errors is very important. Education, ongoing efforts, we have an IT trust mark, security trust mark, which is a benchmark for an organization to undertake appropriate practices for data security. So all of these pieces come into play, but having a standard for data breach notification also puts everybody on notice about what the consumer needs to know in a timely and actionable way.

Mr. {Bilirakis.} Mr. Dodge?

Mr. {Dodge.} The questions about third-party--

Mr. {Bilirakis.} The third party, with regard to third parties, correct.

Mr. {Dodge.} Yeah. So we think that it is important. It is important incentive that the breached entity be obligated to make the notice, but flexibility should exist for parties to contractually determine in the instance of a breach who should issue the notice.

Mr. {Bilirakis.} Thank you. Yes, ma'am.

Ms. {Barrett-Glasgow.} As a vendor, we see lots of increasing requirements from our clients to not only adhere

to security standards but to have indemnification if a breach occurs in our environment of the data that we are holding and processing for them.

Mr. {Bilirakis.} Thank you. Mr. Hartzog?

Mr. {Hartzog.} My recommendation would be maybe, if there is even a possible compromise here, which is if breached entities have no relationship to the consumer whose data they hold. Then perhaps there could be some kind of requirement where you would have to disclose the relationship to the--say we got this information from an entity that collected your personal information which is why you don't recognize us. But we were breached. So that could be one way to handle that.

Mr. {Bilirakis.} Okay, Mr. Chairman. I actually have one more question if you--

Mr. {Burgess.} Ask unanimous consent that the gentleman be able to ask his question. Without objection, so ordered.

Mr. {Bilirakis.} Thank you.

Mr. {Burgess.} It is an immense power that I wield here, Gus.

Mr. {Bilirakis.} Okay, for the panel again, keeping in mind the touchstone of this process is notifying an individual in the event that they need to mitigate the economic risks associated with a breach, which entity is in

the best position to notify individuals after a breach? Is there a reason to deviate from the structure that the States have used? And we will start with Ms. Hyman, please.

Ms. {Hyman.} Are you asking in terms of who is responsible for the notification or which enforcement agency?

Mr. {Bilirakis.} Who would be responsible for the notification.

Ms. {Hyman.} We want to make sure that we are, again, not over-notification or confusing the consumer. So that entity with which they have provided their information to that would have done the transaction would be the first source. Then contractually--and I come back to the previous question about third parties. There are contractual relationships beyond that.

Mr. {Bilirakis.} Again, with regard to the States, how would you--

Ms. {Hyman.} We said that the State Attorneys General should have enforcement opportunities. If it is also the FTC that is undertaking enforcement, one should extinguish the other. They should not happen simultaneously.

Mr. {Bilirakis.} Very good. I am sorry. I am having a little trouble hearing. I apologize. Mr. Dodge, please.

Mr. {Dodge.} Sure. We strongly believe that the obligation to notify should be with the breached entity and

then again, flexibility among parties to contractually determine who sends the notification, if it makes more sense for somebody else to send it. And we agree the State Attorneys General have an important role to play in this.

Mr. {Bilirakis.} Very good. Thank you. Please.

Ms. {Barrett-Glasgow.} In the interest of time, I will agree.

Mr. {Bilirakis.} Okay. Very good.

Mr. {Hartzog.} And I would agree that the current trajectory of the State law is what I would recommend.

Mr. {Bilirakis.} Thank you very much. I appreciate it. I yield back, Mr. Chairman. Thanks for allowing me to ask that last question.

Mr. {Burgess.} The chair thanks the gentleman. The gentleman does yield back. Seeing no further members wishing to ask questions, I would like to thank the witnesses and members for their participation in today's hearing. Before we conclude, I would like to include the following documents to be submitted for the record by unanimous consent: a letter on behalf of the Consumer Electronics Association; a letter on behalf of the Direct Marketing Association; a joint letter on behalf of the American Bankers Association, the Consumer Bankers Association, the Credit Union National Association, Financial Services Roundtable, Independent

Community Bankers Association, the National Association of Federal Credit Unions; an additional letter on behalf of the Marketing Research Association; a letter on behalf of the National Retail Federation; a letter on behalf of the National Association of Federal Credit Unions; a joint letter on behalf of the Consumer Data Industry Association, the Interactive Advertising Bureau, the National Business Coalition on E-Commerce and Privacy, and the National Retail Federation, the United States Chamber of Commerce; and a joint statement for the record on behalf of the National Association of Convenience Stores and the Society of Independent Gasoline Marketers of America.

Pursuant to committee rules, I remind members that they have 10 business days to submit additional questions for the record, and I ask the witnesses submit their response within 10 business days upon receipt of the questions.

Without objection, all of the statements are entered into the record.

[The information follows:]

********** COMMITTEE INSERT **********

|

Mr. {Burgess.} And without objection the subcommittee is adjourned.

[Whereupon, at 12:47 p.m., the Subcommittee was adjourned.]