{York Stenographic Services, Inc.}

RPTS BROWN

HIF077.170

DISCUSSION DRAFT OF H.R. _____, THE DATA SECURITY AND BREACH NOTIFICATION ACT OF 2015

WEDNESDAY, MARCH 18, 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 10:02 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, Olson, Pompeo, Kinzinger, Bilirakis, Brooks, Mullin, Upton (ex officio), Schakowsky, Clarke, Kennedy, Cardenas, Rush, Butterfield, Welch, and Pallone (ex officio).

Also present: Representative McNerney.

Staff present: Charlotte Baker, Deputy Communications Director; Leighton Brown, Press Assistant; Karen Christian, General Counsel; James Decker, Policy Coordinator, Commerce, Manufacturing, and Trade; Graham Dufault, Counsel, Commerce, Manufacturing, and Trade; Melissa Froelich, Counsel, Commerce, Manufacturing, and Trade; Howard Kirby, Legislative Clerk; Paul Nagle, Chief Counsel, Commerce, Manufacturing, and Trade; Olivia Trusty, Professional Staff, Commerce, Manufacturing, and Trade; Michelle Ash, Democratic Chief Counsel, Commerce, Manufacturing, and Trade; Christine Brennan, Democratic Press Secretary; Jeff Carroll, Democratic Staff Director; David Goldman, Democratic Chief Counsel, Communications and Technology; Lisa Goldman, Democratic Counsel; Brendan Hennessey, Democratic Policy and Research Advisor; and Tim Robinson, Democratic Chief Counsel.

Mr. {Burgess.} Chair will recognize himself for the purpose of a 5-minute opening statement. Again, welcome. Today's legislative hearing is the first concrete step for this Subcommittee toward the goal of a single Federal standard on data security and breach notification. In January we heard testimony about the key elements of sound data security and breach notification. I am pleased that so many of the elements discussed at that hearing have been incorporated into the draft legislation.

I also know, and I am aware of, that we just had another data breach that was in the news. I hope that the Committee looks at health care data. Health care data has its own set of policy issues, where, if sharing data is done properly, could have tremendous public benefits and save lives, but there is already law in this area under HIPAA, and taking on health care privacy data in this bill I feel would delay the consumer benefits that we can provide under this draft.

I am very encouraged by the bipartisan approach and commitment shown by my colleagues, Vice Chairman and full Committee Congress--the Vice Chairman of the full Committee, Congressman Blackburn, and Congressman Welch, announcing this draft legislation. This Subcommittee has a history of bipartisan cooperation with the work of Congressman Barton

and Congressman Rush, that they have put a lot into this issue over the years. I am encouraged that this may be the year that we find the paths forward.

The issue of data breach has been before this Subcommittee for a decade, and it is in reference to that that this is such important work. I would just acknowledge the work of previous subcommittee Chairs on both sides of the dais who have worked in this space. Chairman Bono Mack is here with us in the audience this morning. I heard from former Chairman Terry yesterday in the--on the eve of starting this hearing. And certain Chairman Rush, when I was in the minority and on this subcommittee, I know put in a lot of work.

But all the while that we have been working, cybercriminals have continued their operations. They steal, they monetize an individual's personal information, all of that being done in the absence of any national data security requirement. Even today the great majority of states do not have a data security requirement. 10 years in, we do have greater insight into what cybercriminals are doing, and the impact of their activities. Conservative estimates put cybercrime cost to the consumers at $100 billion annually, and cybercrime is estimated to cost the United States economy over a half million jobs each year.

The Secret Service tells us that data breaches are primarily monetized through financial fraud. On average, a third of data breach notification recipients became the victims of identity fraud in 2013, compared with a quarter in 2012, clearly increasing. On a more personal level, individuals are hit twice when there is a data breach. First they need to understand which of their accounts they need to reset, if they need new bank cards, or if they need to freeze their credit report. Luckily, there are many laws to help navigate the process.

Second, the cost across the ecosystem is $100 billion annually, and that is eventually passed on to the consumer in the form of higher fees and prices. The existing patchwork of state laws on data security and breach notification do not seem to have been effective. The noted security blogger Brian Krebs posted an article this week about the new criminal tools to steal customers' payment information, and he ended it with a simple question, are online merchants ready for the coming e-commerce fraud wave? The draft legislation before us this morning addresses this question with both a security requirement for personal information that leads to identity theft and payment fraud, and a breach notification for consumers so consumers can protect themselves.

Some will complain about what is not in the bill. If we actually want to pass legislation, it will be impossible to proof it against what can happen in the future. We cannot shade into areas such as privacy. The--this Administration, and our minority colleagues, over the past 6 years have worked on this, and still can't agree on how to address privacy, and I just want to be very clear on that topic. While we don't tackle privacy in this legislation, we don't preempt it either. This bill is focused on unauthorized access that leads to identity theft and financial fraud. It has nothing to do with permitted access, or when that permission can be given, or what data can be collected. I will also say that Congress must continue to address privacy of all kinds, but not at the price of delaying consumer protections for data security and breach notification.

Another complaint will be around moving the telecommunications, cable, and satellite providers from the Federal Communications Commission to the Federal Trade Commission. I look forward to hearing which agency has been more active--the more active consumer watchdog regarding data security and breach notification in the last 10 years.

I certainly do look forward to continuing the bipartisan good faith negotiations with all interested stakeholders. Negotiation remains open and ongoing, and, of course, the

doors of the Subcommittee are always open.

[The prepared statement of Mr. Burgess follows:]

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

|

Mr. {Burgess.} With that, I would like to recognize the ranking member of the Subcommittee, Ms. Schakowsky, 5 minutes for an opening statement.

Ms. {Schakowsky.} Thank you, Mr. Chairman. I appreciate the hearing today on the draft legislation released last week, and--by Mr. Welch and Ms. Blackburn to require data breach security and reporting. I do appreciate my colleagues' efforts on this legislation, and I agree that there are some positive elements, FTC penalty authority and a data security provision among them.

That said, however, this bill does need significant amendments to achieve the goal of both simplifying compliance for business, and enhancing protections for consumers. I don't believe that goal is out of reach. I don't think that it expands the time that it will take. Maybe by just a bit, but the draft proposal would--has these problems, in my view. It would prevent states from enforcing their own laws related to data security and breach notification. It prevents all private rights of action on data breach and notification. As currently drafted, it would override all common law, including tort and contract law, as they apply to data. Those provisions would leave consumers with fewer protections than they currently have.

This proposal also weakens existing consumer protections under the Communications Act for customers of telecommunications, satellite, and cable companies. And while I believe the FTC can, and should, be empowered to play a stronger role in protecting consumers' data, I don't believe that should come at a cost of eliminating existing FCC protections. The bill would also only require consumers to be notified of a breach if it is determined that a breach has, or will, likely lead to financial harm. That would only occur after the companies regulated under this bill have concluded investigations of breaches to determine the risk of financial harm to each of their customers or users, a process that could take months.

There are many types of harm that go beyond simply financial ones. For example, a data breach that revealed private communication might not have any measurable financial impact, but could cause embarrassment, or even danger. The types of personal information covered by this bill are far too limited. The bill doesn't cover over the counter drug purchases, or other health information not covered by HIPAA. By contrast, the data laws in Texas and Florida protect those types of information. The bill does not cover metadata, which can be used to acquire sensitive personal information. The bill also does not provide FTC rulemaking authority for

defining personal information. This is a major weakness when we have seen the nature of personal information change significantly over time. For example, when the House passed the Data Act in 2009, it did not include geolocation information as part of personal information. Today I think we could all agree that geolocation information should be protected, and that is why we need legislation that allows the FTC to adapt as the nature of personal information continues to evolve. Of course we can't anticipate everything, but we could create some flexibility.

In closing, this bill is very broad, in terms of preemption of state and other Federal laws, and narrow in terms of definitions of harm and personal information. I believe the bill should be narrow where it is now broad, and broad where it is now narrow. I look forward to hearing from our witnesses about their perspectives on this bill, and to moving forward with a strong bill that adequately protects consumers.

With that, I yield the remainder of my time to Mr. Kennedy.

[The prepared statement of Ms. Schakowsky follows:]

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

|

Mr. {Kennedy.} Thank you very much to my colleague, and thank you for--my colleagues on both sides of the aisle for their efforts in pulling this bill together. It is always nice to see a Bay Stater here to testify before the Committee, so I just wanted to give a warm welcome to Sara Cable, Massachusetts Assistant Attorney General with the Consumer Protection Division. Ms. Cable investigates and prosecutes violations of the Massachusetts Consumer Protections Act and the Massachusetts data notification laws and data security regulations. I have no doubt that the work that Ms. Cable does in enforcing Massachusetts data breach laws has protected many across the Commonwealth, and I truly appreciate her being willing to be here today and take some time to share her thoughts and expertise with us about an incredibly important issue.

And with that, Ms. Schakowsky, I will yield back. Thank you.

[The prepared statement of Mr. Kennedy follows:]

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

|

Mr. {Burgess.} Chair thanks the gentlelady. Gentlelady yields back. The Chair now recognizes the Chairman of the full Committee, Mr. Upton, 5 minutes for an opening statement.

The {Chairman.} Well, thank you. We are at a critical point for consumer protection in the U.S. Our interconnected economy, with many great benefits, also poses new threats from thieves, new challenges to information security, that is for sure. And as the Internet weaves itself into the DNA of appliances, cars, clothing, the threats of exploitation multiply, but the most serious underlying criminal purpose remains the same, to steal and monetize personal information, and it has to be stopped.

As data breaches have evolved, the one constant is that identity theft and payment card fraud are the crimes that pay the criminals. According to the Bureau of Justice Statistics, personal identity theft costs our economy nearly $25 billion in ’12, making it the largest threat to personal property today. There is not a single member of this Committee who doesn’t represent someone who has suffered either identity theft or payment fraud.

This bipartisan draft legislation that we consider today establishes a reasonable national security standard, with

flexibility to adapt to changing security technology. The FTC and the State Attorney Generals will be policing companies to hold them accountable for protecting consumers. The draft also focuses on the personal information that criminals have targeted, the cyber gold that attracts today's cyber safecrackers. I want to thank my colleagues Blackburn and Welch for bringing us a big step closer to a bipartisan solution. Other members of the Committee, including Mr. Barton and Rush, have also rolled up their legislative sleeves over the years. And I want to thank Chairman Burgess for making this issue a very top priority on this Subcommittee.

I also commend the narrow approach. By targeting the most sought after personal information in the areas lacking current Federal protections, this bill avoids controversial issues that have derailed past efforts. Our goal is to create clear requirements to secure personal information from, and notify consumers in cases of unauthorized access. The goal is not to broadly regulate the use of data.

I yield the balance of my time to Ms. Blackburn.

[The prepared statement of Mr. Upton follows:]

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

|

Mrs. {Blackburn.} I thank the Chairman for yielding, and I also want to recognize the previous Chairman of this Committee, Ms. Bono, with us today, who have worked so diligently on this issue through the years. I appreciate the guidance and the leadership there. I also want to commend Mr. Welch, who has been co-Chairman of the Privacy Working Group, and the Chairman for allowing the Privacy Working Group a full 2 years to dig into this issue, and to see where we could find agreement. And that is the basis of the draft legislation that we have before us today.

The reason it is important that we do something now is because 2014 was dubbed the year of the breach. Think about the number of breaches that were out there. Our constituents have begun to see this firsthand. It has affected someone in nearly every family. And what they are saying is the issue is getting out of control, and we need to take steps to put the guidance in place so that individuals will know they have the tools that are necessary to protect their data, and, as I say, their virtual you, their presence online.

And I appreciate Mr. Welch and the work he and the Privacy Working Group did to help us come to this point, and I yield the balance of my time to the gentleman from Vermont.

[The prepared statement of Mrs. Blackburn follows:]

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

|

Mr. {Welch.} Congress hasn't been doing its job. We need to pass legislation that is going to deal with this incredible problem. You know, since 2005 a billion consumer records have been hacked into. The current status right now, we have got states trying to do something. 47 different state laws on notice, 12 state laws on data security, but we don't have any national standard, and we don't have any legislative authority for the FTC, or really, for that matter, the FCC to do much, so we have to act and let there be a cop on the beat to protect people.

What this bill does--and this is a discussion draft, and I appreciate the back and forth, but we are going to have to have Mr. Pallone and Ms. Schakowsky very much involved as we go forward. What this does, it gives--it is a narrow bill. In my view, that is smart, because we have got to solve a problem. It gives the FTC explicit statutory authority, and that is being litigated in the Wyndham Hotels case. They can impose robust civil penalties. That is good. It does preempt states, but it doesn't limit the states with respect the states, but it doesn't limit states on privacy issues, where they want to continue having legislative interaction.

This bill does not do some things that would be controversial that are debatable, but should not be part of

this, because it will weigh it down. It is not a privacy bill. The states have continued authority in that space. It is not a bill about net neutrality. Big debate on this panel about the recent order. I happen to support it. Many of my colleagues don't. This bill is not about that. This bill is not about the common law right of action under tort law. Again, a debate here, but not something that we want to weigh this bill down.

Mr. Chairman, I appreciate the focus, the narrow focus on this. I appreciate Jan Schakowsky, the opportunity you gave me to work with the Privacy Group, and I implore all of my colleagues here to keep this going. We had good input from all of the affected parties, the FTC, the FCC consumer groups. We have got to get something done, and we have got an opportunity in this Committee to do it. I hope we can all be part of that.

I yield back.

[The prepared statement of Mr. Welch follows:]

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

|

Mr. {Burgess.} Chair thanks the gentlemen, gentleman yields back. The Chair recognizes the Ranking Member of the full Committee, Mr. Pallone, 5 minutes for an opening statement.

Mr. {Pallone.} Thank you, Chairman Burgess. Today we are discussing a draft data security and breach notification bill released recently by the majority. Data breaches are a plague on consumers, businesses, and our economy as a whole. Reducing the incidences of breaches, and the adverse effects from them, has rightfully been at the top of our agenda since 2005, yet it also has proven to be a complicated issue, without an easy legislative solution. I appreciate the efforts being taken to address the data breach problem, and I appreciate the difficulty of writing legislation that effectively protects consumers and lessens the burdens on the businesses that are victims of criminal breaches.

And while the sincerity of the efforts are not questioned, I do question the merits of the bill before us today. The bill simply does not strike the right balance. There are clearly benefits to creating a unified system for breach notification, but we must be careful that a Federal law ensures that protections for consumers are not being weakened. Many of the 51 state and territorial breach

notification laws provide greater protections for consumers whose personal information is at risk as a result of data breach. For example, at least seven states and D.C. do not require a harm analysis before providing notice to consumers. At least 17 state laws also include a private cause of action. At least nine states' laws cover health information.

In contrast, the draft under discussion today preempts stronger state and Federal laws, requires a financial harm analysis, preempts state private rights of action, and does not cover health or location information. Data breach notification is only part of the solution. The other crucial piece of any legislation should be baseline data security to help prevent breaches before consumers' personal information is put at risk. The draft before us eliminates state data security laws and replaces them with an unclear standard that will surely be litigated and left to judicial interpretation.

As I said at a hearing this past January, I want to be supportive of sound data security and breach notification legislation, but to get there we must ask the right question. The question is not whether any one Federal agency would be better off. The question must always be whether legislation puts consumers in a better place than they are today. And, unfortunately, the draft before us today does not put consumers in a better place, in my opinion.

So before I close, I have to raise a process issue. We received the draft bill last Thursday evening. The 114th Congress seems to have halted a long tradition of sharing text with all members of the subcommittee at least a full week prior to a legislative hearing, and this is not the first time this has happened this year in the Energy and Commerce Committee, as we saw with our Communications Subcommittee. I suspect it is not going to be the last.

Also, I have to take issue--I know this may sound, you know, a little picky, but I have to take issue with Chairman Burgess's opening remarks, and repeat my longstanding belief that having some Democratic support does not make a measure bipartisan. I think that Chairman Upton used better language when he said maybe it is a step closer to being bipartisan. And I appreciate what Mr. Welch said, which is that--he mentioned having the support of myself and Ms. Schakowsky on a bill. I would like to see this bill improved before it moves further through the legislative process so that all members of the Committee can support it, and it can be a truly bipartisan legislative product, which it is not at this time.

I have some time left. I don't know if--did you want additional time? Are you--all right. Yvette, or--everybody is okay? All right. Thank you, Mr. Chairman. I will yield

back the balance of my time.

[The prepared statement of Mr. Pallone follows:]

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

|

Mr. {Burgess.} Gentleman yields back. His observation is noted. I do want to welcome all of our witnesses, and thank you for agreeing to testify before the Committee--Subcommittee today. Today's hearing will consist of two panels. Each panel of witnesses will have the opportunity to give an opening statement, followed by a round of questions from our members. Once we conclude with questions for the first panel, we will take a brief break to set up for the second panel.

For our first panel today, we have the following witnesses. Ms. Jessica Rich, Director of the Bureau of Consumer Protection at the Federal Trade Commission, and Mr. Clete Johnson, the Chief Counsel for Cybersecurity, Public Safety, and Homeland Security at the Federal Communications Commission. Thank you for your participation today. Ms. Rich, you are recognized for 5 minutes for the purpose of an opening statement.

|
^STATEMENTS OF THE HONORABLE JESSICA RICH, DIRECTOR, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION; AND CLETE JOHNSON, CHIEF COUNSEL FOR CYBERSECURITY, PUBLIC SAFETY AND HOMELAND SECURITY BUREAU, FEDERAL COMMUNICATIONS COMMISSION
|
^STATEMENT OF JESSICA RICH

} Ms. {Rich.} Dr. Burgess, Ranking Member Schakowsky, and members of the Subcommittee, I am Jessica Rich, Director of the Bureau of Consumer Protection at the Federal Trade Commission. I appreciate the opportunity to present the Commission's testimony on the Subcommittee's data security legislation.

Reports of data breaches affecting millions of Americans fill the headlines. These breaches involved not just financial data, but other types of sensitive data, such as medical information, account credentials, and even the contents of private e-mails. These events serve as a constant reminder that consumers' data is at risk. Hackers and others seek to exploit vulnerabilities, obtain consumers' sensitive information, and misuse it in ways that can cause serious harms to consumers and businesses. Indeed, identity theft continues to be the FTC's number one source of consumer

complaints, and data shows that over 16 million consumers were victimized in 2012 alone.

Every year new incidents are reported that re-ignite concern about data security, as well as debate about the best way to provide it. Companies must implement strong data security measures to minimize consumers' risk of fraud, identity theft, and other substantial harm. Poor data security practices also creates risks for businesses. Data breaches can harm a company's financial interest and reputation, and also result in the loss of consumer trust. We need strong legislation now for consumers and the health of the commercial marketplace.

As the Nation's consumer protection agency, the FTC is committed to protecting consumer privacy and promoting data security in the public sector--private sector, excuse me. The FTC would like to thank the Subcommittee for proposing enactment of Federal data security and breach notification law, which the Commission has long supported on a bipartisan basis.

The Commission supports a number of elements in the proposed legislation which will give us additional tools to deter unlawful conduct. First, the bill includes a provision requiring companies to implement reasonable data security standards in addition to breach notification, both of which

are essential to protect consumers. Second, the legislation gives the FTC jurisdiction to bring cases against non-profits and common carriers. Third, the bill provides for civil penalties, which are important to ensure adequate deterrents.

However, other aspects of the draft legislation don't provide the strong protections needed to combat data breaches, identity theft, and other substantial consumer harms. First, the bill does not cover precise geolocation and health data, even though misuse of this and other information can cause real harm to consumers, and even though a lot of health information is not, in fact, covered by HIPAA. For example, we brought a case last year against a medical transcription company whose lax security practice resulted in psychiatrists' notes about individual patients being made available on the Internet, available through simple Google searches. Given the definition of personal information in this bill, we would not be able to rely on the legislation to bring that case and seek civil penalties.

In addition to companies being careless with consumer information, hackers have incentives to obtain this data, even when it is not financial. For example, in some of our recent investigations, we have seen bad actors hack into company systems to steal consumers' information so they can extract payments from the companies for its return. A number

of state laws currently protect consumers' health information, but those protections would be preempted under the bill.

Second, the Commission believes that data security protection should apply to devices that collect data, such as some Internet-enable devices. Breaches involving these devices raise broader safety concerns, even if no data is stolen. For example, if a pacemaker isn't properly secured, a breach could result in serious harm to the person using it. Similarly, a malicious criminal who hacks into a car's network could disable its brakes, and other safety features.

Third, the FTC continues to believe that data security and breach legislation should include rulemaking authority under the Administrative Procedures Act. Rulemaking would allow the Commission to ensure that, as technology changes, and the risks from the use of certain types of information evolve, the law keeps pace, and consumers are adequately protected.

Finally, the FTC believes that any trigger for providing notification should be sufficiently balanced so that consumers can protect themselves when their data is at risk without experiencing over-notification. Accordingly, we support an approach that requires notice, unless a company can establish that there is no reasonable likelihood of

economic, physical, or other substantial harm.

Thank you very much for this opportunity to provide the Commission's views. The FTC remains committed to promoting reasonable security for consumer data, and stands ready to work with the Subcommittee as it develops and considers legislation to protect consumers' sensitive information.

[The prepared statement of Ms. Rich follows:]

********** INSERT A **********

|

Mr. {Burgess.} The Chair thanks the gentlelady. Mr. Johnson, you are recognized for 5 minutes for the purpose of an opening statement.

|

^STATEMENT OF CLETE JOHNSON

} Mr. {Johnson.} Thank you very much. Dr. Burgess, Ranking Member Schakowsky, leaders of the full Committee, distinguished members, thank you very much for having--for providing the opportunity to discuss the FCC's current programs and authorities regarding consumer protections for communications data, privacy, security, and breach notification. For decades Congress has recognized that information related to consumers' use of communications services is especially sensitive for reasons that go beyond potential economic harm, such as financial fraud or identity theft. If Americans can't communicate privately, if we are not secure in the privacy of information about our communications, then we can't fully exercise the freedoms and rights of open democratic society. As with medical and health data--health care data, governed under HIPAA, and financial data, governed under Gramm-Leach-Bliley, and other statutes, Congress has long treated communications-related consumer information as a special category of consumer data that calls for expert oversight, tailored protections, and specific enforcement.

Given recent developments, the privacy and security of

sensitive information held by communications networks is actually a much bigger issue now than ever before. For example, public concerns about the availability of telephone call records, the widespread use of fixed and mobile broadband communications, privacy implications of crucial life-saving improvements to next generation 911, and finally, recent cyberattacks, such as the one aimed at suppressing the release and viewing of a motion picture. As the expert agency that regulates communications networks, we continually seek to improve these protections for the good of communications consumers. I will now turn to the legal framework currently in place to protect these communications consumers, and also the responsibilities of communications providers to secure their networks in the first place. The draft bill would alter this legal framework significantly, and would leave gaps, as compared to existing consumer protections for communications consumers.

First, Section 222 of the Act establishes a duty for telecommunications carriers and interconnected VOIP providers to protect the confidentiality of consumers' proprietary information, including call records, location information, and other information related to the telephone service, such as the features of the customer's service, or even the customer's financial status. FCC rules under Section 222

require carriers to notify law enforcement and consumers of breaches, and carriers that fail to meet these requirements are subject to an enforcement action.

Second, Sections 631 and 338(i) apply to cable and satellite TV providers, and they protect consumers' viewing history. That is the TV shows they watch, and the movies that they order, as well as any other personally identifiable information available to the service provider. Here too the--these protections are enforced by FCC enforcement activity. And I would note that many of these protections, including those protections for several particular types of proprietary information, would no longer exist under the draft bill.

If enacted, Section 6(c) of the draft bill would declare sections of the Communications Act, as they pertain to data security and breach notification, to ``have no force or effect'', except with regard to 911 calls. The Federal Trade Commission would be granted some, but not all, elements of the consumer protection authority that the FCC presently exercises. For example, if the draft bill were to become law, the FTC would not have the authority to develop rules to protect the security of consumers' data, or to update requirements as new security threats emerge, and technology evolves.

Finally, while the draft bill attempts to maintain the

protections of the Communications Act for purposes other than data security, the FCC's experience implementing privacy and security requirements for communications consumer data shows that there is no simple distinction between these two interrelated concepts, privacy and security. Whether a company, number one, either by human or--human error or technical glitch, mistakenly fails to secure customer data, or, number two, if it deliberately divulges or uses information in ways that violated consumer privacy regarding that data, that--the transgression is at once a privacy violation and a security breach. In many cases it is the very same thing, and they--there--it is very difficult, practically or legally, to separate the two.

I thank you again for the opportunity to provide a summary of the FCC's programs regarding data privacy and security, and, of course, look forward to answering any questions the Subcommittee may have. We at the FCC, of course, stand ready, and willing, and able to provide any input or assistance the Subcommittee may request as it completes this important work. Thank you very much.

[The prepared statement of Mr. Johnson follows:]

********** INSERT B **********

|

Mr. {Burgess.} Chair thanks both the witnesses for their forthright testimony. We will now go to the questioning portion of the hearing. I will recognize myself for 5 minutes for the purposes of questions.

Let me ask the same question to both of you. First, for the Federal Trade Commission, how many data security cases has the Federal Trade Commission brought to date? And, as a corollary, do you have an idea as to how many investigative hours have been spent on data security cases?

Ms. {Rich.} We have brought 55 data security cases, that is since the early 2000s, but we have actually brought hundreds of, combined, privacy and data security cases, held 35 workshops, completed 50 reports. We have spent--I actually haven't tabulated up man hours, but it is an enormous amount, because for every case we bring, there are actually quite a number of investigations that we look into, but we decide not to bring a Federal court action. So it is millions of hours.

Mr. {Burgess.} Okay, but the total cases was 55, was your response?

Ms. {Rich.} In the data security area, but many of the privacy cases have some data security element too, and there are hundreds of those.

Mr. {Burgess.} Very well. Mr. Johnson, let me just ask the same question to you. How many data security cases has the Federal Communications Commission brought, and then, likewise, the investigative hours that you have--that your commission has spent on the data security cases?

Mr. {Johnson.} Thank you, Mr. Chairman. In the 18 years that Section 222 has been in place, and this is the section that pertains to--primarily to telephone call records, there have been--I don't have the precise number, but I think it is in the realm of scores and scores of cases that pertain to what is called customer proprietary network information. This is call records, location information, time and duration of call, and a whole host of other what is called CPNI protections. I don't have the precise number, and I can certainly get you the precise number, nor the total accumulated hours, but it is scores and scores.

Mr. {Burgess.} To the extent--I think it would be helpful to the Subcommittee if you could make the actual numbers available, and certainly--

Mr. {Johnson.} Of course.

Mr. {Burgess.} --I would allow you to do that for the record. Let me just ask you a question. You brought up the Consumer Proprietary Network Information. How many years after the 1996 Act did it take to fully implement the rules

for CPNI at the Federal Communications Commission?

Mr. {Johnson.} Well, I think that that--I don't know the--which exact rule you are referring to, Mr. Chairman, but there--I think the broad answer is that it is a--it has been underway for 18 years, and there have been multiple improvements and shifts, including for Congressional expectation, technological development, for instance, voice over IP, location information Ms.--that is--pertains to 911. And in 2013 there was a declaratory ruling that the Commission declared that CPNI pertains to information that is collected on mobile devices.

So I guess the accurate answer is that it is--it remains a work in progress, and that is part of the value of having that rulemaking authority, is in order to adapt to Congressional expectations, changes of technology.

Mr. {Burgess.} Maybe for the purposes of clarification for the Subcommittee, as we work through some of these issues, could the Commission provide us a timeline, from 1996 to present, where the rulemaking was involved, where it evolved? Obviously the threat changed over that time as well. But I am--I guess, you know, that is part of my concern, is that it--I get the impression that it took some time from '96 to the point where the rulemaking had evolved to a point where there were actually consumer protections

that were available. But I don't know that, and you are--

Mr. {Johnson.} Absolutely. I will take that--I think that is a very important homework assignment for me, and I--run through very briefly--the section was established in 1996.

Mr. {Burgess.} Right.

Mr. {Johnson.} In 1999 location information was added. In 2007 there was a major problem with what is called pre-texters. And in my old world in--working on intelligence policy, this is essentially a human intelligence collector, where pre-texters would call the telephone company, ask--

Mr. {Burgess.} Right. We had a hearing on it here in this Committee several years ago as well.

Mr. {Johnson.} And so that was something, again, that was at once a privacy and security issue, and in 2007 the Commission issued rules specific to solving that problem. And, again, there have been some other adjustments and improvements in recent years. But we will get you the full story. It is actually--it is--it is an important story about the development of Section 222.

Mr. {Burgess.} The Chair appreciates the gentleman's willingness to provide the information. The Chair recognizes Ms. Schakowsky. Five minutes for questions, please.

Ms. {Schakowsky.} I just want to clarify that my

concerns between the agencies is really with regard to the impact on consumers. I don't want anything I say to seem to reflect a preference for one agency over another, but rather for the protection of the consumers.

So my--if this draft were enacted, regulatory and enforcement authority over data security and breach notification that is currently granted to the FCC would--under certain sections of the Communications Act and its regulations would have no force or effect. It is my understanding that the data security and breach notification protections under the Communications Act are broader than the protections afforded under this draft. The Communications Act provides security protections for information regarding telecommunications subscribers' use of service, but this draft does not provide security protections for all of that information. Instead, it covers only ``the location of, number from which, and to which a call is placed, and the time and duration of such call''.

So, Mr. Johnson, what other information is currently protected under Title II of the Communications Act that would not be covered under this draft?

Mr. {Johnson.} Ma'am, you are correct it--that there are specific pieces of information, both under Section 222 and also the cable/satellite provisions, that are not

protected under this draft. With regard to Section 222, information such as how many calls a person has made, you know, sort of the peak calling periods for that person, does this person make phone calls in the morning, at night, lunchtime, specific features of the service, like call waiting, caller ID, and then other things that may be pertinent to call service, like this--like the financial status of the customer. Is the customer--does the customer qualify for Medicaid, or SNAP, or other low income support? Those would explicitly not be protected by the definition in the draft bill.

On the cable and satellite side, it is--essentially all of it would not be protected. What television shows you watch on cable and satellite, what pay-per-view you order, what you order from the Home Shopping Network, none of this would be protected under the draft bill, and it is--

Ms. {Schakowsky.} So--

Mr. {Johnson.} --presently protected.

Ms. {Schakowsky.} So viewing preferences, or viewing history, none of that would be covered?

Mr. {Johnson.} It is presently covered. It would not be covered under the draft bill.

Ms. {Schakowsky.} No, that is what I am talking about. This bill also voids breach notification obligations required

under the Communications Act, Mr. Johnson, and its regulations, but as I read it, the bill would not require breach notification for a breach of call information. Under the Communications Act, and associated regulations, a breach of customer information, such as call data and viewing habits, requires notice to law enforcement and affected customers. Is that right?

Mr. {Johnson.} That is correct.

Ms. {Schakowsky.} But as we established, much of the customer information currently required to be secured under the Communications Act does not have to be secured under this bill. And if there is no requirement to protect the information, then there is no requirement to provide notice in the event of a breach, correct?

Mr. {Johnson.} That is correct.

Ms. {Schakowsky.} And even for the limited call information that must be secured under this bill, a breached company would not be required to provide notice because call information is not financial in nature, do you agree?

Mr. {Johnson.} That is my interpretation, yes, ma'am.

Ms. {Schakowsky.} So I wondered, Ms. Rich, if you wanted to comment on that. This is a concern that I have for consumers, that I think if we allowed the FCC to continue in its regulations, that we could then make sure we cover

everything.

Ms. {Rich.} We--for consumers--we are also looking at this bill in terms of its effect on consumers, and that is why, in our testimony, we have proposed that the bill apply to more information, geo, health. Communications would also be something that should be added to the bill. We also believe the breach notification trigger should be a bit broader to encompass different harms. So that, we agree, would be an improvement to the bill.

But I--as to jurisdiction, I should say that our position is that we should have jurisdiction in this bill. The FTC should have jurisdiction over carriers in this bill because we have brought so many cases in this area. We bring so much enforcement expertise to the table. We really have been working on this issue since, really, the mid ‘90s. We also believe we should be able to hold different companies that are collecting some of the very same type of information to the same standards on--in our enforcement. You know, Netflix, Google, and Verizon really have a lot of the same information.

And, further, the--we haven’t taken a position on reclassification, but one byproduct of reclassification is it does remove our FTC jurisdiction from over providers of broadband service, so we would actually be--we are actually

able to do less post-reclassification to help consumers than we were able to do before. That being said, we believe--a majority at the Commission believes we should share jurisdiction with the FCC, and not displace the FCC.

Ms. {Schakowsky.} Thank you. I yield back.

Ms. {Rich.} We work very well together.

Ms. {Schakowsky.} Thank you.

Mr. {Burgess.} Gentlelady's time has expired. The Chair recognizes the gentleman from Michigan, the Chairman of the full Committee, Mr. Upton. Did he--about--Ms. Blackburn, then, you are recognized to have 5 minutes for questions, please.

Mrs. {Blackburn.} Thank you, Mr. Chairman, and I want to thank our witnesses for being here.

Mr. Johnson, to you first. Please get your facts and figures all in order, as Chairman Burgess asked, and get that back to us. It is helpful--

Mr. {Johnson.} Yes.

Mrs. {Blackburn.} --to us, and we were hopeful to have that information today to be able to define the number of data security cases that you all have brought forward, not just terming it scores and scores. So let us tighten that up for the record.

Ms. Rich, to you, you talked about the 55 cases that you

all have brought forward, so I want you to walk me through what is the criteria that you utilize when you decide to bring a case forward? What is--what goes into that decision matrix?

Ms. {Rich.} The core concept in our data security program, whether--and we have several different laws we enforce, is reasonableness, and not whether there has been a breach. And we have emphasized a process-based approach that is tech neutral. So for years we--our education and our cases have been emphasizing that the key to data security is to put--is to follow certain key, you know, basic common elements, put somebody in charge, make somebody responsible for the program, do a risk assessment to determine what are the risks in your business, not some checklist that another business with a totally different business model is using, develop a program to address the risks you have just found, and focus in particular on things like the key area--

Mrs. {Blackburn.} Let me interrupt you there.

Ms. {Rich.} Yeah.

Mrs. {Blackburn.} Would you consider, then, that this is more along--you all have an informal set of best practices that you refer back to? Would that be a fair statement?

Ms. {Rich.} Yeah. It is not really informal, because it has been widely publicized in the education materials we

put out in our complaints and orders, which all re-iterate these same elements.

Mrs. {Blackburn.} Okay. All right. Let me ask you this, then. Do you think the draft legislation would limit the FTC's Section 5 authority?

Ms. {Rich.} Well, there is a savings clause, and we are happy about that, but, you know, as we understand it, this is a discussion draft, and so right now we have some concerns that it might weaken the protections that are currently in place. But with the--some of the suggestions we have made for strengthening the bill, we believe it could be quite strong.

Mrs. {Blackburn.} Okay. So you would rather--okay, let me ask you about this, then. What about consent orders? You all have to go ahead and get that consent order to obtain civil penalties for unfair or deceptive practices, so do you believe consent orders are a strong incentive for industry for instituting data security civil penalties?

Ms. {Rich.} We--you are making an excellent point, which is that the bill's inclusion of civil penalties is critical, and we are very supportive of that. Right now, as you note, in order for us to obtain civil penalties, which believe are an important incentive and deterrent from bad behavior, we have to obtain an administrative order first,

and then, if there is a violation, obtain civil penalties. So yes, you are absolutely right, that civil penalties are a key ingredient to the success of legislation.

Mrs. {Blackburn.} Okay. With that, I am going to yield back my time, Mr. Chairman, so we can move on with the rest of the questions.

Mr. {Burgess.} Appreciate--the gentlelady yields back. Chair recognize the gentleman from Massachusetts, Mr. Kennedy, 5 minutes for questions, please.

Mr. {Kennedy.} Thank you, Mr. Chairman. And, again, thank you to the witnesses for testifying. I appreciate the information that you have already offered us today, and as we go through this process.

The FCC has enacted strong regulations to implement their authorities under the Communications Act, and I know you have touched on that a little bit already. These regulations require telecommunications providers to implement a number of specific privacy and security measures to protect consumer proprietary information. I wanted to walk through, with both of you, a little bit about some of those requirements so we can flesh this out a little bit.

So, Mr. Johnson, these regulations require that telecommunications carriers take steps not only to secure customer information, but also discover attempts to gain

unauthorized access to that information, isn't that right?

Mr. {Johnson.} That is correct.

Mr. {Kennedy.} So carriers also, then, must authenticate a customer before providing customer information over the phone, online, or in a store as well?

Mr. {Johnson.} That is correct.

Mr. {Kennedy.} Carriers are required to train their employees in the use of that customer information, is that right?

Mr. {Johnson.} That is correct.

Mr. {Kennedy.} Okay. Are there some other things that are required under the FCC's regulations that you would like to highlight as well?

Mr. {Johnson.} In addition to the--to those that you laid out, Congressman, also--carriers are also required to discipline abuses and to certify compliance with these rules. And, if I may, I would add to that the distinction between enforcement and rulemaking clarity. Of course enforcement is a crucial part of compliance, and the FCC has an Enforcement Bureau that is very active in this space, as is the FTC in the--we partner together on--in many areas, and expect to in the future as well.

The distinction between the present protections in 222 and an enforcement only approach is that the FCC, or in that-

-in this case, the FTC, if this bill were to be enacted, the FCC presently has the ability to get out and engage the public, the providers, to work together through advisory committees, through rulemaking processes, through a whole host of measures, to make clear what the challenges are and what the solutions are before there is a problem. So instead of post hoc enforcement only, there is a solving the problem before it happens, or once it has been spotted, in the case of pre-texting, Mr. Chairman, that you can go after this problem, and seek to solve it, instead of just post hoc--

Mr. {Kennedy.} So proactive versus reactive, right?

Mr. {Johnson.} That is right.

Mr. {Kennedy.} And--so would those requirements be preempted under the current legislation?

Mr. {Johnson.} They would be eliminated.

Mr. {Kennedy.} So, Ms. Rich--thank you, Mr. Johnson. Ms. Rich, if, for example, a telecommunications provider disclosed the number of calls that I made from a specific phone number to a third party, would the FTC be able to bring an enforcement action under this bill?

Ms. {Rich.} We believe that should be added to the bill.

Mr. {Kennedy.} Okay. And would the FTC be able to require that telecommunications providers not disclose that

information unless they obtain customer consent, or should that be added as well?

Ms. {Rich.} Well, that would be a privacy provision, so I am not sure it would be addressed by this bill. But--and I don't think that would be preempted by this bill, the privacy provisions of the CPNI rules. But, in any event, we do think communications should be added to the bill as an element--a data--a piece of data that should be covered.

Mr. {Kennedy.} Okay. I appreciate the feedback. Thank you very much, and I yield back.

Mr. {Burgess.} Gentleman yields back. The Chair now will recognize the Vice Chair of the Subcommittee, Mr. Lance. 5 minutes for questions, please.

Mr. {Lance.} Thank you, Mr. Chairman. Good morning to you both.

To Ms. Rich, the FTC has been a strong advocate for protection of Social Security Numbers, and has often indicated that Social Security Numbers are closely tied to identity theft. I don't think there is any doubt about that. How many state data security and breach notification bills include Social Security Numbers alone as personal information?

Ms. {Rich.} We have that information, but I don't have it at my fingertips, but we would be happy to provide it to

the Committee.

Mr. {Lance.} Thank you very much. Mr. Johnson, did you have an opinion on that?

Mr. {Johnson.} I don't know the answer to that--

Mr. {Lance.} Certainly. Thank you. To Ms. Rich, do you support the inclusion of standalone Social Security Numbers as personal information in the draft legislation?

Ms. {Rich.} Yes. We were very happy to see that in the bill.

Mr. {Lance.} Thank you. And are these data elements not listed in the draft legislation that the FTC has seen tied to identity theft and payment fraud? Are there any data elements not listed in the draft legislation that you would like to see in it?

Ms. {Rich.} Yes. In addition to Social Security Number, driver's license and passport number, and other government issued numbers can also be used to perpetrate identity theft, so we would like to see that information protected standalone, and now it needs to be coupled with other information.

We have also believed that medical--that health insurance numbers can lead to medical identity theft, where people charge--place charges on--in hospitals billed to other people, and it can really accumulate, and they can do that

with simply health insurance numbers. And I believe those are the main elements, besides health and geolocation, which we are not talking about identity theft, we are talking about other information that should be protected. But those are the main additional elements.

Mr. {Lance.} So, to reiterate, other than Social Security, driver's license, and then health identification numbers?

Ms. {Rich.} Yes.

Mr. {Lance.} Thank you. Mr. Chairman, I yield back the balance of my time.

Mr. {Burgess.} Chair thanks the gentleman, the gentleman yields back. The Chair recognizes the gentleman from Vermont, Mr. Welch. Five minutes for questions, please.

Mr. {Welch.} Thank you very much. And I thank the witnesses for your very helpful testimony. Just by way of introduction, I think we have got some areas of real agreement here. Number one, bipartisan agreement that this is a brutal problem. Number two, it is the Wild West. There is no clarity about who is in charge, or what the enforcement is. Number three, there is a desire to get things done that are going to add protection, rather than take it away.

There is some disagreement on policy matters. Like, for instance, on--you, Ms. Rich, indicated you want a stronger--

or as you call it, a stronger trigger notice, and where that balance is--you used that word, balance, that is a debatable proposition. You know, I happen to think that the notice provisions under Gramm-Leach-Bliley--I don't know if you have refinanced your mortgage at all, but you get so much information it is useless, so I want to balance where consumers are protected and notified, but not terrified, and that is a discussion in a debate.

But there are other areas where--for instance, with Ms. Schakowsky, she raised what I thought were some really valid concerns, and this is with respect to the transition of authority. Because my view of the language is that the CPNI that would go to the FTC, you would have that enforcement authority. And the bottom line for me is the concern, which I think is what Ms. Schakowsky was expressing, do we protect the consumers, as opposed to who is in charge.

And I actually do share that, but the privacy provisions that you were talking about, Mr. Johnson, my understanding, and I think, Ms. Rich, you testified to this, the privacy provisions that FCC has would be retained, and not preempted, correct? That is your view, Ms. Rich?

Ms. {Rich.} I would defer to my colleague on that.

Mr. {Welch.} No, I want to ask you, because if we have, essentially, a situation where we think we are in agreement,

but we have language that we are uncertain meets the agreement that we think we have, then that is a different--the nature of that is a different challenge. It is like trying to get the language right. And I appreciate Ms. Blackburn and Mr. Burgess for focusing on, you know, trying to define what the problem is, rather than create additional problems. But my understanding of your testimony was that you believe that privacy was not preempted, correct?

Ms. {Rich.} If I have the current version of the legislation, I thought I saw in there that the privacy provisions of the CPNI rules, and other portions of the Communications Act, were retained.

Mr. {Welch.} Right. And, Mr. Johnson, is that your view as well?

Mr. {Johnson.} Yes, sir. I do think that that is--the language attempts to divide privacy from security.

Mr. {Welch.} All right. So let us say we got the language right to your satisfaction, and the FTC took over authority for CPNI, and you retained--the FCC retained the current jurisdiction it has for privacy. From an agency standpoint, that might not be your preference, but from a consumer standpoint, you would still be holding folks harmless with a new enforcer on some of the elements, is that right?

Mr. {Johnson.} Sir, I would actually say that it is not possible to divide privacy from security, because in most cases the security of information is the privacy of the information, and vice versa. So, for instance, if you have an insider threat, if there is a bad actor in your company, or a mistaken actor in your company, and that person has authorized access to the information, but then mishandles it, or commits some sort of--

Mr. {Welch.} Okay, I am--I appreciate that, and I am going to ask you to help us here, because the spirit that our Chairman has provided here I think is really good. The big problem for everyday people in Vermont is their financial information. A lot of these other things that you have mentioned, they are important, and we have got a lot of work in this Congress to deal with privacy questions--

Mr. {Johnson.} Um-hum.

Mr. {Welch.} --but the--90 percent of the problem for 100 percent of the people is loss of their identity and their financial information. And, you know, the bad guys out there, that is what they want.

Mr. {Johnson.} Um-hum.

Mr. {Welch.} If they want my Social Security Number, it is not for any reason other than to get to my bank account.

Mr. {Johnson.} Right.

Mr. {Welch.} So I think the focus here of a narrow approach that Mr. Burgess has adopted, I think, makes some sense. Now, if there--we don't want to lose rights that people have, but we may need the help of the FTC and the FCC to write that language so that we accomplish this goal that we are accepting is narrow, but without compromising other rights.

Mr. {Johnson.} I--

Mr. {Welch.} So--

Mr. {Johnson.} And I--if I may, sir, I, of course, commend you, and all of you, for trying to tackle this issue. When I was a Senate staffer on the other side, I tried it as well, and we didn't quite get there. It is--I think there--the two things with regard to consumer protections that I would like to mention are, number one, with regard to communications consumer protections, it is a different type of information.

And I think you will hear in this next panel some very expert, knowledgeable witnesses say that data is data, a server is a server, and I would just respectfully disagree that, with regard to call data, with regard to data that flows over networks, cable/satellite, it is specific to the network engineering, and how these networks actually--

Mr. {Welch.} All right. My time is running out, but

here is the one request I am going to make of you. You have identified a problem. We need you to identify a solution, because this is not a policy difference that you are describing now. This is a practical challenge that you are describing. Let us get your help in solving that.

Mr. {Johnson.} --absolutely.

Mr. {Welch.} I yield back.

Mr. {Burgess.} Chair thanks the gentleman. Gentleman's time has expired. The Chair recognizes the gentleman from Texas, Mr. Olson. Five minutes for questions, please.

Mr. {Olson.} I thank the Chair. Welcome, Mrs. Rich, and Mr. Johnson. Sadly, data breaches have become common news. Just this morning we learned about Primera Health Care. 12 million of their customers lost their data, had it exposed to hackers. They were attached in May, discovered the attack in January, and found out recently what had happened. We can do better, but we need to take a balance approach to data breach notifications. We have to protect consumers, but we can't be a burden to companies and hinder the legal uses of data.

This draft doesn't fix all the problems, but it is a small but important step in the right direction. I have a few questions for you this morning. The first ones are for you, Ms. Rich. How many people work in your division in the

FTC?

Ms. {Rich.} We have a privacy division of about 45 people, but we have a number of regional offices, and a number of other offices that work on various privacy issues, like Do Not Call, or privacy issues related to financial information, so we have quite a number of people working on privacy. We, of course, could always use more, but--yeah.

Mr. {Olson.} How many folks on data security? All 45, or more than 45? And how many people focus on data security within the FTC, or your division?

Ms. {Rich.} I don't have at my fingertips exactly, but almost everyone in the division works on both privacy and data security. And then, as I said, there are people in other parts of the agency who also work on these issues. So--I can get you more information, if you would--

Mr. {Olson.} Thank you.

Ms. {Rich.} --like, but--yeah.

Mr. {Olson.} Do they determine what a reasonable data security practice is? Do they do that, as a matter of policy?

Ms. {Rich.} We have standards that we have put out, both in our original Gramm-Leach-Bliley safeguards rule, in all of our complaints and orders. As I said, we lay out a process that is reasonable security. We consider, you know,

various factors, like the sensitivity and volume of data, et cetera, and the staff attorneys who work on this follow the standards that we follow throughout the agency, and that we have announced to the public in particular cases.

Mr. {Olson.} Do they make sure companies use good practices? If so, how do they do that, ma'am?

Ms. {Rich.} We--in investigations, we evaluate whether reasonable security was followed, and whether these types of processes I talked about was--were followed.

Mr. {Olson.} And I am sure you have to have people with very special skills. How hard is it to find those people? Is that a problem for you, ma'am, need more people with the skills to go after these hackers?

Ms. {Rich.} We have very well trained attorneys and investigators. We also have a lab unit that helps with--if there is any forensics involved. And we have experts and technologists, both on staff, and that we consult with.

Mr. {Olson.} Thank you, Ms. Rich. Mr. Johnson, for you, my friend, how many folks in your department work on data security? Not cybersecurity, but data security, within the FCC?

Mr. {Johnson.} It--Congressman, I can get you a specific answer. It is a little--ours--our--it is not divided quite as neatly for us as it is at the FTC, in the

Consumer--

Mr. {Olson.} Ballpark, 10, 20, 30?

Mr. {Johnson.} I would say dozens of people work on various aspects of this in the Public Safety Bureau, that is the bureau that I am in, in the Enforcement Bureau, also the Wireless Bureau, the Wire Line Bureau, the Media Bureau. It is an issue that covers--in the Consumer Protection Bureau, essentially every bureau of the FCC has a role in this in some form or fashion.

Mr. {Olson.} And how about finding really qualified people? Hard time finding the people and skills you need at the FCC to do your job with these data breaches?

Mr. {Johnson.} I would say that the FCC is--has the most qualified network engineers and communications lawyers, and, importantly, communications economists that I have run across. It is an expert agency in the communications field.

Mr. {Olson.} So it sounds like you balanced enforcement with the market, communications, economics, and so you are actually a partner in this endeavor, so thank you for that. I am out of my time. Yield back.

Mr. {Burgess.} The Chair thanks the gentleman. The Chair now recognizes the gentleman from Illinois, former Chairman of the Subcommittee, Mr. Rush. Five minutes for questions, please.

Mr. {Rush.} Thank you, Mr. Chairman. I really am enjoying the input, and the conversation both ways, in regards to this particular matter. I view the issue before us as an issue that is really--that we have to maintain the understanding that data security and privacy are really like two sides of the same coin, and we can't bifurcate these two issues.

I think we have to proceed with, really, the understanding that, in order to be forced to really serve the American people, and begin to deal with this issues--these issues that they are confronted with, both in terms of privacy and also data security, that we can't waste our time in trying to separate these two issues. And I don't think the outcome would be an outcome that we want to achieve, and that would really help us out in the problem that all of us are vitally concerned about.

I want to ask Ms. Rich, recently the FC announced that broadband providers would be regulated as common carriers. Under these particular rules, if a broadband provider were to be the subject of a data breach, which agency would have primary responsibility for ensuring that any Federal standard is enforced? And, Mr. Johnson and Ms. Rich, I want you to answer those question--this question, beginning with you, Ms. Rich.

Ms. {Rich.} Prior--we have not taken a position on reclassification generally, but, as I mentioned, a byproduct of it is we--it limits our ability to protect consumers when the companies that perpetrate the violations are broadband providers. So if a broadband provider had a breach, and it was--pertained to their provision of broadband service, and not some ancillary service, we would no longer be able to protect service in that area. We would like, of course, to have somebody, maybe somebody here, restore that jurisdiction to us. We don't, however, object to the reclassification.

Mr. {Rush.} Mr. Johnson, what are your--

Mr. {Johnson.} Congressman--

Mr. {Rush.} --comments?

Mr. {Johnson.} We are--my focus in work, and also at this hearing, is the--is--are the provisions that pertain to data security of communications data. I am certainly aware of the effect that Title II reclassification has, particularly on Sections 201, 202, and 222. And I will just--if it is okay with you, I will leave it at that, because I have never practiced law with regard to the Federal Trade Commission Act, and I will defer to the Federal Trade Commission, and--

Mr. {Rush.} Well--okay. Well, thank you so much. Ms. Rich, can you clarify one piece of your testimony, if you

will? You are advocating to lift the common carrier exemption, but not to take away regulatory or enforcement authority from the FCC, am I correct? That is--how would that be done? What do you suggest?

Ms. {Rich.} Well, we share jurisdiction with a lot of different agencies in a lot of different areas, and, you know, we have--for example, with the CFPB, we have an MOU with them. We have, for years, shared jurisdiction with the FCC as to do not call. We did share jurisdiction over broadband providers, proprietor re-classification, and we can successfully coordinate, and make sure there is no duplication.

So what we are saying is we think, as the agency that is most experienced in the data security area has can be very effective in protecting consumers that we should be--we should have jurisdiction over carriers, but that we--that the FCC--the majority of our commission believes that that doesn’t mean the FCC shouldn’t--should be displaced in its jurisdiction.

Mr. {Rush.} Okay. Is there--in terms of the--your practice that you have regarding these memorandum of understandings, does that create a burdensome issue for the consumer? Is there--does that complicate their lives, or--

Ms. {Rich.} No, not for the consumer at all. In fact,

the consumer potentially has two cops on the beat. But what the MOUs and the coordination is usually for is to make sure that there is no duplication and burdens created for businesses. For example, the two agencies, without communicating with each other, both investigating the same company at the same time.

Mr. {Rush.} Mr. Johnson, you want to comment on--

Mr. {Johnson.} I think she stated it very well, sir.

Mr. {Rush.} Mr. Chairman, thank you, and I yield back.

Mr. {Burgess.} Chair thanks the gentleman, the gentleman yields back. The Chair recognizes the gentleman from Kansas, Mr. Pompeo. Five minutes for questions, please.

Mr. {Pompeo.} Thank you, Mr. Chairman, and thank you both for being here today. I suppose I am not surprised, but I am troubled by how little conversation there has been this morning about cost to consumers. When you talk about protecting consumers, there is very little discussion about what this will mean, right? If a business is paying money, it gets passed along, and there is just remarkably little discussion about what it really means to someone who can least afforded whatever services that we are dealing with. I think that is very important.

I would hope that the two of you would appreciate that too, but instead what I get is two government agencies, each

of which wants increased authority, increased power, more control, the capacity to define rights, sort of the historic governmental actions. I would hope, when you think about the consumers that you are tasked to oversee that you would at least consider their economic well-being as well.

Ms. Rich, in that vein, you have asked for a--you said that the definition contained--really, the notice provision, you weren't happy with it. You suggested alternative language. You said you would support an approach that ``requires notice, unless a company can establish there is no reasonable likelihood of economic, physical, or other substantial harm''. So you have flipped the burden of proof now to the consumer, right? Right, to the business which they have contracted with to demonstrate that there is no harm. What do you think the cost of a change like that would be?

Ms. {Rich.} I think the burden is already flipped in the draft. All we are proposing is that the--instead of it being limited to financial harm, that it be--include economic, physical, or other substantial harm.

Mr. {Pompeo.} Fair enough. I want to go on to Mr. Johnson. Mr. Johnson, you--I think in response to a question you said that there were--you didn't know the exact date, or you were going to bring us that, but you said there were

scores of cases? Is that right?

Mr. {Johnson.} Yes, sir, of--

Mr. {Pompeo.} That you brought? And you identified two in your written testimony, if I got it right. Is--

Mr. {Johnson.} I think the--if I remember correctly, the two that are in the footnote in the written testimony--

Mr. {Pompeo.} Right.

Mr. {Johnson.} --were from--were just two examples from last year that were concluded. I--we are--I would draw a distinction between cases that are investigated, cases that are pursued, cases that are settled, and not necessarily cases that all end in a--

Mr. {Pompeo.} Are these the only that have--that are of record? You said there are scores and scores. There are two identified. Are there others that you could have put in this--

Mr. {Johnson.} Absolutely. Yes, sir, and I committed earlier--

Mr. {Pompeo.} And would any of those have actually been data breaches? Because neither of these, as described in your testimony, are actually what we are dealing with here today.

Mr. {Johnson.} Well, I think the--

Mr. {Pompeo.} One is a Do Not Call case, according to

your testimony, and one was a violation of--

Mr. {Johnson.} That--yes, sir, that--your question underscores the distinction that we think is important with regard to communications data. It is not just breach of Social Security Numbers or credit card numbers. It is about--information about what people do on the telephone, what do they do with cable and satellite TV, and it is a much broader set of data that is specific to the networks that hold, and manage, and deliver that data.

So it is not--it is harder for us to hone in on, this was a data breach of Social Security Numbers, than it is to talk about how we prospectively and proactively protect the consumer in a way that is actually, I think, to your original point, is cost effective, because it allows us to engage ahead of time with the providers. And I can give a number of examples about how we do that in a way that aligns it with business interests to protect the consumer, while also letting the companies sort of--

Mr. {Pompeo.} Yeah.

Mr. {Johnson.} --lead the solutions, yeah.

Mr. {Pompeo.} I am not sure I agree with you. I went back and read the Notice of Apparent Liability that you have issued, and when you--the language you used implies that if you have a breach, then your security is, per se,

unreasonable, and your privacy policy is deceptive. Is that the FCC's position?

Mr. {Johnson.} I don't know the exact line that you are going at there, but if you are--do you know which action you are referring to, sir?

Mr. {Pompeo.} I do, but I just want to--I want to go more generically. I want to kick it out from the particular case. Is it the case that it is the FCC's view that it is a per se--is, per se, unreasonable, and your privacy policy is deceptive, if there was a breach?

Mr. {Johnson.} No, sir, I don't think that is the case. In fact, in our rules, it requires--on the 222 side, it requires reasonable measures to discover and protect against unauthorized access.

Mr. {Pompeo.} Great. Thank you. Mr. Chairman, my time is up. I yield back.

Mr. {Johnson.} I should--do you--if I might, sir, the one additional note is that on the cable/satellite side, and this is another distinction with the bill, the standard is not just reasonable. It is as necessary to protect, so it is a much higher standard in the cable/satellite viewing preferences case.

Mr. {Pompeo.} Thank you.

Mr. {Johnson.} But it still--I wouldn't say it is a per

se violation.

Mr. {Burgess.} Chair thanks the gentleman. Gentleman's time has expired. The Chair recognizes Mr. Cardenas. Five minutes for questions, please.

Mr. {Cardenas.} Thank you very much, Mr. Chairman. I want to thank the witnesses for all of your service. It is an issue that is becoming more and more important. But one thing that I would like to underscore is that I look at this as similar to what we all, as Americans, thankfully, take for granted, that in any community we have government police. And let me tell you, when communities hire private policing, or what have you, talk about things getting out of control, and talk about lowering the standard of the kind of security that community has.

There is certainly a drastic difference between hiring a security guard versus calling 911 and having the true police force show up. So I want to thank both of you, and both of your departments, for what you do for us to keep us safe. And certainly to keep the cost effectiveness of your purpose I believe is about American consumers, and making sure that we fortify you with the resources you need so you can have the intelligent individuals, and the hardworking individuals to go ahead and make sure that breaches don't happen as often as possible, we can be preventative.

Because let me tell you, what we pay in taxes is nothing compared to the person who gets their information breached. They lose their house, their entire credit report goes to the wastebasket, and they lose everything. And then in many, many cases it is years, and years, and years before that individual, or that family, can actually get back to being right, and their entire reputation is, again, goes to the wastebasket. As far as on paper, people think of them, because their bank account was cleaned out, they couldn't pay their mortgage, they lose their home, they can't run their business, or what have you, because they no credit, they can't get access to capital, et cetera. So let me tell you, when you--when we allow you to do your job well, I think that less and less of that does happen to our American public.

So, with that, I only have time for perhaps one question. I want to refer back to the--FTC recently released a staff report on Internet of things. The Internet of things refers to the ability of devices to connect to the Internet, and send and receive data. As the report acknowledges, many of these devices are vulnerable to being hacked. About 60 percent of web enabled devices have weak security, and that is what has been reported.

In September of 2013, the FTC took its first action against an Internet of things company when it brought a

complaint against TRENDnet, a company that manufactures web-enabled cameras, for misrepresenting the security of its cameras. In that case, it was not personal information in electronic form that was accessed, but rather live feeds from the cameras, including the monitoring of babies.

So, Ms. Rich, do you agree that reasonable security measures include implementing procedures and practices that limit the ability of hackers to remotely access control Internet connected devices?

Ms. {Rich.} Yes. You have touched on two things that are very important to us about this bill. First, device security. That is--it is because of our work on the Internet of things that we realized that it is very important to security devices so they can't--even regardless of the personal information involved, they can't be taken over and used in ways--for example, medical devices that--or automobiles, which I discussed in my--at the beginning to hurt consumers.

And also, TRENDnet--our case against TRENDnet was an example where it wasn't financial data that was exposed, it was pictures of very private things happening in homes, and that kind of sensitive information does need to be protected.

Mr. {Cardenas.} Okay. Thank you. Ms. Rich, what type of access control measures would limit the ability of hackers

to remotely accessing controlled devices, and how could companies implement those measures to make consumers safer?

Ms. {Rich.} We believe the legislation should actually just include a reference to protecting device security in order to make sure the--that is--that devices are protected from that kind of interception.

Mr. {Cardenas.} And also, generally, are the people who have been attempting to hack, and it is my understanding that it is in the millions and millions of attempts per year on American companies, and on our government, et cetera, are those hackers limited in their budgets? Do they seem to have a limited budget per year, and they stop doing what they do, and they wait until next year's budget?

Ms. {Rich.} There are very sophisticated hackers out there who are very motivated, and many of them aren't even in this country. And many of them do these--they are so good at what they do, they don't actually require a huge budget.

Mr. {Cardenas.} Okay. I don't know if we could ever even the playing field, but I would love to see that we fortify you with the resources you need to protect us. Thank you very much, Mr. Chairman.

Ms. {Rich.} Can I just add something? I want to make sure--I feel like I have been too modest in the way I described our 55 cases, because those were completed cases

that ended in an order. And if we did include investigations, and all of the--and closing letters, and all of the activity we engage in that doesn't lead to a signed order, there are hundreds of data security cases.

Mr. {Burgess.} The Chair thanks the gentlelady for the clarification. The Chair now recognizes Ms. Brooke from Indiana. Five minutes for questions, please.

Mrs. {Brooks.} And I want to thank all of the witnesses for valuable time educating the public, educating all of us on the proposed changes to further safeguard sensitive consumer information by providing the timely to these individuals. Also want to commend the Chairman on all the work that has been done. As a new member to Energy and Commerce, I know there has been a lot of work done over the years, and, obviously, the growing nature of cyberinfrastructure in all of our lives, it makes this so very important.

I have to tell you, we did--before the hearing today, in 2014 alone, the Indiana Attorney General's Office received more than 370 data breach notifications, and more than 1,300 identity theft complaints in Indiana. Actually--that was, actually, I thought, kind of low, considering many of us have just received notification from our insurance company about the breach in Indiana of potentially up to 80 million

customers.

But I want to ask, from your perspective, Ms. Rich, at the FTC, how does a national security standard in the draft bill--wouldn't a national security standard help consumers, in theory? And--because I am not hearing that you are interested in a national security standard, but that, in fact, we should continue to allow 47 to 50 different state standards to be in place. Talk to me about a national security standard, and what, you know, what your thoughts are on that. Because I am not hearing that you are in favor of that.

Ms. {Rich.} We absolutely agree that a national security standard would be helpful. It would make very clear what the expectations are. It would fill the gaps, not--only 12 states have data security laws, even though 47 have data breach laws, if I am up to speed on all the laws that have passed. But we--

Mrs. {Brooks.} Could you--

Ms. {Rich.} We absolutely--

Mrs. {Brooks.} --explain to us the distinction between data security laws versus data breach laws?

Ms. {Rich.} I just want to qualify what I was saying, and then I definitely--

Mrs. {Brooks.} Okay.

Ms. {Rich.} --will. But we are concerned about a national standard if it would water down protections that are currently in place today, which is why we are suggesting some modification to this discussion draft to strengthen it, so that it wouldn't weaken the protections in place today. Because if it preempts the state laws, and they--the main thing there is health. To preempt state laws that provide data security for health information, and that is already provided now, then there won't--there would be fewer protections for health information. So that is our concern. But yes, in theory, we absolutely do support a national standard.

In terms of the difference between data security and data breach, data security is protecting the data so there isn't a breach. And, in fact, the FTC's focus has been chiefly on that, not as much breach notification, in part, because we don't have breach notification authority, except in a narrow area. So data security is very, very important, and that is why, right at the outset, I thanked the Committee--the Subcommittee for including data security, and not just data breach notification, which is, you know, after the breach happens you tell consumers, but the horse is already out of the barn.

Mrs. {Brooks.} Can you explain--in your prepared

testimony you talked about it is critical that companies implement reasonable security measures in order to prevent data breaches. Can you elaborate? I was just Googling to try to find out what, under FTC, reasonable security measures mean. And I know that is a broad question, but yet--can you please, you know, share with us what reasonable security measures mean to the FTC? Because that is actually how you determine which cases to take or not take. Is that not really the crux of the issue?

Ms. {Rich.} Yes. So we--in reasonableness, we are referring to a bunch of factors which we have laid out again and again. The sensitivity and volume of information involved, you might want to have stronger security if you are talking about, you know, Social Security Numbers, than simply what, you know, size dress a person wears. The size and complexity of the data operations, a small company won't need to put as many protections in place if they have smaller data operations. And the cost of available tools to secure data and protect against known vulnerabilities. If there are not available tools out there that a company can learn about and use, it would not be--even if it could cause harm to consumers, it would not be reasonable to expect them to have known that.

Now, those are factors to look at, but we also really

emphasize a process-based approach. Because if you undertake a responsible process, you should be able to get to the outcome of reasonable security. And also, process-based approach is tech neutral, so put somebody in charge. I was talking about this a bit earlier. Make somebody responsible. Somebody should be lying awake at night, worrying about this. You know, do a risk assessment. Put procedures in place to address those risks, focusing on such areas as training. Oversee your service provider. Periodically do evaluations and updates of your program. If you do those procedural things, and read all the information out there that provide guidance on what is reasonable security, you should be able to get to the reasonable security outcome.

Mrs. {Brooks.} Thank you very much, and I look forward to also learning, in the future, Mr. Chairman, how the FTC-- we are all focused on preventing the breach, enforcing if there has not been adequate security. I would love to know more about what we are doing to go after the hackers, and whether we never hear that we ever catch the hackers. Thank you, and I yield--

Mr. {Burgess.} Chair thanks the gentlelady for that observation. Chair recognizes the Ranking Member of the full Committee, Mr. Pallone. Five minutes for questions, please.

Mr. {Pallone.} Thank you, Mr. Chairman. I wanted to

ask Mr. Johnson these questions. I have a lot, so I am going to try to go through it quickly, if you could answer quickly. If this bill were to pass, Sections 201, 202, and 222 of the Communications Act, and all associated regulations, which include broad consumer privacy and data security protections, would no longer be in effect with respect to security of data in electronic form and breach notification.

So, Mr. Johnson, can you walk us through some examples of the types of consumer information that could have been required to be protected by Internet service providers under those sections? You know, first start, you know, could Internet browsing history have been protected?

Mr. {Johnson.} Well, I think the--that section, Section 222, has, for 18 years, been focused mostly on voice--on telephone communications. As of last month the Commission's reclassification of broadband Internet access service expanded 222 to broadband providers, and there are presently no specific rules in place that pertain to the broadband service providers.

But I think that underscores the value of having--of public notice and comment rulemaking procedures to determine what exactly--what precisely that requires in--

Mr. {Pallone.} So would you say that Internet browsing history could have been protected? Yes or no.

Mr. {Johnson.} It could be, potentially.

Mr. {Pallone.} All right. How about the unique identifiers for wireless devices?

Mr. {Johnson.} I think in--by unique identifiers, could you tell me a little bit more?

Mr. {Pallone.} Well, what about the--what about--I mean, just tell me what you think would be protected, or could be protected--

Mr. {Johnson.} Well, what would--

Mr. {Pallone.} --if it isn't at this point.

Mr. {Johnson.} The bill does transfer some of the protections for CPNI for call records data to the FTC, but what it doesn't transfer is a number of other things that pertain to the call service. And that is--this is just on 222. For instance, how many calls a person makes in a day, what time they call, specific features of their call service, call waiting, caller ID. And, importantly, things that are not related to the telephone calls, but could be related to the service that they have, their financial status, whether they are low income. And that is just on 222. The bill also would remove the existing--all of the existing protections for cable and satellite and television viewing history, and related information.

Mr. {Pallone.} So let me just as a couple more. I know

there are only 2 minutes. If the bill were enacted, the FCC would not be able to require Internet service providers to protect sensitive customer information?

Mr. {Johnson.} I think that is true. I think that is--

Mr. {Pallone.} And the FCC would not be able to bring enforcement actions against Internet service providers that did not protect that information?

Mr. {Johnson.} I think that is correct.

Mr. {Pallone.} And as you read this bill--and this is really the most important thing. As you read this bill, with regard to Internet service providers, would there be any protections for these types of customer info, beyond what is listed as personal information, in the definition section?

Mr. {Johnson.} That is--I think there would not be beyond that definition, which is specific to financial harm and fraud--

Mr. {Pallone.} All right.

Mr. {Johnson.} --and identity theft.

Mr. {Pallone.} All right. Thanks so much.

Mr. {Burgess.} Chair thanks the gentleman. Gentleman yields back his time. The Chair recognizes gentleman from Mississippi, Mr. Harper. Five minutes for questions, please.

Mr. {Harper.} Thank you, Mr. Chairman, and thank you both for being here. Ms. Rich, I just have a question. The

legislative draft calls for uniform data breach and information security requirements housed at the FTC, including leveling the playing field by bringing telecommunication, cable, and satellite providers under the FTC regime. In your opinion, is the FTC the appropriate agency to oversee data security for the Internet, how shall we say, ecosystem?

Ms. {Rich.} We have been the lead agency on data security for now over 15 years, and we believe we should continue to provide that leadership, which is why we do want--we appreciated nonprofits being in the bill, and we appreciated carriers in the bill. The bill even, though, recognizes that others have a role to play. It allows the states to enforce, even if--as it preempts, it allows the states to enforce, and we would welcome that partnership with the states.

And as I mentioned before, we are--want to have common carrier authority so we can protect consumers, but we would be--we don't believe we should displace the FCC, or the majority of the Commission don't believe we should displace the FCC, so we would like to partner with them too in protecting consumers in the carrier area.

Mr. {Harper.} Thank you, Ms. Rich, and I yield back the balance of my time.

Mr. {Burgess.} Chair thanks the gentleman. Gentleman yields back. The Chair recognizes the gentleman from North Carolina, Mr. Butterfield. Five minutes for questions, please.

Mr. {Butterfield.} Thank you very much, Mr. Chairman. Thank you for holding today's hearing. Thank you to the witnesses for their testimony. This is absolutely an important issue, Mr. Chairman, that many members of this Subcommittee are familiar with. You know, we have worked over the past few Congresses precisely on these concerns. As members of the Subcommittee know, data breaches are occurring in alarming numbers all across the country. Just in North Carolina, our Attorney General estimates that about 6.2 million North Carolinians have been affected by data breaches since 2005, that is over the last 10 years, so I am glad we are addressing this issue today.

Our good friend, and Chairman of the Subcommittee, Mr. Rush, former Chairman of the Subcommittee Mr. Rush, introduced a bipartisan bill entitled ``The Data Accountability and Trust Act'', and during my time as Ranking Member of this Subcommittee, I worked very closely with then Chairwoman Bono, who I think I see here today, on the Secure and Fortify Electronic Data Act. There is plenty of precedent for finding bipartisan solutions on this subject.

There are some issues with the discussion draft before us today, and I encourage the majority to work with us so we can finally produce meaningful legislation that will give consumers the protections that they deserve, and businesses they--that--and businesses. They certainly need to grow and thrive.

Let me just address one or two questions to the witnesses. I may not take up the full 5 minutes, but I want to discuss the APA rulemaking authority for just a moment. One important thing about that authority is that it allows an agency, such as yours, any agency with that authority, to implement a law over time. It is particularly important for laws concerning issues in which technical advances are common, and fairly quick, to be flexible and agile. As lawmakers, one thing we hate is having to revisit a law we recently passed because it is already out of date.

When Congress passed the Children's Online Privacy Law, it allowed the FTC to amend the definition of personal information through regular APA rulemaking procedures. Mr. Johnson, can you explain how the FCC has been able to ensure that Section 222 of the Act has stayed relevant at all times? How has Section 222 been updated to deal with problems over time, such as, most recently, when carriers were pre-installing software onto devices that had security flaws?

Mr. {Johnson.} Yes, sir, and I have already committed to providing a detailed timeline of FCC's history with 222, but I think that is a--your question is--gets right to the heart of the value of having the flexibility and the agility to adapt a statute to the changing technological landscape, and also the changing public expectations and Congressional expectations.

So since the--since Section 222 was enacted in 1996, entitled ``Privacy of Consumer Information'', there have been a number of shifts. Obviously technologically, but also with regard to Congressional expectation. The first was in 1999, when, as part of the Wireless Communications Public Safety Act, the Commission added location information into the protected information under Section 222, and that is because 911 location accuracy is crucial.

There was just a--tragically, a woman in Georgia who made a 911 call on the border of a county line, and neither of the two call centers knew where she was, and it cost her her life, and this is something that we are trying to improve. And now, under a new rule that was enacted--or was--the Commission voted on earlier this year, hopefully soon the location accuracy will include being able to pinpoint a--where a person is, which room in a multi-story building they are in if they need help. But there are obviously incredibly

specific privacy concerns that come with that type of location information.

Mr. {Butterfield.} Absolutely.

Mr. {Johnson.} So that is the type of thing that was added in 1999, and it has been improved over time, and--including the one that you mentioned, with regard to information collected on mobile devices in 2013.

Mr. {Johnson.} Right. All right. Let me go to Ms. Rich. Ms. Rich, your testimony called for FTC to be granted APA rulemaking authority to carry out the draft bill. Can you give us an example, beyond COPA, where such limited authority has allowed the FTC to deal with problems over time? And, finally, are there any instances where not having APA rulemaking authority inhibited the Commission's ability to effectively deal with problems?

Ms. {Rich.} The chief reason we want rulemaking authority in this area is, as you note, to allow us to adapt the consumer protections to make sure consumers are effectively protected, even as technology changes. So the Ranking Member mentioned geolocation as one type of information that we wouldn't have thought to protect just--not too many years ago, but another example is--we now know that facial recognition--the information that is collected through facial recognition is very sensitive, and we wouldn't

have thought of that. It was only recently that it was recognized that Social Security Number alone could be used to perpetrate identity theft, particularly in the case of children, who don't have rich credit histories, and so it is very easy to take the Social Security Number, and pass it off as somebody else's.

So those are some examples of information we wouldn't have even known to protect a few years ago. And yes, we have a number of instances where we have used our rulemaking to not just adapt to change, but to respond when there were needless burdens on businesses in a law. We did that in CAN-SPAM. We used our rulemaking there. So there are a lot of examples.

Mr. {Butterfield.} Thank you very much, and thank you, Mr. Chairman, for not calling time prematurely on the witness. Thank you.

Mr. {Burgess.} Chair thanks the gentleman. Chair recognizes the gentleman from Oklahoma, Mr. Mullin. Five minutes for questions, please.

Mr. {Mullin.} Thank you, Mr. Chairman. Mr. Johnson, I would like to spend most of my time, if not all my time, visiting with you. Do you believe that a breach of information involving a number of someone's calls could maybe lead to theft or financial fraud? You mentioned about the

cell phones a while ago. Do you see this could maybe cause a bigger problem down the road?

Mr. {Johnson.} As--let me make sure I understand your question. Could a breach of call data--

Mr. {Mullin.} Of information. A breach of information involving the number of someone's call. Could this lead to a bigger problem?

Mr. {Johnson.} I guess it--let me not engage in hypotheticals, but I guess you could come up with some scenarios in which the--a breach of non-financial telecom information--

Mr. {Mullin.} I mean, when you open that box, it leads down a road that is unknown. Like you said, you are being hypothetical on it.

Mr. {Johnson.} Um-hum.

Mr. {Mullin.} And I think there is a lot of work that needs to be done. Now, obviously we want to protect the consumer. It is tragic what you brought up a while ago. I think most of us here read about that. We want to be able to protect people. I mean, I live way out in the middle of nowhere. My driveway is literally a mile long. The only way I get cell phone coverage is--

Mr. {Johnson.} Best way to--

Mr. {Mullin.} --with the antenna that goes up my

chimney, and I would want someone to be able to respond. There is no 911 address--

Mr. {Johnson.} Right.

Mr. {Mullin.} --where I live.

Mr. {Johnson.} Right.

Mr. {Mullin.} And I get that. But at the same time, I don't want to open it up to exposing us to even a bigger risk. All of us live in fear of fraud. The first time I had experience with that, someone went to school on my Social Security Number in California. At that time, I hadn't even been to California, and I got a phone call wanting to know what has happened. So it is something that we need to worry about.

Going on--you pointed out in your testimony, under the proposed bill, the FCC could lose rulemaking authority over data security. Has there been a--has the FCC effective--have been effective in using the authority to protect consumers in the 21st century?

Mr. {Johnson.} I would say, sir, that this is a--this will always be, as a cybersecurity--focus of my work is cybersecurity, and has been for years, this will always be a work in progress.

Mr. {Mullin.} Right.

Mr. {Johnson.} We are not going to solve this problem.

But I would say that I have--since I have been at the FCC, I have been very impressed with the clarity of the expectations that have developed, particularly on that--on Section 222 of--

Mr. {Mullin.} Well, do you know how many regulatory documents the FCC has published since ’96?

Mr. {Johnson.} I don’t know. You mean new rules?

Mr. {Mullin.} Yeah, new rules. Yeah.

Mr. {Johnson.} We are committed to providing a full list of not just rules, but activities.

Mr. {Mullin.} Well, according to the Federal Registry, the FCC has published nearly 14,000 rules since ’96.

Mr. {Johnson.} Pertaining to--

Mr. {Mullin.} No.

Mr. {Johnson.} Overall?

Mr. {Mullin.} Overall. Do you know how many of those pertain to our 21st century security issues that we are having?

Mr. {Johnson.} I would have a ballpark, but I--it sounds like you--

Mr. {Mullin.} Give me a ballpark.

Mr. {Johnson.} --an answer.

Mr. {Mullin.} I don’t, because--seriously, we did a lot of research trying to find it, and I really could not find

it. In fact, my follow-up was, could you provide the information--

Mr. {Johnson.} There have been a few rulemakings and declaratory rulings on--specifically pertaining to 222, and we will get you those exactly.

Mr. {Mullin.} Are they being implemented right now?

Mr. {Johnson.} Yes, sir.

Mr. {Mullin.} Do you know how long it is going to take?

Mr. {Johnson.} Well, it is--I--it has been, and will always be, an ongoing process, but they are being implemented, and--

Mr. {Mullin.} So it takes years to implement this?

Mr. {Johnson.} Well, I don’t know if I would--I think the premise of your question may be that it finishes at some point, and the--

Mr. {Mullin.} Technology doesn’t finish--

Mr. {Johnson.} Right.

Mr. {Mullin.} --and it seems like we are being very reactive, and we are not being proactive. We are responding to issues that happened years ago, and what we are trying to do is be in front of it.

Mr. {Johnson.} I understand.

Mr. {Mullin.} And if we continue to be reactive, how are we ever going to get ahead of the game?

Mr. {Johnson.} Actually, I think you are absolutely right about the need to be proactive, and that is the value of having rulemaking authority.

Mr. {Mullin.} And I agree with that, but the problem that I have is, just recently, the FCC went all the way back to 1930. So how is that being proactive? I mean, we are wanting--you are wanting to keep the authority and have more authority. We are wanting to move forward. We are wanting to start being proactive, not reactive. You are making the argument that you want to keep it, but the recent actions of going all the way back to 1930 to a rule, how in the world, with today's technology, is that being proactive?

Mr. {Johnson.} You are referring to the open Internet--

Mr. {Mullin.} Yes.

Mr. {Johnson.} --order?

Mr. {Mullin.} Of course I am.

Mr. {Johnson.} I will stay disciplined and remain in my lane on that. My focus is ensuring that the laws and policies are in place to ensure that telephone calls go through, that 911 calls have--

Mr. {Mullin.} So let us finish on this, then. Do you really believe the FCC can continue to be proactive, or do you feel like you guys are being reactive?

Mr. {Johnson.} I think, actually, it--we are not only

trying to be, but we are being proactive, and I can give you two examples. One is--

Mr. {Mullin.} No, it--my time is out, but I am just going to tell you, from my opinion, it looks like we are being extremely reactive. Mr. Chairman, thank you. Mr. Johnson, thank you for your time. I yield back.

Mr. {Burgess.} Chair thanks the gentleman. Gentleman yields back. Chair recognizes the gentleman from Illinois. Five minutes for questions, please, Mr. Kinzinger.

Mr. {Kinzinger.} Well, thank you, Mr. Chairman, and thank the witnesses for being here and spending a little time with us today, and thank the Chairman for calling this hearing. I probably won't take all 5 minutes. I basically just have one question. I want to explore the issue of e-mails, and in this draft bill, e-mail, data breach, et cetera. I know in Florida there is a--their data breach and security notification law actually requires--actually allows for e-mail addresses, passwords, and--because in many cases many people have the same e-mail and passwords into different sites, as well as, you know, they use it for login into something bigger.

Ms. Rich, in your testimony you note that within the draft legislation the definition of personal information does not protect some of the information which is currently

protected under state law, I would guess that would be part of it with the e-mail. Could you please expand on which elements that exist in the state law that would be most important for us to consider within a Federal statute, and would you include e-mail and passwords in that?

Ms. {Rich.} I believe passwords are already in there in various capacities, but yes, the most important elements we--would be health, geolocation, and e-mail--and communications. And as I--and device security. And as I mentioned earlier, we believe--we have seen evidence that passport, driver's license, and other government issued numbers could be used, like Social Security Number, to perpetrate identity theft. So that is my list.

Mr. {Kinzinger.} Now--and let me ask--so let us talk a little more about e-mail address and password. Could an e-mail address and password combination, could that lead to economic harm, and how could you see that happen? Is it more than just somebody has access to your e-mail? Could that lead to bigger economic harm if that is stolen?

Ms. {Rich.} I can't spin out all the hypotheticals, but e-mail address and password could get you into somebody's account, allow you to read their e-mails, allow you to communicate with perhaps accounts they have already set up with some sort of automated, you know, I know when I interact

with accounts, I have often set it up, I know this is not a great practice--security practice, so that I can pretty quickly get on, it remembers me. So I think there are probably a lot of scenarios we can spin out with e-mail and password.

Mr. {Kinzinger.} Okay. And do you have any ideas as to, like, how do we reach that right balance of, you know, finding out what can be breached, and there is a problem, and also understand that we don't want to create legislation that is entirely too burdensome to people?

Ms. {Rich.} I think that the current draft already covers a nice broad class of information, and we are very complementary of the current draft. These were just a few additional items that we believe could cause consumer harm if they are intercepted by somebody else. And it is not an endless list. These are a few things we believe should be added.

Mr. {Kinzinger.} Okay, great. And I will yield back a minute and 40 seconds, Mr. Chairman.

Mr. {Burgess.} Thank you. Chair thanks the gentleman, gentleman yields back. Seeing there are no further members wishing to ask questions, I do want to thank both of you for your forbearance today. It has been very informative. Thank you for participating in today's hearing. This will conclude

our first panel, and we will take a no more than 2 minute recess to allow the staff to set up for the second panel. Thank you, and this panel is dismissed.

[Recess.]

Mr. {Burgess.} Mr. Leibowitz, we will begin with you. Five minutes for your opening statement, please.

|

^STATEMENTS OF JON LEIBOWITZ, PARTNER, DAVIS, POLK, AND WARDWELL, LLP, CO-CHAIRMAN OF, AND ON BEHALF OF, THE 21ST CENTURY PRIVACY COALITION; SARA CABLE, ASSISTANT ATTORNEY GENERAL, OFFICE OF THE MASSACHUSETTS ATTORNEY GENERAL; MALLORY DUNCAN, SENIOR VICE PRESIDENT AND GENERAL COUNSEL, NATIONAL RETAIL FEDERATION; LAURA MOY, SENIOR POLICY COUNSEL, OPEN TECHNOLOGY INSTITUTE, NEW AMERICA; AND YAEL WEINMAN, VICE PRESIDENT, GLOBAL PRIVACY POLICY AND GENERAL COUNSEL, INFORMATION TECHNOLOGY INDUSTRY COUNCIL

|

^STATEMENT OF JON LEIBOWITZ

} Mr. {Leibowitz.} Thank you so much, Mr. Chairman. Chairman Burgess, Ranking Member Schakowsky, members of the panel, I want to thank you for inviting me to testify at this important hearing. Chairman Burgess, you and I worked together in the past on FTC related health care issues, and you bring a wealth of experience to your new role. And Ranking Member Schakowsky, you have been a leader on consumer protection issues, going back to your work at Illinois Public Action. Just as importantly, listening to this--to the panel and the questions, I can just tell that both of you are committed to finding practical solutions to real problems,

which is why you will certainly develop many bipartisan initiatives going forward.

Along with Mary Bono, your former Chairman, I serve as--who is sitting over there, your former Chairman, I serve as co-Chair of the 21st Century Privacy Coalition. Our group is composed of the Nation's leading communications companies, which have a strong interest in modernizing data security laws to bolster consumers' trust in online services, and confidence in the privacy and data security of personal information. We are very supportive of the discussion draft legislation and what it seeks to accomplish.

Data security is an issue that I have cared deeply about for many years, going back to my time as a commissioner on the FTC. In fact, on behalf of the FTC, I testified before this Subcommittee on this issue back in 2006. In testimony then, and it was testimony for a unanimous Federal Trade Commission, we urged Congress to ``enact strong data security legislation that requires all businesses to safeguard sensitive personal information, and gives notice to consumers if there is a breach.'' And since then, as you know, the need for legislation has only grown dramatically.

You know all the statistics. Members have mentioned them. In 2014 we saw a number of data breaches. Just this morning in the Washington Post I read about a hack that may

have exposed 11 million people, Primera customers, and their sensitive personal information. And when these breaches happen, they typically expose sensitive information. That is what all of the members had said in the first panel, how important that information is to consumers.

Data breaches resulting in the exposure of personal information can result in substantial harm to consumers. Companies that fail to take responsible measures to protect this information need to be held accountable. And that is why our coalition commends Representatives Blackburn and Welch, for releasing the Data Security and Breach Notification Act draft. The discussion draft contains elements we believe are essential for effective data breach and data security legislation. Let me highlight just a few of them now.

First, the draft includes both breach notification standards and substantive data security requirements. While notifying consumers that a breach has occurred is important, it is ultimately of little value if companies are not required to put into place reasonable data security systems to protect consumers' sensitive information. In the first instance, these security requirements have to be strong, they should be clear, and they should be flexible to give consumers confidence, while giving companies a fair

opportunity to comply with the law.

And some of this--I was listening to the back and forth with Mr. Pallone and the two witnesses earlier. It seems to me that some of the information they were talking about that might not be covered by the FCC could be covered, and would be covered--currently would be covered by the FTC in its UDAP statute, its Unfair and Deceptive Act or Practice statutes. We can talk about that more in the Q and A.

Second, the bill would replace the ever-changing patchwork of 47 different breach laws with a single Federal standard. A single Federal law reflects the reality that data is in cabin within individual states, but inherently moves in interstate commerce. Consumers in every part of the country are entitled to the same robust protections, and companies are entitled to a logical and coherent compliance regime, and only a bill with state law preemption can accomplish that.

Third, the draft smartly puts enforcement authority in the hands of America's top privacy cop, the Federal Trade Commission, while also empowering each state's Attorney General to enforce the Federal standard. The Federal Trade Commission, under both Democratic and Republican leadership, has, for many years, been our country's foremost protector of data security. The FTC has brought, and you heard this

before from Jessica Rich, brought more than 50 data security enforcement actions in the last 10 years. And the draft would give the FTC more powerful tools, including fining authority, which it doesn't have now, to protect consumers and punish companies for inadequate protections. And moreover, by empowering state AGs to enforce the new Federal standard, the bill will ensure there are no gaps in enforcement. I think this bill is better for consumers than current law.

Mr. Chairman, given the President's strong endorsement for data breach legislation, as well as the growing support of the FTC, we believe you are poised to enact a law that provides strong protections for consumers, and holds companies to a single robust standard. In short, this measure would provide a practical solution to a real problem facing all Americans, and I commend members of this subcommittee for working on a bipartisan legislation.

With your permission, I ask that my full statement be put into the record. Thank you.

[The prepared statement of Mr. Leibowitz follows:]

********** INSERT C **********

Mr. {Burgess.} Without objection, so ordered.

Ms. Cable, welcome to the subcommittee. You are recognized. 5 minutes for your opening statement, please.

|

^STATEMENT OF SARA CABLE

} Ms. {Cable.} Thank you. Good morning, Chairman Burgess, Ranking Member Schakowsky, distinguished members of the subcommittee. Thank you for inviting me here today to testify. My name is Sara Cable, and I am an Assistant Attorney General with the Office of the Massachusetts Attorney General, Maura Healey, and I am here today on behalf of my office to present some of our concerns with the bill.

My comments today are informed by my office's experience enforcing Massachusetts data security and breach laws, which are regarded as among the strongest in the country. My office works hard to use those laws to protect our residents, and we believe that our consumers are better protected as a result. We are encouraged that the Subcommittee recognizes a critical necessity of data security and breach protections. We share this goal. This is our most sensitive information. Yours, mine, our children, our parents, our co-workers, our friends. We are all impacted, and we all deserve robust protections.

We understand Federal standardization is the thrust of this bill. We do, however, have serious concerns that the standards set by this bill are too low, preempt too much, and

hamstring the ability of my office, and that of the other Attorney General offices across the country, to continue our important work of protecting our consumers. It is our concern that this bill would--as drafted would set aside the robust consumer protections that already exist in Massachusetts and many other states, and replace them with weaker protections at a time when strong protections are imperative.

My first point focuses on the bill’s proposed data security standard. We agree strong data security standards are essential. This is how breaches are prevented. This is how the whole business of providing notice of breaches can be prevented. The bill would require ``reasonable security measures and practices.'' Our concern, however, is that it does not specify of delineate precisely what practices or measures are required. It may be true reasonableness is a useful standard in general, but it--standing alone, it is not particularly useful when trying to understand what actual practices and measures are required.

We think that the only way reasonable can be determined under the bill as drafted will be through piecemeal protracted litigation, and the standard will differ from case to case and company to company. It will cause needless confusion, expense, and risk for companies, who are forced to

guess what measures and practices will ultimately be considered by--considered reasonable.

We think Massachusetts has the better approach. It has in place data security regulations that are tech neutral, process-oriented, and, importantly, describe the basic minimum components of a reasonable data security program. Some of those components are--you have heard them from the FTC earlier today, conducting a risk assessment, developing, implementing, and maintaining a written information security program, establishing computer security controls, and many others. The Massachusetts regulations are consistent with those currently in place under Gramm-Leach-Bliley and HIPAA. We believe that they provide stronger protections to our consumers. Our view is that the bill as drafted would erase these strong protections, and, we believe, would ultimately be harmful to consumers.

My second point concerns the scope of the bill's preemption. Put simply, we think it is too broad. It would restrict my office's ability to enforce our own consumer protection laws. It would prevent innovative states from legislating in this field in response to purely local concerns, for example, a breach involving a Massachusetts company and Massachusetts residents only. Under my interpretation, I think the bill might even go further, and

it might possibly restrict states from enforcing, for example, criminal laws relating to the unauthorized access of electronic communications. It might possibly also preempt a state's ability to enforce the security obligations under HIPAA, an enforcement power given to the states under the High Tech Act. These laws, and others, relate to the issue of unauthorized access to data in electronic form, and under the current language of the bill, we believe the--our state's ability to enforce those laws would be preempted.

Finally, the bill hamstrings my office's ability to protect Massachusetts consumers. Currently, under Mass law, we get notice of any breach involving one or more Massachusetts residents. From January 2008 through July 31, 2014 Massachusetts has received notice of over 8,600 breaches, impacting over five million Massachusetts consumers. That is in Massachusetts alone. Under this bill, we would receive none of those notices. We believe this is a critical omission in the bill. It restricts our ability to enforce the requirements of the bill, and we believe ultimately it will make our job of protecting our consumers a lot more difficult.

And with that, I thank the Committee for their--Subcommittee for their efforts, and for inviting me today. Thank you very much.

[The prepared statement of Ms. Cable follows:]

********** INSERT D **********

|

Mr. {Burgess.} The Chair thanks the gentlelady.

Mr. Duncan, welcome to the Subcommittee. You are recognized 5 minutes for the purpose of an opening statement.

|

^STATEMENT OF MALLORY DUNCAN

} Mr. {Duncan.} Thank you, Dr. Burgess, Ranking Member Schakowsky, members of the Committee for inviting us here today, and particularly Congressmen Blackburn and Welch for their efforts to produce this draft legislation. Thank you too for the courtesy and consideration you and your staffs have shown to us and our members over the past many months. The result of those discussions, and undoubtedly many more, is a working draft that is significantly better than introducing--legislation introduced in prior Congresses. We look forward to continue working with you to help turn the draft into a legislative product that will provide increased security and protection for consumers, ameliorate burdens on business, and establish meaningful and reasonable standards for all.

I would like to set out three or four principles that have guided our work. Number one, breaches affect everyone. Every entity that has a significant breach of sensitive data should have an obligation to make that fact publicly known. Public notice serves two goals. First, it provides consumers with information they might be able to use to better protect themselves from identity theft. Second, the fear of public

notice strongly incentivizes companies to improve their security. Both goals are important. Enacting legislation that exempts some entities from public notice, or that perpetuates notice holes that would allow companies to hide breaches undermines both.

Two, if one is a mid-sized regional company, or an e-commerce startup struggling with the consequences of a breach, the existing morass of inconsistent laws are little more than traps for the unwary. We need Federal preemption that works.

Three, if we are going to preempt the state laws, we owe it to the states, and to their citizens, not to adopt a weak law. We should seek legislation that reflects a strong consensus of the state laws and carefully strengthen them where doing so supports the other two principles.

And four, if we are to specifically adopt data security standards, they should not be defined technical standards, and they must be comprehensible and actionable from the perspective of the companies against whom they will apply.

With those principles in mind, I would like to address a few areas of the draft. One, there is not good reason why a breach law should apply a high standard for reporting against some companies, such as retailers, restaurants, dry cleaners, and other small businesses, while requiring little or no

notice from some of the biggest firms in America holding the same sensitive data, be they cloud services like Apple, or payment processors like Hartline when they suffer a breach. Not only does the draft excuse them from general public notice, undermining security incentives, the draft allows big businesses to shift liability for their breaches onto smaller business. This is worse than what exists under the state laws. It must be fixed.

Two, preemption. In general, the preemption language in the draft is much better than in previous Congress's bills. If the notice holes are filled, it could replace the conflicting welter of state requirements with a single strong law. The one area for concern is the clause that specifically excludes some laws from preemption. Federal jurisprudence suggests that when that is done, the entire preemption clause could be placed in jeopardy.

Three, there are portions of the draft that are inconsistent with the considered strong consensus of state laws. For example, we know of no state law that expressly exempts communication service providers, and that would allow them, even when they know they have a serious breach, to get away with providing no notice to anyone at all. That is a notice hold you could drive a truck through.

Finally, as to data security, when the FTC applies

generalized standards to businesses, such as unfairness or deception, as--or, as should be proposed here, reasonable security standards, they are enforced under Section 5 of the FTC Act, which calls for a cease and desist order before penalties can be imposed. The law allows businesses to understand what is intended by the vague standards before they are made subject to massive penalties.

While going directly to damages might be appropriate for an objective on/off requirement, like giving notice within 30 days, it does not make sense when the legal requirement is simply to do something reasonable, or not to be unfair. That is the way the Commission has worked very effectively for over 100 years. Congress should not leave companies subject to fines for practices they could not know in advance, or unreasonable in the eyes of the FTC. That must be remedied.

Thank you for the opportunity to speak today. We look forward to working with you to craft a strong, effective, and fair law.

[The prepared statement of Mr. Duncan follows:]

********** INSERT E **********

|

Mr. {Burgess.} The Chair thanks the gentleman.

The Chair now recognizes Ms. Moy. Five minutes for your opening statement, please.

|

^STATEMENT OF LAURA MOY

} Ms. {Moy.} Thank you. Good morning, Dr. Burgess, Ranking Member Schakowsky, distinguished members of the Subcommittee. Thank you for your shared commitment to addressing data security and data breaches, and for the opportunity to testify on this important issue.

Consumers today share tremendous amounts of information about themselves. Consumers benefit from sharing information, but they can also be harmed if that information is compromised. For that reason, 47 states, and the District of Columbia, all currently have data breach laws on the books, and several states have specific data security laws. Many states also use general consumer protection provisions to enforce privacy and security.

To preserve strong state standards, and the ability to protect protections to the needs of their own residents, a Federal law should set a floor for disparate state laws, and not a ceiling. But, in the even that Congress seriously considers broad preemption, the new Federal standard should strengthen, or at least preserve, import protections that consumers currently enjoy. This bill, however, would weaken consumer protections in a number of key ways. These concerns

must be addressed, and if they are not addressed, it would be better for privacy to pass no bill than to pass this bill as currently drafted. I will highlight five particular concerns.

First, the bill's definition of personal information is too narrow. The bill threatens to weaken existing protections by eliminating state laws covering information that falls outside of its narrow terms. For example, health information, as others have mentioned, falls outside this bill's definition of personal information. As a result, passing this bill would mean eliminating breach notification coverage of that information in Florida, Texas, and seven other states.

Second, this bill would condition breach notification on a narrow financial harm trigger. Data breaches may lead to a number of serious harms beyond merely those that are financial in nature, one reason why seven states in the District of Columbia have no harm trigger at all, and why triggers in another 26 states are not specifically financial in nature.

Third, the bill's general reasonableness security standard would replace the more specific security standard set forth in many state laws, and the FCC's rules implementing the Communications Act. Some states have

specific data security standards in place, and the FCC's CPNI rules require carriers to train personnel on CPNI, have an express disciplinary process in place for abuses, and certify on an annual basis that they are in compliance with the rules. This bill threatens to eliminate these carefully designed security requirements, replacing them with a general reasonableness standard.

Fourth, this bill would supersede important provisions of the Communications Act that protect telecommunications, cable, and satellite customers. Consumers rely on the Communications Act, and the FCC's implementation of it, to protect the very sensitive information that they cannot avoid sharing with the gatekeepers of communications networks. But this bill threatens to replace those protections with weaker standards. In addition, this bill would eliminate protections for the viewing histories of cable and satellite subscribers that fall outside the bill's definition of personal information. The proposed reduction of FCC authority could not come at a worse time for consumers, right as the FCC is poised to apply its Title 2 authority over data security and breach notification to broadband.

The bill strives to eliminate FCC authority only insofar as it relates to information security or breach notification, while preserving the FCC's authority to set privacy controls.

But privacy rules that give consumers the right to control their information are of greatly diminished value when there are no security standards to protect against unauthorized access.

Fifth, the bill could eliminate a wide range of existing consumer protections that may be used to enforce both privacy and data security. The bill is designed to preempt state law and supersede the Communications Act only with respect to information security and breach notification, but in practice it would be exceedingly difficult to draw the line between information security and breach notification on the one hand, and privacy and general consumer protection on the other.

We are not unequivocally opposed to the idea of Federal data security and breach notification legislation, but any such legislation must strike a careful balance between preempting existing laws and providing consumers with new protections. The draft Data Security and Breach Notification Act of 2015 falls short of that balance, but we at the Open Technology Institute do appreciate your commitment to addressing these issues, and we hope to work with you to strengthen the bill and strike a better balance as it moves forward.

Thank you, and I look forward to your questions.

[The prepared statement of Ms. Moy follows:]

```
2443   *************** INSERT F ***************
```

|

Mr. {Burgess.} Thank you for your testimony.

Ms. Weinman, thank you for--welcome to the Subcommittee. You are now recognized for 5 minutes for the purpose of an opening statement.

|

^STATEMENT OF YAEL WEINMAN

} Ms. {Weinman.} Thank you. Chairman Burgess, Ranking Member Schakowsky, and members of the Subcommittee, thank you for the opportunity to testify today. My name is Yael Weinman, and I am the Vice President for Global Privacy Policy and the General Counsel at the Information Technology Industry Council, known as ITI. Prior to joining ITI in 2013, I spent more than 10 years as an attorney at the Federal Trade Commission, most recently as an attorney advisor to Commissioner Julie Brill.

The 60 technology companies that ITI represents are leaders and innovators in the information and communications technology sector. These are companies that are committed to the security of their customers' information. The reality remains, however, that while organizations race to keep up with hackers, these criminals attempt to stay one step ahead. And when a network is compromised, and personal information has been breached, individuals may be at risk of identity theft or financial fraud.

Consumers can take steps to protect themselves from identity theft or other financial fraud following a data breach. Federal breach notification legislation would put

consumers in the best possible position to do so. In the written testimony I provided to you in advance of this hearing, I included the set of nine principles that ITI recommends be included in Federal breach notification legislation. The draft legislation that is the subject of this hearing reflects a number of these important principles. I highlight three.

First, the legislation preempts the existing patchwork in the United States of 51 different regimes. That is 47 states and four territories. Such preemption is critical in order to streamline notices and avoid consumer confusion. Second, the legislation's timeline for notification recognizes that notification can only take place once an organization determines the scope of the data breach, and has remedied vulnerabilities. The timeline included in the draft legislation also permits the necessary flexibility to enable companies to delay notification at the request of law enforcement. Third, the legislation does not require notification if data is unusable, recognizing that power security tools have been developed that avoid risks if data has been compromised.

ITI appreciates how these three important elements are incorporated into the draft legislation. Greater clarity and discussion is needed, however, in a number of areas, and I

highlight three today.

First, the description of the level of risk, and the potential ensuing harm that would trigger the notification, appears to be broad. The threshold of reasonable risk, combined with the phrase economic loss or economic harm could lead to over-notification. It is unclear how economic loss or economic harm is being distinguished from the phrase financial fraud that also appears in the text. Year after year identity theft tops of the list of consumer complaints reported to the FTC, and identity theft or financial fraud are the appropriate triggers for providing consumer notice. And, upon notification, consumers can then take the necessary steps to protect themselves.

Second, with regard to the timing of notification, as currently written, the timeline for a covered entity to notify consumers if a third party suffered a data breach is unclear. The third party needs to remedy vulnerabilities and restore its systems before the covered entity provides notice. The draft should be clarified that the third party will be given the opportunity to restore its system prior to the point in time that the covered entity is required to provide notice to consumers.

Third, the maximum penalty amounts set in the draft legislation are high, $2.5 million maximum for each violation

of the data security section, and a $2.5 million maximum for notice related violations arising from a single incident. These amounts appear punitive, and do not seem to reflect that an organization that suffered a data breach, in most cases, is the victim itself of criminal hackers.

As ITI and its member companies continue to study the draft, and as we gather feedback, we look forward to sharing that with members of the Committee. Thank you, and I am happy to answer any questions.

[The prepared statement of Ms. Weinman follows:]

********** INSERT G **********

|

Mr. {Burgess.} The Chair thanks the gentlelady, thanks all the witnesses for your forthright testimony today. We will move into the question and answer portion of this panel. Recognize myself for 5 minutes for questions.

And, Mr. Leibowitz, if I could, let me start with you. You are familiar with the draft legislation before us. Do you think consumers would be more or less protected with respect to information held by telecom providers under this draft?

Mr. {Leibowitz.} I think--look, my view is that consumers--if this bill were to pass tomorrow, be signed into law, consumers would be in a better position, and let me just tell you why I think that.

First of all, the, you know, the FTC, as the witnesses--both witnesses acknowledged in the previous panel, has been a leader, America's top consumer protection cop, including in the data security area, with more than 50 cases, and hundreds of investigations. There is an emerging consensus, and I think this is critically important, that the most appropriate way to protect personal information, and this is at the core of your bill, is with strong, but flexible, data security standards. It is not with prescriptive rules.

And there is also an ever-changing patchwork of state

legislation. Now, I have seen legislation, when I was at the FTC, that sometimes took state AGs entirely out of the business of enforcing the law. You do not do that, and I think that is critically important, because you want state AGs to be a top cop here. And nobody wants to see any gaps in the legislation. I do not read this legislation as having any gaps, but we certainly want to work with you, if that seems to be the--if--to tweak--to do some tweaking, if that is necessary.

Mr. {Burgess.} Well--and I thank you for that response. So just in general, you--with your experience as Chairman of the Federal Trade Commission, you would interpret this draft legislation as strengthening consumer protections across the board?

Mr. {Leibowitz.} I do. And let me just come back to one question, because it came back in the--came up in the first panel, about the issue dual jurisdiction. And I understand that sometimes the FTC and the FCC work together, and sometimes they can work together as a--very collaboratively.

But just as I believe that the FTC should be the sole Federal enforcer of data security, because I think it does a really good job, and it has expertise, and it is concentrated on that for decades, really going back to the Fair Credit

Reporting Act passed in the 1970s, you know, I also wouldn't want to see, for example, the FCC go into the business of spectrum auctions, right? That is something that the FCC does really well. It is a terrific agency at that, and, you know, I think you should just let each agency play to its strengths and to its expertise. Shouldn't be any gaps in the legislation, I don't believe there are, but that is the way, I think, to sort of improve the protections that companies have to have, and ultimately improve the lives of consumers.

Mr. {Burgess.} Thank you, sir. Ms. Weinman, let me just ask you, you are a former FTC attorney advisor. Tell me what you see is the difference between privacy and security.

Ms. {Weinman.} Thank you for the question. Privacy relates to how an organization uses data, with whom it chooses to disclose that data. Security relates to the underlying security of that information, and the access to which would be unauthorized. That, to me, is the key word in distinguishing between privacy and data security.

Mr. {Burgess.} And is that difference important for the Subcommittee to consider in its drafting of the bill?

Ms. {Weinman.} Absolutely. I think that, in some ways, privacy and data security are often conflated. But I think, with respect to this bill, you do a good job of separating out the two, and focusing on data security. So I think it is

something to keep in mind, because there is often conflation, but I think it is important to keep those two concepts distinguished, and I think this bill does a good job of that.

Mr. {Burgess.} Mr. Leibowitz, let me come back to you just on that issue of privacy and security--data security requirements. Do you feel the bill is doing an adequate job in that regard?

Mr. {Leibowitz.} I do, Mr. Chairman, and, you know, you can look at them as sort of Venn diagrams with a slight overlap. You can look at them as--along the lines of a continuum. But I think you can separate them. I think you do a very good cut in your discussion draft. And you concentrate on what Mr. Welch said, and Mr. Cardenas, and others had said, is the most--and Ms. Brooks said is the most important information here is the personally identifiable information. It is what the hackers really care about, right? And that is what you need to have the highest level of protection for, data security, and you need to give notification to consumers.

Mr. {Burgess.} Very good. My time has expired. I will yield back. I just want to--time for questions is limited, and I do have some questions that I am going to submit, and ask for a written response, Ms. Cable, in particular for you, and some of the issues that happened around the High Tech Act

of Massachusetts, but I will do that in writing.

And I will recognize Ms. Schakowsky. Five minutes for questions, please.

Ms. {Schakowsky.} Before--because he has a bill on the floor, I am going to yield right now out of order, Mr. Kennedy, for questions.

Mr. {Kennedy.} I want to thank the Ranking Member for the generosity, and, Mr. Chairman, thank you for calling the hearing. To all of our witnesses today, thank you for spending the time, thank you for your testimony. I had the pleasure of introducing Ms. Cable this morning from Massachusetts, so thank for being here, ma'am. And I wanted to get your thoughts, as an enforcement lawyer from Massachusetts--we have heard a number of criticisms of the draft bill today, but I would much rather focus on how we can make this bill stronger, or the data security and breach notification aspects a bit better.

So, in your opinion, ma'am, what are some of the most critical data security standards in Massachusetts law that you believe are not represented within the framework of the proposed bill?

Ms. {Cable.} Sure, of course, and I will echo what was previously said by the FTC, and I alluded to in my testimony. You know, this is a framework that includes, at the first

step, an evaluation and assessment. What personal information does the company have, where is it, how do they use it? What are the reasonably foreseeable risks to that information, both internal and external? It is the process of taking stick and evaluating what the risks are that is not reflected in this current draft of the bill that I believe is critically necessary. And you can see that reflected in Gramm-Leach-Bliley standards, and I believe the HIPAA security rule as well.

Stemming from that process are, then, the safeguards that need to be put in place. Again, Massachusetts law leaves open, and gives companies some flexibility, what are the specific safeguards. They include things like restricting employee access to information on an--on a business need basis only. It includes simple things you might not even think about, changing passwords when someone leaves the company, for example.

There is--computer security systems need to be paid careful attention to because of the volume of data they can store, and the many points of access to that data. So perimeter security, such as firewalls, anti-virus protection, software patches. The Massachusetts data security regulations are technology neutral. They leave open, and they contemplate changes in technology and improvement in

procedures, but they establish a minimum concept of protecting your computer's security network. There are many more, but, you know, I think it is a process oriented--it requires a company to take an introspective look at itself and its information, and it is an iterative, evolving process, and I think that is what is important about it.

Mr. {Kennedy.} So, given that, Ms. Cable, do you think that should be--or that framework should be a national benchmark, or what additional requirements do you think you could suggest to further enhance the protection of consumers' data?

Ms. {Cable.} Well, I think it has been--it was suggested in first panel, and it is the concept of FTC rulemaking authority. And I think that is something that--

Mr. {Kennedy.} Um-hum.

Ms. {Cable.} --that our office would support a closer look at.

Mr. {Kennedy.} And maybe that is the answer to this next question, but how can we ensure that the data security standard is responsive to rapidly evolving technologies and increasingly sophisticated cyber attacks?

Ms. {Cable.} I think, you know, giving the FTC the authority and flexibility to, you know, enact regulations that are sufficiently flexible and responsive is one way to

do it. And, you know, I think we--I haven't heard anyone espouse this--the opposite of this proposition, which is these need to be neutral, they need to be flexible. There is a way to do that. There are established frameworks in Federal law that do that.

Mr. {Kennedy.} So if I--just got about a minute left, and a discussion that has come up over this legislation a couple of times now is over preemption. And so, in your mind, and as a practitioner, can you give us some suggestions on--does it have to be all or nothing, or are there some ways we can present--preempt some things, like the content of the notice, for example, but not others, to allow for that flexibility?

Ms. {Cable.} Absolutely, yes. Thank you for the question. I think preemption absolutely does not need to be an all or nothing approach. We have heard the patchwork 47 or 51 different data notice regimes, approximately 12 data security standards. What I hear more, regarding a compliance burden, is with responding to a breach, versus how do you prevent a breach in the first instance.

I think there is some work that might be done in limiting the scope of the preemption to address the specific burdens that are being articulated, and enable a rapid response to a breach. But I think the states are innovative

in the field of data security, I think they are nimble. You know, our view is the preemption is just simply too broad.

Mr. {Kennedy.} I have only got about 10 seconds left. I might submit in writing a question about the--any concerns over the enforcement mechanisms, or the limits on the civil penalties for your consideration.

Ms. {Cable.} Of course.

Mr. {Kennedy.} Thank you for coming here.

Ms. {Cable.} Happy to answer.

Mr. {Leibowitz.} And if I could just add point to respond to your question? I mean, these are--

Mr. {Kennedy.} Yeah.

Mr. {Leibowitz.} It is my--it is on my time, or--

Mr. {Kennedy.} It is not.

Mr. {Leibowitz.} --on your time?

Mr. {Kennedy.} It is up to the Chairman.

Mr. {Leibowitz.} If it is--if the Chairman--

Mr. {Burgess.} Gentleman may respond.

Mr. {Leibowitz.} --unanimous consent? Thank you. Again, you raise very good questions about how to think through the next iteration--

Mr. {Kennedy.} Um-hum.

Mr. {Leibowitz.} --and, obviously, we want to work with you to--

Mr. {Kennedy.} Um-hum.

Mr. {Leibowitz.} --do that.

Mr. {Kennedy.} Okay. Thank you. I appreciate it.

Mr. {Burgess.} Chair thanks the gentleman, gentleman yields back. Chair recognize the gentlelady from Tennessee, Ms. Blackburn. Five minutes for questions, please.

Mrs. {Blackburn.} Thank you all, and I appreciate the conversation, and--that you would be here and weigh in on the discussion draft. Mr. Leibowitz, I have to say, it looks normal and natural to see you at that witness table, and we are happy to have you back.

Ms. Weinman, I want to come to you first. We haven't talked a lot about the third party notice obligations, so I would like to have you walk through what you see as the strengths and weaknesses of the third party notice obligations.

Ms. {Weinman.} Thank you for the question. I will begin by setting the stage with some defined terms. So the covered entity is generally the entity that has the relationship with the customer, or the consumer, use whichever word you are more comfortable with. And then the third party, or another term used in here would be a service provider, is the one that might perform services on behalf of that covered entity, but would also have personal information

in their possession as a result of their B to B relationship with the covered entity, business to business.

So the gap that I pointed out in my oral statement is that it is unclear when the covered entity would be required to provide notice to its customers when the third party suffered a breach. It is very clear when the covered entity would have to provide notice when it itself had been breached, but when the third party had been breached, it is unclear whether the timeline begins when that third party has had the opportunity to determine the scope of its breach, and had taken steps to remedying vulnerabilities, and restored its systems.

Mrs. {Blackburn.} Okay. Let me ask you something else. You mentioned the amount of compliance time, with businesses having to comply with all the different state laws. So is there any way that you can quantify what this would save to businesses by having preemption in place, and having a national standard? Have you thought through it in that regard, as--the cost savings to business?

Ms. {Weinman.} I don’t have a quantifiable number, in terms of compliance costs. That is not something that I have put together. I can point out, though, in terms of--the compliance costs would be considerable, considering the legal time. The redirection of resources that could be devoted to

other critical areas once a data breach occurs is also a question of opportunity cost. If you are spending a lot of time figuring out your notice regime with 51 different frameworks, that is taking time and money away from other areas that you can be focusing on--

Mrs. {Blackburn.} Okay.

Ms. {Weinman.} --following a data breach.

Mrs. {Blackburn.} Mr. Duncan, I saw you shaking your head. Let me come to you on that, because you mentioned in your testimony that you all have for years called on Congress to do something on breach notification. You also talk about modeling a Federal bill on strong consensus of existing state laws, and, in the context of third party notification, all of the existing state laws require notice from a third part to a covered entity after a breach.

So I want you to talk to me about two things. I want you to reconcile your support for a national standard based on the state laws with your issues regarding the structure of the state laws for the third party. And then also I want you to talk a little bit about cost, and the preemption, and what it would do to--what it would save consumers and businesses in the process.

Mr. {Duncan.} Thank you, Congressman Blackburn. There are three very good questions. In terms of the states,

virtually all of the states do have an arrangement by which third parties would report directly to the entity for whom they were providing, say, a service, and that would be the general rule. What has become increasingly clear to the--to a number of state Attorney Generals is that trying to provide notice like that in every situation actually will not provide effective notice.

There is an example, for example, in our testimony that talks about the Hartline breach, which was a huge breach. 80 million data points, I believe, realized. And in that case, Hartline did the right thing. It didn't follow the state laws. In fact, it went beyond them, and provided the notice itself directly. Had they done otherwise, because Hartline was a payment processor for hundreds of retailers, it would have had--told each of them, and each of them would have had to tell all their customers about Hartline's breach, so consumers would have received hundreds of notices for what was actually one breach.

So there is becoming a realization among the state AGs that we are--really should be focusing on effective notice, rather than this strictured--structured notice that is contained in some of the state laws. So it is an evolution of that. This presents a double problem when we go to the subset that Ms. Weinman just talked about, which was service

providers, because in this case, under the draft language, in some circumstances, they would provide no notice at all, and that certainly--it shouldn't be a situation that someone who knows they have a notice--knows they have a breach can find themselves in a situation in which they say nothing to anyone, not even to law enforcement.

And finally, as to cost, this is a very significant consideration. You must consider that this law is going to apply not just to the largest companies in America. It is going to apply to the first person who has 15 dry cleaner front--shops. How much will he or she have to stay up at night, wondering about whether or not they have met an amorphous data security standard to--going forward? And that imposes tremendous costs on the operation of our businesses.

Mrs. {Blackburn.} Mr. Chairman, my time has expired, and I will yield back, but I would ask Mr. Leibowitz, I can see that he was trying to respond to that, just to submit in writing his response, or someone later can call on him for his response to that question.

Mr. {Burgess.} Chair thanks the gentlelady. Gentlelady yields back. Recognize Ms. Schakowsky. Five minutes for questions, please.

Ms. {Schakowsky.} Thank you, Mr. Chairman. So I haven't heard anyone, except for Mr. Leibowitz, say that if

the bill were to pass as is that consumers would be better protected. I didn't hear the first panel or the second panel--it seemed to me that lots of people--everyone had suggestions of how the bill could be made better. If I am wrong, would you tell me that? Okay. So I--and Mr. Leibowitz also said he is happy to work with us, so I think we have some work to do.

I wanted to ask a question about personal information that has come up several times. And--so when--let me ask Ms. Cable. In terms of personal information, what does your law include? And I want to ask Ms. Moy kind of a more global--other states as well. Go ahead, Ms. Cable.

Ms. {Cable.} Thank you for the question. For Massachusetts, the definition of personal information is actually narrower than what is being considered in this bill. It includes name--first name and last name, or first initial and last name, plus one of the following components, Social Security Number, driver's license number, or other government issued ID number, and that is state government issued ID number, or a financial account number with or without the security code required to access the account.

Ms. {Schakowsky.} So many of us, I think, think that the requirement in the bill is too narrow, that it is just financial harm. And I would like to get Ms. Moy, if you

could answer, what kind of information do you think is missing now that we are taking this important step of looking toward protecting consumers. What do you think ought to be there?

Ms. {Moy.} Thank you. Thanks so much for this important question. So, as I mentioned in my testimony, there are a number of pieces of information that are covered by other laws. In particular, health information is covered by a lot of states. But I think, you know, we could go back and forth about particular pieces of information that should or should not be included in the definition of personal information here, but the big picture here is really--the bottom line is that there are broad categories of personal information that are currently covered under a number of state laws, and under the--

Ms. {Schakowsky.} Well, let me ask you this, then, because I think it would be--help to outline for us. You noted that this bill does not protect the serious harms that a breach of information could cause, so I am wondering if you could draw a picture for us of what some of those serious harms could be.

Ms. {Moy.} Sure. So, for example, you could imagine that if your e-mail address and password were compromised. So that might not be a--an account identifier and a password

that is necessarily financial in nature, and would fall within the scope of this bill, but if my personal e-mails were compromised, I am--I would certainly experience some harm. I am sure I would experience not only emotional harm, but perhaps harm to relationships, perhaps harm to reputation. And, you know, and I think that the--a common sense question here is just, if my e-mail address and account password were compromised, would I want to be notified? And--absolutely. I think that is just there--just some common sense there.

Ms. {Schakowsky.} Let me ask you this. Are--let us say a woman is a victim of domestic violence--

Ms. {Moy.} Um-hum.

Ms. {Schakowsky.} --but geolocation is not protected. Could she be at risk in some way?

Ms. {Moy.} Right, thank you. So I think one of the things that I did highlight in my written testimony is that because both of--the definition of personal information, and the harm trigger that is premised on financial harm, there are categories of information, like geolocation information, or like information about call records, that, if compromised, could result in physical harm. So a domestic violence victim, for example, might be concerned not only about her geolocation information, but perhaps about her call records.

If she called a hotline for victim assistance, or if she called a lawyer, those are pieces of information that she absolutely would not want to be compromised.

Ms. {Schakowsky.} In terms of the role of the FTC having some flexibility in defining what personal information would be, what position have you taken?

Ms. {Moy.} Right. So I think it is--I think that it is critical that we provide for flexibility in the definition of personal information in one way or another. Whether it is through agency rulemaking, or through state law, it is really important that we be able to adapt a standard to changing technology, and changing threats.

So I mentioned in my testimony the growing trend of states including medical information in their definition of personal information. In fact, two states just this year have passed bills that will include that information in their breach notification later this year, and that is not an arbitrary change. The reason that that is changing is because there is a growing threat of medical identity theft, and it is really important to build in flexibility to account for those changes.

Mr. {Leibowitz.} And if I could just follow up on Ms. Moy's points very quickly, in support, I think, of most of them. You know, I think geolocation--and your point. I

think geolocation is critically important. When we were at the FTC, we expanded geolocation under COPPA to be a condition present. It is something you may want to take a look at.

It is also important to note that the Massachusetts law, which is one of the most progressive laws of the state, has a narrower definition of data security. This is a well-intentioned piece of legislation, and reasonably we can disagree about where to draw the line, but it is broader than 38 states, that don't have it.

And then the point--I--the other two very quick points I want to make, on the ISP point that you mentioned before, Mallory--Mr. Duncan, you know, if a service--aware of a data security breach, they must notify the company of the breach, and they have an obligation to reasonably identify any company, to try to reasonably identify.

And then, finally, on rulemaking, obviously, I came from the FTC, I came and testified in support of this legislation, or signed testimony. I would just say, and maybe this is overall for the legislation, this is my belief in it, it always was when I was there, is you just don't want to let the perfect be the enemy of the good here. You want to make sure you move forward for consumers. Reasonable people can disagree about exactly where that is, but getting some things

sometimes is better than, you know, not getting everything.

Mr. {Burgess.} The Chair thanks the gentleman for his observations. Gentlelady's time has expired. Chair recognizes the gentlelady from Indiana, Ms. Brooks. Five minutes for questions, please.

Mrs. {Brooks.} Thank you, Mr. Chairman, and I want to build on what the gentleman from Massachusetts was saying, is that we have to get this right, and--perfect is the enemy of good here. And I have heard--I am not familiar with Massachusetts statute, and, obviously, with there being so many statutes, the problem is that we in Congress, while we have been talking about it for years and years and years, and I applaud all the work that has been done in Congress in the past, we have got to move something forward here, because terrorist organizations, nation-state organizations, are continue--they are going to always continue to come up with more ways and new ways to hack and get this information.

And it is becoming, I think, one of our constituents' greatest security concerns, truly, and we have got to get this right. And I don't believe that having 51 different standards is good. We have got to get, you know, we have got to move on this and improve. And I think--my previous question to the director of the FTC, the reasonable security practice, and if we were to adopt, for instance,

Massachusetts, how you have set out, and what I would love to see is the state Attorney Generals work with the Committee and the members who have put forth this legislation, and let us get this right.

And so if--for instance, if the reasonable security practices that you delineate in Massachusetts, those are flexible, but yet they set out the process, would that satisfy you on the reasonable security piece, Ms. Cable?

Ms. {Cable.} Yes, thank you for the question, and I agree and appreciate this is a critical issue, and action--there needs to be action, and I really applaud the Subcommittee for taking up this issue, because it is complicated and it is difficult.

I think, you know, I happen to very much like the Massachusetts data security regulations, but, of course, I have to say that.

Mrs. {Brooks.} Sure.

Ms. {Cable.} I think they are, however, a good framework, a recognized framework, and something that commercial entities are used to seeing. And I think the issue with preemption, what makes it concerning to us, is the standard of data security that is being set. We don't think it is sufficiently defined, and therefore we think, as a result, it may not be sufficiently robust. And so, at least

from Massachusetts perspective, this is not better off for our consumers if reasonable security measures and practices result in a downward harmonization across the nation of a lower standard of security.

And I might add, lower security, logically, I think, will result in an increased incidence of breaches, an increase in notice obligation, and an increase of all of the problems we are discussing today. I really think the data security standard is a critical element. I think the reasonableness standard is maybe a good lode star guidepost, but this--the measures and practices need to be more defined.

Mrs. {Brooks.} Mr. Leibowitz, would you like to comment on those remarks?

Mr. {Leibowitz.} Well, I mean, at 50,000 feet I agree that you don't want to ratchet down, you want to ratchet up the level of data security. I think the fact that 38 states don't have any data security obligations at all is very telling. And, again, as Ms. Cable acknowledged, you know, one of the most progressive pieces of legislation that states have written is the Massachusetts law. On the data security side, it has a narrower definition.

So I think, again, and going back to Mr. Welch's point and Mr. Cardenas's point, it is like what do people care about when--what hackers care about, they care about the

personal identification and the financial information. And what do consumers care about, and at the FTC--and the FTC continues to do great work here, you know, they care about their Social Security Number. They care about their financial information being taken. They care about, you know, economic harm more than anything else. And that is what drives this problem more than anything else. It is not ideological groups. It is, you know, people engaged in fraud and criminal activities that the FTC and the state AGs have been prosecuting, will continue to be able to do in the bill.

Mrs. {Brooks.} Thank you. And one completely different issue, Ms. Weinman, you talked about the providers must restore their system, that entities should restore their system before notification. Can you explain why that would be necessary when it does seem that speed in getting out notifications--although we know that often those who are breaching and hacking can sit on this information for years, they don't often use it immediately. But why do you propose that an entity needs to have the time to restore its system, as you have said, before notification?

Ms. {Weinman.} As currently drafted, the bill does allow that restoration of system on--for a covered entity, and I think it is critical that that be the case because if an entity provides notification, it is essentially making

public that its system has been compromised, and it could render itself further vulnerable to additional attacks by those same hackers, or other hackers. So I thank, and applaud, the Subcommittee for recognizing that point in time when notification should begin should be at a time when the system has been restored.

Mrs. {Brooks.} Thank you. I yield back.

Mr. {Burgess.} The Chair thanks the gentlelady, and Chair recognizes gentleman from Vermont, Mr. Welch for 5 minutes for questions.

Mr. {Welch.} Thank you very much, sir. I want to take up a bit from where my colleague, Ms. Brooks, was with the Attorney General's Office from Massachusetts. First of all, thank you for your testimony. Second, thanks for the good work that Massachusetts does. Third, we are pretty proud of our Attorney General and consumer protection in Vermont. They have a standard and an--they have a solid standard, and an aggressive consumer protection division, like you do, and they have made some of the same arguments to me about this bill that you just made, so message received.

But I just wanted to go through a few things. Number one, the bill does use this term reasonableness, and I think there has been a debate, even--not--on all sides, including among consumer activists, whether something that is flexible

has the potential to meet the challenges as they emerge, as opposed to--what I heard in your testimony is a more detailed set of guidelines that is--according to your testimony is working for you.

But I guess I am just looking for some acknowledgment that there is a legitimate argument to approach it in a prescriptive way, or in a general way that gives a little more flexibility to the enforcer, in this case Massachusetts. Would you agree with that?

Ms. {Cable.} Yes, thank you for your question, and I would reiterate I work closely with colleagues from the Vermont Attorney General's Office. It is a fantastic office, and I enjoy working with them. I think the issue of data security standards, and whether they are flexible--

Mr. {Welch.} Right.

Ms. {Cable.} --flexible or prescriptive, I think you can have standards that articulate components of what a data security system framework should look like, but an awful lot of flexibility with how you meet those standards, and I--

Mr. {Welch.} Well, right, and that is where it is genuinely difficult. Because, you know, if Ms. Brooks was able to get all the Attorney Generals to come up with what was the best approach, that might be persuasive to all of us, because there are Republican and Democratic Attorney Generals

out there.

A second thing that I wanted to talk about is this question of an obligation on the part of the companies. There is an enormous incentive for thieves, criminals, to try to hack our information. They get our money. There is an enormous incentive--I am looking for all you--your reaction on this--for companies to have their computer systems be as safe as possible, because they are victims too in this case. I mean, look what happened at Target. People lose their jobs. It is brutal on the bottom line for these companies. So I see that as a practical reality that we can take advantage of. I mean, is that consistent with you, as an enforcer?

Ms. {Cable.} I would absolutely agree, and I would note, you know, much of my effort is not spent trying to find gotcha moments and--

Mr. {Welch.} Right.

Ms. {Cable.} --enforcing. We have received notice of over 8,600--

Mr. {Welch.} Yeah.

Ms. {Cable.} --breaches, and I think, we ran the numbers, we have had 13 actions.

Mr. {Welch.} But you would be in agreement--

Ms. {Cable.} I would, and I would--

Mr. {Welch.} Yeah.

Ms. {Cable.} Most of my time is spent--

Mr. {Welch.} I don't have much time, so let me get a--

Ms. {Cable.} Of course. I apologize.

Mr. {Welch.} --few more. You have been very helpful. The other thing Mr. Duncan was talking about, effective notice, and this goes back, again, to kind of practicality. If I get these bank notices when I do this mortgage refinancing, it literally gives me a headache, and I get less information. All I need to know are three things, what is my rate--what is my interest rate, when is the payment due, and what is the penalty if I don't meet the time? That is all I need to know. And--so this effective notice issue, I think, is something that, on a practical level, all of us want to take into account.

So let me go, Ms. Moy, to you. I want to, first of all, thank you and your organization for the great work you have done, and also for being available to try to answer my questions.

Ms. {Moy.} Thank you.

Mr. {Welch.} You had mentioned something that every single one of us would be really concerned about, if there was any way that we were passing legislation that was going to make a woman of domestic violence more vulnerable. All of

us would be against that, okay? So I don't see in this legislation how that is happening, but if, in your view, it is, I would really welcome a chapter and verse specification as to what we would have to do to make sure that didn't happen. And I think we would all want to be on board on that. So could you help us with that--

Ms. {Moy.} Thank you, I appreciate that question, and I have appreciated working with your office as well. So I think, you know, this is--this question mostly gets to what the--what standard is set for the harm trigger, right? I mean, because there are certain types of information, or certain situations where information may be compromised or accessed in an unauthorized manner, and you could look at that situation and say, this information really couldn't be used for financial harm, or we think it is unlikely that that is the--that was the motivation of the person who accessed that information.

Mr. {Welch.} Okay. My time is running up, so I--

Ms. {Moy.} Yes.

Mr. {Welch.} --apologize for interrupting, but if--

Ms. {Moy.} Um-hum.

Mr. {Welch.} --you sent us a memo on that, and--

Ms. {Moy.} Absolutely.

Mr. {Welch.} --Attorney Cable, if you sent us some

specifics, I--that would be helpful to the Committee, because I know Ms. Schakowsky was very interested in a lot of the points you made, as well as all of us, I think.

Ms. {Moy.} Absolutely.

Mr. {Welch.} Thank you.

Ms. {Moy.} Thank you.

Mr. {Welch.} I yield back.

Mr. {Burgess.} Chair thanks the gentleman. Chair recognizes the Vice Chair of full--of the Subcommittee, Mr. Lance. Five minutes for questions, please.

Mr. {Lance.} Thank you very much, Mr. Chairman.

Mr. Leibowitz, in your opinion, what benefit have class actions brought to consumers after a data breach?

Mr. {Leibowitz.} Well, let me start by saying, I think class actions have an enormous value in a lot of areas. Civil rights areas, others as well. In this area, I don’t think that class actions have much benefit, except for the lawyers who bring them. And what they also do is they incentivize, or the create incentives, I think, for companies to emphasize legal protections, rather than actual reasonable data security.

And I will just make sort of one other point, which goes back to the FTC, which is, if the FTC brings a case, and it gets compensation for consumers, all that compensation goes

back to the consumers. They--$200 million to 400,000 people who were victims of mortgage service fraud by Countrywide, and that is one other benefit. But I also believe that, you know, class actions can be vitally important, as I am sure you do, in some areas.

Mr. {Lance.} In other words, your point is that when the FTC does it, the--FTC personnel are in the public sector, and the full benefit goes to those--

Mr. {Leibowitz.} The entire--

Mr. {Lance.} --who have been harmed?

Mr. {Leibowitz.} Yes.

Mr. {Lance.} It is an indication why we should be supportive of our Federal workforce--

Mr. {Leibowitz.} And--

Mr. {Lance.} --and for colleagues who serve in Federal service. Would others like to comment on that? Attorney General Cable?

Ms. {Cable.} If I may?

Mr. {Lance.} Certainly.

Ms. {Cable.} Thank you, Congressman.

Mr. {Lance.} Certainly.

Ms. {Cable.} I would just note--consumer restitution is a critical tool that we have in our toolbox under our Consumer Protection Act. We use it--we like to use it. If

we can get the money, we distribute it. I noted under this version of this bill, it does not expressly allow us to seek consumer restitution, and it also denies the consumer a private right of action. We think that is a bit of an oversight in the event a consumer is actively harmed here. State AGs under this bill would not be able to seek consumer restitution, under one interpretation.

Mr. {Lance.} Thank you, Attorney General. Mr. Leibowitz, do you wish to comment further or not? No? Thank you.

Mr. {Leibowitz.} No, sir.

Mr. {Lance.} Ms. Weinman, do you have a concern about state common law claims adding additional security or notification requirements for companies if a Federal law is enacted?

Ms. {Weinman.} I think that this bill strikes a useful balance in pre-empting the current state data security requirements and the breach notification, so I think this bill strikes a good balance in that area.

Mr. {Lance.} And you believe that because the country would move forward uniformly, and this would be something that would be on the books for the entire nation?

Ms. {Weinman.} Yeah, and it would streamline the notification process across the board, across the 51 regimes

for which I have, you know, a 19 page chart. So I think that would definitely be useful.

Mr. {Lance.} Yes. Thank you. Mr. Chairman, I yield back the balance of my time.

Mr. {Burgess.} Chair thanks the gentleman. Chair recognizes the gentleman from New Jersey, Mr. Pallone. 5 minutes for questions, please.

Mr. {Pallone.} Thank you, and I have been to, like, three different meetings since I was last here, so hopefully I will be understandable here. Under current law the FTC does not have enforcement authority over common carriers, including telecommunications, cable, and satellite services, and the discussion draft lifts the common carrier exception to allow the FTC to bring enforcement actions for violations of the provisions of this bill.

And I wanted to ask each member of the panel, and I am just looking for a yes or no because I have a whole series of things here, if you could just say yes or no, assuming the draft did not include preemption of the Communications Act in Section 6C, do you support lifting the common carrier exceptions in the context of data security and breach notifications, yes or no? We will start to the left.

Mr. {Leibowitz.} Yes.

Mr. {Pallone.} Ms. Cable?

Ms. {Cable.} I have--I apologize, I think I am out of my expertise, so--

Mr. {Pallone.} You have no response?

Ms. {Cable.} I have no response.

Mr. {Pallone.} All right. Mr. Duncan?

Mr. {Duncan.} We don't have a preference as to which agency covers it.

Mr. {Pallone.} That is--

Mr. {Duncan.} The only requirement is that everyone be covered.

Mr. {Pallone.} Okay. Ms. Moy, yes, no?

Ms. {Moy.} If it did not eliminate provisions of the Communications Act, yes.

Mr. {Pallone.} Okay. And our last--

Ms. {Weinman.} I will give a similar response to Mr. Duncan, that it is not an issue that would implicate ITI members, so--

Mr. {Pallone.} All right.

Ms. {Weinman.} --I am not expressing a preference one way or the other.

Mr. {Pallone.} All right. Now I just want to ask my next two questions of Ms. Moy, because I may not have a lot of time. Lifting the common--I have two. First, lifting the common carrier exception without nullifying the data security

and breach notification provisions of the Communications Act would mean that there are two cops on the beat, so to speak, so what are the benefits to joint jurisdiction among the FCC and the FTC? To Ms. Moy only.

Ms. {Moy.} Thank you, thank you so much. So I think one of the major benefits is that the two agencies have different strengths, and they could work together to use their strengths to complement each other and ensure the best protection for consumers. For example, the FCC is primarily a rulemaking agency that uses its authority to set standards prospectively, and the FTC is primarily an enforcement authority. It would be really nice if they could work together to establish the standards in the first place, and then enforce them in the second place.

I think also the FCC has a lot of very important expertise in this area, working with telecommunications networks, and other communications networks, and just--and the focus on privacy is a little bit different. The focus on privacy at the FCC is more about the reliability of the networks, and the fact that consumers have no choice but to share information with these very important networks in their lives, whereas the focus of the FTC on privacy is a little bit more about what is fair with respect to consumers. And, again, it would just be really nice if those agencies could

work together in that area to use their expertise, or their respective expertise, in a complementary manner.

Mr. {Pallone.} And then I have a second one to you only, and if I have time, we are going to go to the others. Do you think there are any drawbacks to having FTC and FCC enforcement? Are you concerned about consumers being confused by having two enforcing agencies?

Ms. {Moy.} I am not concerned about that. I think that where we have seen agencies work together in the past, I don't think that there really is confusion for consumers. For example--I am sorry, I am blanking, but the FTC and the FCC have worked together on the, for example, Do Not Call, and--of telecommunications customers. And I really don't think that there is any risk of confusion for consumers of having those agencies work together.

Mr. {Pallone.} All right, one more question. I will start with you, and then--we have time, we will go to the others. Do you have any suggestions for how legislation can ensure that companies are not burdened by duplicative enforcement?

Ms. {Moy.} I am sorry, that companies are not burdened by--

Mr. {Pallone.} By duplicative enforcement. Any suggestions for how legislation could ensure that companies

are not burdened by duplicative enforcement?

Ms. {Moy.} Well, I think that--I mean, the premise of the question is that duplicative enforcement is necessarily more burdensome for companies, and I don't think that that is necessarily the case. You know, as I said, the FCC and the FTC can work together and use--and--to formulate standards and enforce them in a uniform way. And I think that they would have an incentive to do that, so as not to--so as to maximize the efficiency of their resources toward that goal. And I think that that incentive would sync up quite nicely with the incentive of companies--of having the two agencies work in step with each other, so as not to seem like two separate--totally separate regimes.

Mr. {Pallone.} All right, thanks. I think I have run out of time, Mr. Chair.

Mr. {Duncan.} If I--

Mr. {Pallone.} Thank you.

Mr. {Duncan.} If I might just mention, on that point, under the structure of the bill, both the FTC and the state AGs would have enforcement authority, and that is an option that works, at least in that context. From our perspective, as long as everyone has the same obligations, and duties, and responsibilities, then it is less of an issue.

Mr. {Leibowitz.} Yeah. And the only thing I would add

is that there is a--sort of an evolving consensus that what you really want, Mr. Pallone, is a flexible enforcement standard that is strong with enforcement. And you also want to treat the same information the same way, not under different regimes. So, you know, Google can collect information, Verizon can collect information, Comcast can collect information. A variety of other companies can.

And, for the most part, I think where this bill wants to go is in a data breach context. And in the data security context, more importantly, treat them equally.

Mr. {Burgess.} Chair thanks the gentleman. Gentleman's time has expired. Chair recognizes Mr. McNerney. Five minutes for your questions, please.

Mr. {McNerney.} Well, I want to thank the Chairman and the Ranking Member for allowing me to participate in this hearing, even though I am not a member of the Subcommittee. I appreciate that. And I want to say I appreciate the efforts of my colleagues, Mr. Welch, Mr. Burgess, and Mr.--Mrs. Blackburn for crafting this bill. It is clearly needed. And it may not be perfect yet, but it can be improved, and it is much better to start from the draft than to start over--than to over to start over. So I have a couple of questions here.

Ms. Weinman, you mentioned that the civil penalties for

breach of notification are excessive for a company that is a victim of a criminal act. Do you think it would be okay to lower the penalties, or to have some flexibility? And if you think flexibility is the way to go, how can you do that in this kind of a bill?

Ms. {Weinman.} I think lowering would be a good step, and I think there is flexibility built into the assessment of civil penalties within the bill, but I think lower the maximum penalties would make sense in the context of the fact that companies themselves are the victims of criminal hackers. So there is some discretion with regard to civil penalties within the bill, however I do think the maximum amounts set out in there should be lower. And I note that the current figures in there are, in fact, five times higher than what we have previously seen in other proposals, so I just make a note of that.

Mr. {McNerney.} Well, I mean, you could consider some breaches to be gross negligence, and deserving of significant penalties, so--

Ms. {Weinman.} Well, that flexibility is built into the language, but I do think that the ceiling could be lower in the draft.

Mr. {McNerney.} Thank you. Ms. Moy, you know, preemption is a very tricky issue. We want states to have

flexibility, but you mention that there ought to be a floor. But how could you create legislation that had a floor, but allowed states like Massachusetts flexibility to go, you know, more stringent, if they wanted?

Ms. {Moy.} I think--thank you for the question, and thank you. I do recognize that it is very difficult to craft the appropriate standard here, and thank you for taking up this difficult issue. I, you know, I think that you could set a standard that says, this is the minimum standard, and that state laws will not be preempted to the extent that they create additional standards above that, or beyond that.

But, you know, but also, as I have said in the written testimony, and as I mentioned earlier, we are not necessarily opposed to the idea of preemptive legislation, but I do think that it is important, if we are going to do that, to ensure that the new Federal standard, the new uniform Federal standard, is better for consumers than the current draft. I just--I think it is really important to strike the proper balance between preemption and protections for consumers, and this just doesn't quite get us there.

Mr. {McNerney.} Now, you mentioned that you felt that the draft would lower consumer protections over a wide range of consumer protections. Could the bill be strengthened to include those current protections?

Ms. {Moy.} I believe that it could be, and I think--I would be very happy to work with the Subcommittee to figure out ways that we could get there.

Mr. {Duncan.} Congressman--

Mr. {McNerney.} Thank you.

Mr. {Duncan.} --one of the reasons that we are here today is because there are already 51 conflicting laws out there. If Congress doesn't simplify the system to some extent, then we will simply have 52 laws out there, and that is not moving us forward.

Mr. {McNerney.} Thank you. Well, Mr. Duncan, you mentioned that--the importance of enacting laws that holds accountable all entities that handle personal information. Can you discuss how you would improve the draft legislation to modify the covered entities?

Mr. {Duncan.} Certainly. We would expect that a good law would require that every covered entity have the same obligation, that third parties--for example, the way the bill is written now, some entities do not even have a duty to determine--to examine and determine whether or not they can find information out about a breach. There has got to be the same level requirement all the way across the board.

Congresswoman Schakowsky asked earlier whether or not we could support this legislation. I would say this draft is a

major improvement over what we have seen before, but if we could have equal applicability across all entities, and fix some of the issues with the FTC, we could support this.

Mr. {McNerney.} Thank you--a lot of good information has come out that might help improve the bill, so, Mr. Chairman, I yield back. Thank you again.

Mr. {Burgess.} Chair thanks the gentleman. Gentleman does yield back. The Chair recognizes Mr. Pallone of New Jersey for a unanimous consent request.

Mr. {Pallone.} Thank you, Mr. Chairman. I ask unanimous consent to submit for the record a letter from 12 consumer groups to yourself and Ms. Schakowsky.

Mr. {Burgess.} Without objection, so ordered.

Mr. {Pallone.} I guess we have another one too, Mr. Chairman, from the Consumers' Union, in addition to the one from everyone else.

Mr. {Burgess.} The Chair thanks the gentleman. Without objection, so ordered.

[The information follows:]

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

|

Mr. {Burgess.} Seeing that there are no further members seeking to ask questions, I do want to thank all of our witnesses. I know this has been a long hearing, but I thank you for participation today.

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 National--of the Credit Union National Association, a letter on behalf of the Marketing Research Association, a letter on behalf of the National Association of Federal Credit Unions, a letter on behalf of the Online Trust Alliance, a letter on behalf of the Consumers' Union, statement on behalf of the National Association of Convenience Stores, a letter on behalf of the American Bankers' Association, the Clearing House, Bankers' Consumer Association, Credit Union National Association, Financial Services Roundtable, Independent Community Bankers of America, and the National Association of Federal Credit Unions, and the response of the Secret Service to questions submitted for the record at our previous Subcommittee data breach hearing on January 27, 2015.

[The information follows:]

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

|

Mr. {Burgess.} Pursuant to Committee rules, I remind members they have 10 business days to submit additional questions for the record, and I ask witnesses to submit their response within 10 business days upon receipt of the questions. I thank everyone for their participation this morning. This Subcommittee hearing is adjourned.

[Whereupon, at 1:15 p.m., the Subcommittee was adjourned.]