NEAL R. GROSS & CO., INC.

RPTS WALTER

HIF166160

FCC OVERREACH:

EXAMINING THE PROPOSED PRIVACY RULES

TUESDAY, JUNE 14, 2016

House of Representatives,

Subcommittee on Communications and

Technology,

Committee on Energy and Commerce

Washington, D.C.

The subcommittee met, pursuant to call, at 10:15 a.m., in Room 2123 Rayburn House Office Building, Hon. Greg Walden [chairman of the subcommittee] presiding.

Members present: Representatives Walden, Latta, Shimkus, Blackburn, Lance, Guthrie, Olson, Pompeo, Kinzinger, Bilirakis, Johnson, Long, Collins, Cramer, Eshoo, Welch, Yarmuth, Clarke, Loebsack, Rush, Matsui, McNerney, and Pallone (ex officio).

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

Also present: Representative Schakowsky.

Staff present: Rebecca Card, Assistant Press Secretary; Melissa Froelich, Counsel, Commerce, Manufacturing, and Trade; Kelsey Guyselman, Counsel, Telecom; Grace Koh, Counsel, Telecom; Paul Nagle, Chief Counsel, Commerce, Manufacturing, and Trade; David Redl, Chief Counsel, Telecom; Charlotte Savercool, Professional Staff, Communications and Technology; Dan Schneider, Press Secretary; Dylan Vorbach, Deputy Press Secretary; Gregory Watson, Legislative Clerk, Communications and Technology; Michelle Ash, Minority Chief Counsel, Commerce, Manufacturing, and Trade; Jeff Carroll, Minority Staff Director; David Goldman, Minority Chief Counsel, Communications and Technology; Tiffany Guarascio, Minority Deputy Staff Director and Chief Health Advisor; Jerry Leverich, Minority Counsel; Lori Maarbjerg, Minority FCC Detailee; Matt Schumacher, Minority Press Assistant; Ryan Skukowski, Minority Senior Policy Analyst; and Andrew Souvall, Minority Director of Communications, Outreach and Member Services.

Mr. Walden. Good morning, everyone. I would like to thank our witnesses for joining us today to offer their expert counsel as we convene the Subcommittee on Communications and Technology hearing on FCC Overreach: Examining the Proposed Privacy Rules.

Today's hearing is a direct result of the FCC's premeditated efforts to supersede the Federal Trade Commission's successful, enforcement-based approach to consumer privacy with its own predetermined vision of what consumers want and how the Internet should function. The hearing title aptly sums up this approach up as an "overreach," but fails to convey the scope of the damage the Commission's actions could have on consumers. The Commission shortsightedly looks at one just piece of the Internet and despite evidence to the contrary assumes that regulating it will improve privacy. The Commission shortsightedly overlooks the history of this industry and the value of innovation in ISP service offerings. And, the Commission overlooks the value of competition, both among ISPs and between ISPs and other online industries.

In short, the FCC seems unable to see ISPs as ISPs. It still sees them as siloed cable, wireline, and wireless companies and regulates them as though the Internet has not changed everything.

The Internet has long been known for being disruptive. And

that is a good thing. Rare is an industry that the Internet has not changed and for the better. This has long been enabled by the Federal Trade Commission's approach to consumer privacy on the Internet. Grounded in informed consent and backed by enforcement of broken promises, the FTC's approach to privacy, I believe, has allowed companies to innovate and experiment, sometimes successfully, and sometimes to their detriment, with business models and services without the Federal Government deciding before the fact what consumers want.

Despite the Internet's track record as arguably the greatest economic value and job creation engine the world has ever known, the FCC wants to tinker where there isn't a demonstrated problem. Perhaps more insidiously, the FCC has gone so far as to manufacture a problem so that it could "solve" it, remaking ISPs in their desired image.

ISPs are not unique among Internet companies when it comes to access to customer data. This isn't conjecture, it is the conclusion of the report written by privacy expert, Peter Swire, who served in both the Obama and Clinton administrations. The regulations would give consumers a false sense of security about their privacy by only applying to just one part of the Internet that has access to their data. Consumers expect and should have a uniform experience on the

Internet. The FCC's approach would protect your data only as far as your ISP is involved. This could be particularly confusing for consumers when their ISP is also a provider of "edge services" on the Internet. Consumers shouldn't have to be experts on IP interconnection or routing to understand what level of privacy their data will enjoy.

The impacts of these rigid regulations have the potential to disrupt an ecosystem that has flourished for years, and unfortunately, it is consumers who will pay the price. The FCC has proposed a set of regulations that would not only single out ISPs based on, I believe, faulty assumptions, it would affirmatively prevent ISPs from competing. A robust record of comments warns of higher costs, stifled innovation, and fewer service offerings. None of these are risks we should be willing to take or consequences we are willing to put on American consumers. We should be encouraging competition, not slowing it down with burdensome and inconsistent regulations.

I and other leaders on the committee called for the FCC to reconsider its current approach. As commenters in the record suggest, the FCC should engage in thoughtful discussions with industry to develop flexible and consistent rules, mirroring the FTC framework that has proven successful in today's digital

marketplace. This needs to occur before any more taxpayer dollars are wasted on developing and defending complex regulations that will harm consumer welfare.

I am grateful for the expertise we have on today's panel. We will hear from experts in the privacy field, including the former Chairman of the Federal Trade Commission. It is my hope that we can generate a productive dialogue that incorporates what has been successful in the past, the lessons we can learn from the flawed proposed rules, my opinion, and most importantly, what best serves American consumers. The Internet has helped to shape our economy in ways we could have never imagined, so we must work together to preserve the competition and innovation the Internet embodies. Thanks to our witnesses for being here and I look forward to hearing your testimony.

I yield the balance of my time to the vice chair of committee, Mr. Latta.

Mr. Latta. I thought it was a promotion, maybe. Not now. But thank you very much, Mr. Chairman. Thanks to our witnesses for being with us today. I really appreciate you holding today's hearing. And once again, we have seen damaging implications arising from the FCC's decision to reclassify broadband Internet access service providers as common carriers.

The Open Internet Order removes ISPs from the jurisdiction

from the Federal Trade Commission and divided oversight from the privacy practices of the Internet ecosystem between the FTC and the FCC. As a result, the FCC proposes customer privacy regulations exclusively to the ISPs. It is evident that consumer private information should be protected. However, the FCC's approach is not the answer. The FCC's proposal would fragment the current and successful privacy framework established by the FTC, unfairly target ISPs, and confuse consumers with unnecessary notifications and disruptions.

I believe today's hearings will bring attention to this matter and encourage the FCC to offer a privacy framework more consistent with the FTC approach. It is vital that consumers are granted strong protections and companies are treated equally in order to foster competition and innovation.

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

Mr. Walden. I thank the gentleman and I would ask unanimous consent to put some letters into the record, some documents, the Upton-Walden-Burgess letter to the FCC regarding privacy, the telecom industry letters to myself and to the ranking member. We have a letter from the Advertising Retail Association to both myself and the ranking member; CCA's letter to myself and Ms. Eshoo, and I believe Mr. Olson plans to submit his bipartisan letter to the FCC. Without objection, we will put those in the

record. And with that, I now turn to my friend from California, the ranking member of the subcommittee, Ms. Eshoo, for her opening comments. Good morning.

Ms. Eshoo. Thank you, Mr. Chairman. Good morning to you and to all of the members and to the witnesses. Thank you for holding this hearing. It is an important one.

One of the most important responsibilities the subcommittee has is to protect consumers and it is why we always examine the issues, or we should, through this lens because it is a core responsibility of the subcommittee.

Today, we are examining the issue of privacy and a proposal by the FCC to give consumers more control over how the data collected on their online activities is used. Now this is an issue that matters enormously to the American people. A Pew research study from 2013 found that 68 percent of Internet users believing existing laws are not good enough or not strong enough in protecting online privacy. The same study found that 69 percent of users think it is somewhat or very important to have control over who knows what websites they browse. Seventy percent think it is somewhat or very important to have control over who knows their location when they use the Internet.

The FCC's proposal focuses on ISPs, the Internet service providers, and the data they are able to collect on their

subscribers. ISPs know what websites their subscribers visit and where a user is located when they connect to the Internet. ISPs have access to this even when user data is encrypted. This information is personal to many consumers as the numbers as I just stated that were collected by Pew.

The FCC is proposing to give them control over how it is used. The proposal emphasizes three main points: choice, transparency, and security. These are fundamental privacy principles. Consumers should have control over how their personal data is used when it is shared with others and knowledge about what data is being collected about them. They should also be confident that their data is being protected.

Critics of the FCC's approach argue that it is unfair to apply rules only to ISPs. They argue that edge providers should also be subject to the same rules. Consumer privacy should be protected, I believe, across the Internet. But the FCC lacks the authority to regulate edge providers. Critics also say that consumers will be confused by rules that only apply to ISPs.

Consider the Pew research that asks consumers how confident they were that they understood what is being done with their data. Only 50 percent answered that they were. Consumer confusion is essentially the status quo. The FCC is trying to change that, using the authority that it has and not going beyond that. There

would be huge objections here if that were the case.

Some will point to the Federal Trade Commission and argue that it is the position to protect consumer privacy. They have a different responsibility. In my view, theirs was really essentially after the fact, after something takes place. The reality is that the FTC really lacks to authority to take action against ISPs and while the FTC might agree that this isn't an ideal outcome, it does not argue that the FCC shouldn't act. Instead, it offers constructive comments and has repeatedly called on Congress to take steps to protect consumer privacy.

The irony is that Republicans on the committee are actively trying to gut the FTC's authority under the guise of so-called process reform. I think we have seen the same thing in the subcommittee with the FCC. Instead, we really should be working on meaningful, bipartisan reforms that will enhance the ability of these agencies to protect consumers. Instead, I think some sand is being thrown in the gears of both the FCC and the FTC.

On this side of the aisle, we are ready to work on legislation that would give both agencies the tools they need to protect the public. So I really look forward to today's discussion not only from both sides of the aisle, but obviously from the experts we have at the table.

And Mr. Chairman, I don't know whether you have heard this

or not, but the Court has come out with a decision today on net neutrality but because it is a very long, I am going to reserve my comments for later. But the Court has spoken, so with that, I will yield back the time I don't have.

Mr. Walden. The gentlelady yields back the negative time, 18 seconds.

We will now go to the gentlelady from Tennessee, Ms. Blackburn, the vice chair of the full committee for opening comments.

Ms. Blackburn. Thank you, Mr. Chairman. I want to thank you all for being here with us to continue to look at this issue on privacy and the proposed privacy rules. I think it is no secret that having the FCC look at privacy rules is something has caused some problems and heartburn and concern for those of us on this side of the dais. We know the FTC has traditionally held this authority and we respect the work that they have done there.

I think it does warn of exactly what we have talked about through the entire net neutrality debate which is government overreach and getting outside of their set wheelhouse, if you will, and their authority that they are given. They are so into mission creep. So as we look at what has come forth, yes, it does cause us some concern.

Ms. Eshoo mentioned the edge providers and we need to know

that service providers are the ones that are getting all of the attention right now, really a disproportionate share. When you contrast that with the edge providers and the edge providers are the ones who really collect and hold more data and that is largely unregulated and primarily it is being ignored.

So we are concerned that what the FCC is seeking to do is going to end up doing less to protect consumer data, that it would be another of these false hopes that something is being done when indeed the opposite is happening, that it is going to lead to industry confusion within the Internet ecosystem and that it confirms the fears that Title II reclassification was more of a power grab than it was something that would be constructive to the health of the Internet and that ecosystem as referenced by our chairman in his opening remarks.

And at this time, I am yielding time to I think Mr. Shimkus.

Mr. Shimkus. No.

Ms. Blackburn. Not to Mr. Shimkus. Who was seeking time? No one. I am yielding back, Mr. Chairman.

Mr. Walden. The gentlelady yields back the balance of her time. Before I go to the ranking member of the committee, I am going to yield such time as he may consume to the gentleman from Ohio for a point of personal privilege.

Mr. Johnson. Thank you, Mr. Chairman. I appreciate the

committee's indulgence this morning. I would like to introduce some of my family members that are here with me this morning. I have my mother, my aunt, and my two first cousins, all of whom played a very substantial, influential role in my upbringing and my beliefs and my character where I am today. So I would just like to welcome them, and I yield back, Mr. Chairman.

Mr. Walden. In fact, mom, if you want to share a few comments about the character --

Mr. Johnson. Reclaiming my time, Mr. Chairman.

Mr. Walden. We are glad you are all here. Bill does a great job on the committee and in the Congress.

Now I will recognize the ranking member from New Jersey, Mr. Pallone, for opening comments.

Mr. Pallone. Thank you, Mr. Chairman, and our Ranking Member Eshoo and our three witnesses for being here today.

We are just learning, I was upstairs so you probably already mentioned it, we are just learning that the D.C. Circuit Court of Appeals has upheld the FCC's Open Internet Rules, and I have always been a strong supporter of net neutrality and the FCC's net neutrality rules. While I have not had time to review the court's decision yet, but it seems that it was a big win for consumers and it puts the FCC's privacy proposals on firm legal ground.

For more than a decade, an overwhelming majority of Americans have agreed that privacy is fundamentally important on the Internet. And according to a recent study by the National Telecommunications and Information Administration, 84 percent of Americans are worried about their privacy and security online. Half of the households surveyed are so worried about their privacy that they limit their economic and civic activities when they go online. Another survey, this one from the Pew Research Center earlier this year, found that nearly three quarters of Internet users say it is very important to them that they have control over who has access to their information. And it is important that we take these opinions and concerns into account as we move forward with this hearing today.

It is also important that we listen to the American people about the best ways to ensure that they have more control over their information.

The FCC has clearly been listening and proposed new privacy rules for broadband providers. While many questions about the FCC's proposals are still unanswered, I support the agency's desire to do more to protect consumers. Unfortunately, critics of the FCC came out quickly in opposition to the proposal before they even knew the details. They say that the FCC's proposed privacy rules are fatally flawed because they only reach broadband

providers, not websites or social media.

I agree that protecting consumers across the Internet ecosystem is important as well. But I cannot agree with those that claim that consumers should not get privacy protections anywhere because they cannot get them everywhere. In the face of uncertainty created by a company's privacy policies, nearly 70 percent of Internet users would prefer the government do more to protect their personal information. Consumers want more protection clearly, not less protection. And this is where Congress has work to do.

In order to address the legitimate concerns consumers have about their privacy online, we should give the Federal Trade Commission authority to adopt its own rules over websites. That would allow the FTC to craft privacy rules for websites as well. This sounds like a common sense approach but just last week, the Commerce, Manufacturing, and Trade Subcommittee marked up a bill that would make the problem worse. The bill I am talking about would effectively gut the FTC.

And I think it is kind of ironic that my colleagues would praise the FTC and its expertise in their privacy letter to Chairman Wheeler, while at the same time advancing bills through the Committee that seek to cut the FTC's legs out from under it. And giving the FTC authority to adopt new rules would help ensure

our privacy is safe, no matter where we go on the Internet or how we connect because I believe that when consumers are safe, we are all better off.

I don't know if anybody else wanted my time, you do? I will yield the remaining time to Mr. McNerney.

Mr. McNerney. I thank the ranking member. Data security is critical to consumers. Over the past few years, we have seen many examples of private information leaking into the open, whether it is the OPM leaks or the data breach at Target.

In an age of information with consumers engaging commerce online, they trust those businesses to keep their information safe. That trust, in many ways, is the foundation of our economy. Consumers deserve to know that when they hand over critical information such as their Social Security Numbers or their billing addresses, that that data will be kept safe.

The FCC has come up with some strong proposals that help address data security in at least one sector of the economy. In its Notice of Proposed Rule Making, the Commission also asks a number of key questions. The Commission seeks to comment on the important question of how to ensure that consumers' data continues to be protected as the technology advances. The Commission further asks under what circumstances should trigger the issuance of notifications to consumers or law enforcement agencies once

data breaches occur.

I would like to commend the FCC in taking these first steps toward better securing the data of consumers and I hope that the FCC will move forward in a thoughtful fashion. Consumers ought to be the central focus of this debate and we must do better in protecting their online information.

I yield back to the ranking member.

Mr. Walden. And he yields back the balance of his name. So we will now proceed to our excellent panel of witnesses. And we have the Honorable Jon Leibowitz, co-chair 21st Century Privacy Coalition and former chairman of the Federal Trade Commission; Paul, Ohm, professor at Georgetown University Law Center and faculty director, Georgetown Center on Privacy and Technology; and Doug Brake, telecommunications policy analyst for the Information, Technology, and Innovation Foundation. A terrific panel of witnesses and I think the subcommittee will get break benefit from their counsel and their opinions.

And we will start with the Honorable Jon Leibowitz. Good morning. Be sure to pull that mic close, push the button and you are on. Thank you for being here.

STATEMENTS OF THE HONORABLE JON LEIBOWITZ, CO-CHAIR, 21ST CENTURY PRIVACY COALITION; PAUL OHM, PROFESSOR, CENTER ON PRIVACY AND TECHNOLOGY, GEORGETOWN UNIVERSITY LAW CENTER; AND DOUG BRAKE, TELECOMMUNICATIONS POLICY ANALYST, INFORMATION AND INNOVATION FOUNDATION

STATEMENT OF THE HONORABLE JON LEIBOWITZ

Mr. Leibowitz. Thank you, Chairman Walden, Ranking Member Eshoo, Ms. Blackburn, and Mr. Welch of the Privacy Working Group of this committee, other distinguished members of the subcommittee. I appreciate your inviting me here to testify today. And I am here on behalf of the 21st Century Privacy Coalition which I chair with former Representative Mary Bono. And I am delighted to be here with Professor Ohm, who was a critical part of our FTC team when we drafted the update of the Children's Online Privacy Protection Act, as well as to be here with Mr. Brake.

Our coalition is comprised of the nation's leading communications companies, which have a strong interest in bolstering consumers' trust in online services. We believe the best way to ensure protection of consumer privacy is through a comprehensive and technology-neutral framework based on the type of data being collected and how it is used, rather than on the

type of entity collecting the data. And that is exactly the approach that the FTC has taken in its decades of robust privacy enforcement. Decades.

The FTC has held hundreds of companies, large and small, accountable for breaking their privacy commitments to consumers in a way that causes consumers harm. And by taking an enforcement-based approach, rather than setting out prescriptive rules, the FTC has powerfully protected consumer privacy while permitting the type of high-tech innovation that has yielded huge benefits to all Americans.

Indeed, the FTC approach has been so successful that in 2012, the White House called for the FTC to be solely responsible for protecting the privacy of every American across every industry and that includes ISPs. Last year, as we know, the FTC's sister agency, the FCC, reclassified Internet service providers as common carriers as part of the Open Internet Order. And that decision removed ISPs from the FTC's jurisdiction, thus ending the strong safeguards consistent across industries that the FTC provided to consumers of broadband services.

Having assumed sole jurisdiction to protect privacy among ISPs, the FCC is currently engaged in a rulemaking. Now our coalition was initially encouraged by Chairman Wheeler's stated aim to craft the proposed broadband privacy rules in a manner and

I quote "consistent with the FTC's thoughtful, rational approach," and with the core principles of the FTC's 2012 Privacy Report in mind. But the FCC's proposed rules, as currently drafted, fail to achieve its own goals or to protect consumer privacy.

Instead, the proposed rules impose a restrictive set of requirements on broadband providers that don't apply to other services that collect as much or more consumer online data. These ISP-specific rules do not provide clear benefits to consumers. They would disrupt broadband providers' ability to compete with other online entities. And at the FTC at least, we very much support -- or they very much support that type of competition. They could create consumer confusion. So the goals may be laudable. I have no doubt they are. But the draft rule betrays a fundamental lack of understanding regarding how the Internet ecosystem works. Most troubling, the FCC's proposed rules may well discourage the very broadband investment that the FCC is statutorily obligated to promote, thereby harming the very consumers it is supposed to benefit.

Let me highlight four salient flaws in the FCC's proposal. First, it is not technology neutral. It would impose prescriptive rules on only a subset of the Internet ecosystem and that would lull consumers into a false sense of believing that

they are making a choice that would apply across the Internet ecosystem.

Second, the FCC's proposal would impose opt-in consent requirements for non-sensitive data and basic everyday business practices like marketing to a company's own customers, first party marketing. That makes no sense at all.

Third, the NPRM as drafted would exempt only aggravated data from its requirements and would miss the opportunity to create consumer benefits from de-identified data, not identified data, de-identified data.

And fourth, the proposal would impose an unrealistic time line for breach notification and mandate massive over-notification for data that is not sensitive. And that would cause consumers to ignore even important messages from their ISPs.

And don't take my word for it. Ask my former agency, the FTC. Though it is unanimous comment and the unanimous comment is important to the FCC, it is framed diplomatically. There are more than 25 separate instances where it raises concerns about the FCC's approach, 25, more than 25. There is no need for the FCC to embark on this dangerous path.

And by the way, after today's D.C. Circuit decision on the Open Internet Order, getting privacy right is even more important. I also want to point out that the FCC rules threaten to undermine

the United States' position in international negotiations on cross border data flows, including the U.S.-E.U. Privacy Shield.

But with that said, I do want to make one point. Final rules are often more balanced than proposed ones and we can see a lot of improvement when it goes from an NPRM to a final rule. But the FCC's current proposal is a solution in search of a problem. It would create inconsistent standards across the Internet and add to consumer confusion. It could undermine innovation as well. For all these reasons, the 21st Century Privacy Coalition's view is that the FCC should adopt the FTC's time-tested and proven approach and it can do that by rule. Thank you. Happy to answer questions.

[The prepared statement of Jon Leibowitz follows:]

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

Mr. Walden. I thank the gentleman for his testimony. We will now move to Mr. Ohm from the Georgetown University Law Center and Faculty Director, Georgetown Center on Privacy and Technology. Mr. Ohm, we look forward to your testimony. Thanks for being here today.

STATEMENT OF PAUL OHM

Mr. Ohm. My pleasure. Thank you very much, Chairman Walden, Ranking Member Eshoo, and other members of the subcommittee. My name is Paul Ohm and I am a professor at the Georgetown University Law Center and thank you very much for inviting me to discuss this very, very important issue about the Federal Communications -- I guess now D.C. Circuit blessed -- moved to protect the privacy of consumers of broadband Internet access service. I hope you don't mind if I refer to this BIAS entity as ISPs or Internet service providers instead of using the Washingtonese that has been thrown around.

My bottom line is fairly simple to state. The FCC's rule is number one, unambiguously authorized by law. And number two, it is a wise rule. Let me take those in turn.

Nobody in this debate disputes that Section 22 of the Telecommunications Act of 1996 instructs the FCC to promulgate rules to protect the privacy of information gathered by telecommunications providers. The underlying circumstances have changed a bit. And when I say a bit, I urge you to remember that this was 1996. This wasn't the Dark Ages when this statute was enacted.

These changes to the ecosystem of the Internet actually

raise, not lower, the importance of having a statute like Section 222. But at any rate, due to the clarity of a statutory text, it is my belief that the burden should be on those who would rewrite the statute, much more on those who would ask the FCC to ignore the plain terms of the statute, rather than on the agency attempting to apply the statute.

Number two then, let me tell you why I think the law is a wise one. Congress' act reflects the well-reasoned conclusion that telecommunications providers owe a heightened level of privacy to their customers. I give four reasons why this is so in my written statement: history, choice, visibility, and sensitivity. But let me focus on the latter two and I will refer you to my written statement for the arguments about history and choice.

Number one, visibility. Your Internet subscriber provider sits at a privileged place in the network. They are the bottleneck between you and the Internet. This gives them the ability to see part of every single communication that leaves your computer and returns to your computer. For unencrypted websites, this gives them complete and comprehensive visibility. They can see everything including the content of their communications. It is a regrettable fact in 2016 that so many websites are still unencrypted including many, many, many of the most popular ones.

But even for encrypted websites, although the view of NISP is partially obscured, there is plenty that can see. They can basically compile a list of the domain name of every website that you visit, when you visit it, how often you return to it, and how much data you transfer with it. And they can even track how often you linger on an open page in some cases.

This all leads to the second factor that leads me to conclude that Congress was well justified in 1996 in enacting Section 222, sensitivity. I will be honest. Law professors have kind of embarrassed themselves in a battle for metaphor to try to get people to understand what we are talking about when we are talking about something that has never happened in human history before, that there are entities that are sitting over your shoulder watching you read compiling a complete list over time of every single thing that you do on the web. Some have called this a digital dossier, others have said that this invades an individual's right to intellectual privacy, not intellectual property. And I have called this the database of ruin. Very subtle, I know.

But all of these speak to the problem of allowing people to develop a complete accounting of what we read, who we speak to, what we say, who we associate with and with the rise of the mobile broadband, where we go on a minute-by-minute basis.

Okay, in my last minute, I would like to say that these four factors, history, choice, visibility, and sensitivity, led Congress to do in 1996 what it has done several times before, enact a sectoral privacy law just like they did with doctors and HIPAA, just like they did with schools and FERPA, just like they did with credit agencies in the Fair Credit Reporting Act. Congress, you, did this as well, for telecommunications providers.

Two closing thoughts. Number one, when Congress enacts a sectoral privacy law as they have in here to face a heightened risk of privacy, it makes great sense for Congress to draw bright lines. Many of the people, including Mr. Leibowitz, have said that the FCC should instead ask Internet service providers to look at every piece of content and decide whether it is sensitive or non-sensitive and then decide there whether or not it is subjected to heightened privacy rules or not.

So let us imagine that this were the base for HIPAA, that your doctor would have a conversation with you, you would talk about your diagnoses, and the doctor would constantly be calculating whether what you just told him was sensitive or non-sensitive. And if they concluded that it was non-sensitive, they would be able to sell that information to a pharmaceutical company. That is not the way we have written HIPAA. That is not the way we have written the Wiretap Act. Nor is it the way that

we have written Section 222 last.

If there is one thing that really, really gives me a lot of joy about the vigorous debate that is having around here, it is that there is so much commentary lavishing praise on the Federal Trade Commission for the amazing work it does protecting consumers' privacy and Chairman Leibowitz says there is a lot of credit for that. I am so grateful to him that he hired me to be a senior policy advisor to advise the Commission on privacy issues. I think it would be folly though to use the FTC's successes as an excuse to dismantle one of the only meaningful privacy laws we have for online privacy.

Just like we shouldn't use the FTC successes to take jurisdiction away from health and human services of our doctors and healthcare or the Department of Education over education records, nor should we do it with the FCC and telecommunications. It is either a marvel of institutional design or maybe dumb luck that the FCC and the FTC have a lot of complementary skills, abilities, staff, expertise. There is no contradiction here. The FTC cannot go it alone. I think it is wonderful that we have two privacy cops on the beat online. Thank you. I look forward to your questions.

[The prepared statement of Paul Ohm follows:]

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

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

Mr. Walden. Thank you, Mr. Ohm. We appreciate your comments. We will now go to Doug Brake who is a telecommunications policy analyst for the Information, Technology, and Innovation Foundation. Mr. Brake, it is up to you now. Thank you for being here.

STATEMENT OF DOUG BRAKE

Mr. Brake. Chairman Walden, Ranking Member Eshoo, members of the subcommittee, thank you for inviting me to share the views of the Information, Technology, and Innovation Foundation on the ongoing proceedings of the Federal Communications Commission to regulate broadband privacy.

ITIF is a nonpartisan think tank whose mission is to formulate and promote public policies to advance technological innovation and productivity growth. The FCC's proposed privacy regime does a remarkably poor job of balancing those goals, innovation and productivity, with other policy interests. For this ITIF has opposed the FCC's privacy undertaking in its entirety. Congress should direct the FCC towards a model that better balances privacy, innovation, and overall consumer welfare. Here, the Federal Trade Commission should be the guiding path.

A consistent application of the FTC's privacy guidelines across different platforms in concert with existing industry practices and commitments will see the continued dynamic competition and innovation that has driven the success of the Internet to date. A uniform approach is especially warranted as broadband providers' access to data is neither comprehensive nor

unique. My primary concern is how the FCC's proposal would unnecessarily stifle innovation. Boiled down, the proposal is a three-tier consent scheme that require opt-in consent required for uses of data that are not communications related. The entire regulatory scheme is explicitly structured around what business practices broadband providers participate in and not consumers' expectation of privacy or risk of harm.

The overly broad opt-in requirements sets the wrong default choice that will reduce consumer welfare, productivity, and innovation. Most people are happy to make tradeoffs around privacy and other values such as convenience, price, or functionality, but requiring the extra step of opting in would sharply reduce participation rates in data-dependent offerings.

Privacy-sensitive consumers are well motivated to opt-out and can do so under existing practices, but the FCC proposal would effectively shut off new business models that would benefit the majority of broadband consumers. The FTC's approach, on the other hand, is a clear alternative that offers a better balance of policy objectives. The Federal Trade Commission enforces unfair and deceptive trade practices as informed by high level, technology neutral guidelines, industry best practices and company commitments. The FTC framework has successfully applied to an incredibly diverse set of actors in the Internet

ecosystem by allowing flexibility for firms to develop the specifics of privacy and security practices and stepping in where problems develop. The FTC does not have to predict technological advancements or changes in business practices. Firms can then internalize or outsource different functions in fast-paced industries with a focus on efficiency, rather than compliance. And even application of privacy oversight will provide a better environment for dynamic competition across platforms, allowing carriers' continued entry into areas like targeted advertising and would avoid discouraging new entrants and exploring provision of broadband.

So the FCC proposal is a bad approach to promote innovation with nothing to gain over the well-established FTC framework, but furthermore, provider access to data simply does not justify heightened sector-specific regulation. To justify sector-specific rules, one would expect an unusually high risk of harm from broadband providers. As a factual matter, that heightened risk does not exist. Broadband providers do not have anything near comprehensive nor unique access to customer data. The past 2 years have seen a dramatic and continuing trend towards pervasive encryption which prevents broadband providers from accessing the content or detailed web addresses of consumers browsing.

The uptick in encryption is a profound structural limitation in the amount and kind of information that is available to broadband providers, an unpredicted shift that should chasten us from broad, prescriptive regulations. Other trends, such as a growing popularity of proxy services, availability of virtual private networks, and consumers relying on multiple networks throughout the day further weaken the claim for sector-specific regulation. Heightened rules would also set a bad precedent, giving advocates the fulcrum to ratchet up European style privacy regulations across the rest of the Internet ecosystem in a way that could do significant damage to what is a bright spot in the U.S. economy.

To sum up, there certainly is a legitimate government interest in ensuring customers have a transparent notice and choice over how their information is used. But the FTC framework offers a far better balance of competition, innovation, and consumer protection. Given the advent of tools to protect privacy and opt-out options already available, there is no actual harm the FCC needs to correct and no justification for special rules peculiar to the FCC's jurisdiction.

Large changes in privacy policy like those proposed should be set through an open and democratic legislative process, not creative, statutory reinterpretation by an independent agency.

Congress should direct the FCC to either leave privacy with the FTC or adopt regulations in line with the FTC framework.

Thank you again for this opportunity to appear before you today and I look forward to your questions.

[The prepared statement of Doug Brake follows:]

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

Mr. Walden. Thank you, Mr. Brake. We appreciate your testimony and that of your colleagues at the witness table. I will start off with questions.

You know, we are hearing, obviously, a lot about privacy. It matters to consumers and as the Internet develops and you have got edge providers, you have got ISPs, there is a question about control of privacy and whether it translate all across the way we hear it. In fact is the debate over set-top box. If you change out everything, there are some entities that are covered by some statutes, and others that may not be covered by others. we hear it in some of the search engine debate and Facebook debate and the political side. Is somebody manipulating the algorithms and what you are looking at and what you get to see in the off ramps versus the sort of common carrier piece of this.

I guess my question, I will start with Mr. Brake, how does the information collected by ISPs differ from information collected by some of these other platforms such as Facebook or Google or any of the large platforms that are used widely by consumers today? And would you argue that one of these collects more or less or better quality or more verifiable? Is there similar standards for consumers regardless of where they go or do they vary? Which is strongest?

Mr. Brake. Thank you, Mr. Chairman, for the question.

It is a good question. There has been a lot of discussion about this issue in the record at the FCC and previous interest. I say in my statement that the ISP's collection of information is not unique, but in truth it is unique in the sense that every actor in this ecosystem has a unique view on customer data that everyone is unique, no one is unique. And so everyone has a different perspective, a different access to different kinds of valuable information. And I think that should leave us to have the goal of a single set of overarching principles instead of going case by case and trying to develop specific sector rules for each individual actor. I think that is -- I mean that is essentially nightmare fuel for me.

Mr. Walden. So your point is -- your recommendation, I won't put words in your mouth but is pick an agency, pick a set of rules, apply to everybody?

Mr. Brake. Right. Have a set of high-level, technology neutral principles that can apply both to just sort of ordinary data collection that we are all familiar with or to new -- potentially very invasion practices that haven't even been thought of yet.

Mr. Walden. All right.

Mr. Brake. So we want an overarching framework that can oversee all of this.

Mr. Walden. Mr. Leibowitz, what is your thought on that? Turn on your mic, please. We can't collect data if your mic is not on.

Mr. Leibowitz. You can't collect that way. Others can, but you will not. I understand and the hearing record won't. Look, I would just point out, look at my phone. Right? I am sending a text or I am sending an email and who is collecting that data? Well, it might be the ISP. It might be the browser. It might be the operating system. It might be the manufacturer. There are a number of different entities that can collect that data. And so why would you view one differently than the other? Wouldn't you want to have similar privacy protections for consumers? And the FTC approach, which is an approach that recognizes that sensitive data should be protected, is one that you could incorporate into an FCC rulemaking if the agency, if the FCC wanted to.

I will just make one more point which is, and Professor Ohm correctly noted, that is not enough encryption now. But there is no doubt that encryption is growing. And Peter Swire, who was the privacy czar in the Bill Clinton administration, issued a paper earlier this, actually, late 2015 in which he pointed out that by the end of this decade, 70 percent of all, 70 percent of all information will be encrypted. And 42, I believe, of the top

50 websites already encrypt. So we are seeing a trend towards encryption. It is leveling off the kind of information that different entities can collect. And that is why you should have a similar --

Mr. Walden. Now Mr. Ohm, Professor Ohm, made the case that it is good to have two cops on the beat. Again, I won't put words in your mouth, but what I heard was better to have two agencies doing this, one sort of before the fact, one after the fact, based on their current regimes. Is that accurate, Mr. Ohm?

Mr. Ohm. Oh, absolutely. I think there is the kind of specter of lots of competition, turf warfare. When instead if you look at the Memorandum of Understanding that was put together by the staffs of these two agencies, when you look at the fact that one of them has ex ante rulemaking which we are watching unfold right now, while the other has ex post enforcement, when you look at the fact that the FTC has -- sorry, the FCC, has decades, decades and decades of building up staff and expertise on related questions about incentivizing broadband build out. All of these things, there is no conflict at all. There is no inherent conflict.

Mr. Walden. But do you think that these other entities should also be covered? Should everybody from a Google Facebook to Comcast, whomever, should they all have the same privacy --

Mr. Ohm. One way to read the Swire report is privacy is in shambles in lots of different places across our digital ecosystem. Right? I think that is a conclusion that flows quite directly from the later sections of that paper. So the question is what do you do with that conclusion if you think Professor Swire is right? One is we throw up our hands and say we are not going to have privacy anymore. The other is well, we have one statute that is aggressive and works really well, let us go ahead and enforce that one and consider other statutes, right?

I mean I can be persuaded that there are entities that threaten privacy similarly to what ISPs do. I could absolutely be persuaded of that, but that would require an additional act.

Mr. Walden. That is kind of what we do here.

Mr. Ohm. That is right. That is right.

Mr. Walden. Mr. Leibowitz, real quick.

Mr. Leibowitz. If I can just slightly disagree the professor, who is one of the most creative lawyers I have ever worked with. It is worth pointing out that there aren't two cops on the beat now with respect to ISPs because in fact the FCC in its Open Internet Order took jurisdiction away --

Mr. Walden. From the FTC.

Mr. Leibowitz. From the FTC.

Mr. Walden. Right.

Mr. Leibowitz. There used to be two cops on the beat and it was the FTC that did almost all of the privacy enforcement.

Mr. Walden. Right.

Mr. Leibowitz. And the second thing is I am not quite so sure how clear it is that in 1996 Congress gave this broad grant of authority to the FCC because if you look at Section 222, it is about as clear as mud. And the other thing is if it was so obvious that Section 222 created a privacy protection regime for ISPs, you would think that at least one of the several Democratic chairmen of the FCC and there were some very good ones after the '96 Act including Reed Hunt, Julius Genachowski, and Bill Kennard, would have discovered this earlier. No one discovered it until very, very recently. I question that discovery.

Mr. Walden. Right. I have got to cut it off. I have gone way over. I thank the indulgence of the committee. We go to Ms. Eshoo for a round of questions.

Ms. Eshoo. Will you grant me the same time that you took? How is that?

Mr. Walden. I would be happy to do that.

Ms. Eshoo. Thank you, Mr. Chairman. Thank you to the witnesses, all excellent. I really want to salute you and Mr. Brake, happy anniversary.

Mr. Brake. Thank you very much.

Ms. Eshoo. Ten years of the founding of ITIF and excellent work. I think it is worth just very quickly stating the following. The FTC and the FCC have different sources of legal authority and they have different tools that they can use to protect consumers. The FTC generally lacks the same rulemaking authority under the Administrative Procedures Act that the FCC has. Instead, the FTC relies on Section 5 of the FTC Act which prohibits unfair deceptive acts and practices.

Now under Section 5, the FTC is limited to bringing enforcement actions after the fact. It often sets guidelines. It encourages industry best practices. And then if they fail to follow, it can result in an enforcement action.

On the other hand, the FCC has authority to set clear rules of the road that companies must follow. Now the FTC staff which is a little different than what you said, Mr. Leibowitz, in your description, at least the way I took it, the FTC staff follow comments in this proceeding that are generally supportive of what the FCC is trying to do. The FTC did describe the fact that ISPs could be subject to different rules, the rest of the Internet industry is not optimal, but nonetheless, they offered constructive comments and pointed to its repeated calls for Congress to take steps.

Now the FCC, obviously, operates under Section 222 of the

'96 Telecom Act. I was there. I helped write it, Mr. Leibowitz. We knew what we were doing and we are proud of it.

Mr. Leibowitz. I was there as well.

Ms. Eshoo. I don't think your description "clear as mud" is fair. I think that is meant to muddle the conversation, but that is my view.

Now Professor Ohm, your testimony discussed the difference in data collection between edge providers like Google and ISPs. Can you elaborate, I don't have that much time left, more on the different relationships that consumers have with ISPs as compared with edge providers?

Mr. Ohm. Certainly, absolutely, and I will try not to take too much of your time. It boils down to choice. So you choose your search engine. You choose your social network. You choose your email provider. And if you are unhappy with their privacy handling policies, then you can exit. You can choose another, right?

And I guess on one level you do choose your ISP, although in wide swaths of America, that is not true. In rural areas, there is only 13 percent of people have more than one choice for broadband ISP. And so if you are unhappy with what your broadband provider is doing, you cannot exit. Not only that, but when you leave your email provider or you leave your social networking site

and you go to another website, you escape the visibility of that prior edge provider.

Now don't get me wrong, edge providers are trying like mad to increase the visibility they have on the web and in some instances they are being quite successful. They are nearing ISP levels of visibility which is why I said to the chairman a moment ago, we might want to talk about whether we need regulations in other areas as well. But choices define an answer to the question you have asked.

Ms. Eshoo. Can you define or describe the kind of profile an ISP could create of a subscriber using only data that is encrypted?

Mr. Ohm. Sure. So even with the prevalent form of encryption which is HTTPS, they are still privy or ISP is still privy to the domain name, the domain name of the website you visited. I will fully concede that with this form of encryption, they don't know whether you are reading an article about Orlando or an article about the D.C. Circuit opinion, but they do know that you are at The New York Times website or they do know that you are at a blog that is a highly-specific blog.

And I think that it is important at this moment in time to compare what can be known through a domain name, versus the telephone numbers that we were focused more on in 1996. Sometimes

a telephone number tells you a lot about what you likely said during that call. Quite often that is true for domain names.

So picture, if you will now, these domain names which are quite revealing. Imagine it almost visibly trailing after you in an indelible trail that is now being stored at a corporation 1,000 miles distant that you never met before. So this is what is being kept on a minute-by-minute, second-by-second basis. It is never being disposed of and up until now ISPs have been pretty restrained in not using that, for example, to sell advertising to you.

Ms. Eshoo. You know, there is an irony here to me. And that is that the American people have always been I think justifiably suspicious of big government, what it can do, what it holds, how it can be used against people. And yet, in this debate, we are saying or some are saying it is all right. It is okay. We can be tracked. We can be traced. We can be followed. It is sitting on each shoulder. Somehow, for some, that seems acceptable.

So I don't think that. I just don't. I think that sensibility of the American people is on target. And at any rate, I am way over my time. Thank you to the three of you. I appreciate it.

Mr. Leibowitz. May I just add a comment? And I agree with you --

Ms. Eshoo. I think my time is up.

Mr. Walden. I will give you an extra minute.

Mr. Latta. And I agree with you.

Ms. Eshoo. But I don't want to hear --

Mr. Leibowitz. Privacy protection is critically important.

Ms. Eshoo. Yes, quickly.

Mr. Leibowitz. But I do think that you have to keep in mind, and let us assume Section 222 is upheld, constitutionally. We will stipulate to that for purposes of this discussion, even though no less an authority than Larry Tribe has raised constitutional concerns about it.

Ms. Eshoo. Oh, come on. Get to your point.

Mr. Leibowitz. My point is this. If you go back to the --

Ms. Eshoo. You don't like it. I get it.

Mr. Leibowitz. If you go back to the constructive criticism in the FTC's comment and there are 28 points where it makes suggestions, the biggest suggestion it has is have an opt-in for sensitive data. Have an opt-in for maybe Deep Packet Inspection. Those are things that are in the 2012 privacy report that we worked on. But if you do that --

Ms. Eshoo. I don't know. I have to tell you -- do you know how I would respond to that? If you have children and their pals, ask them.

Mr. Leibowitz. I do.

Ms. Eshoo. How they like what you are suggesting.

Mr. Leibowitz. And I think that my coalition would have far fewer rejections --

Ms. Eshoo. I don't think it flies.

Mr. Leibowitz. -- if the FCC just took the FTC's advice in the comment.

Ms. Eshoo. Thank you.

Mr. Walden. Thank you.

Ms. Eshoo. Thank you, Mr. Chairman.

Mr. Walden. You are welcome. And now we go to the ranking member of the subcommittee -- I keep doing that -- vice chair of the subcommittee, Mr. Latta.

Mr. Latta. Boy, okay. Thank you, Mr. Chairman. And thanks to our panel for being here today. I really appreciate your testimony today.

And Mr. Brake, if I could start with you. In the NPRM, the FCC proposes to treat device identifiers such as IP addresses as personally identifiable information which in turn could not be shared with third parties absent affirmative consent from the owner of the device. Since many Internet devices utilize IP addresses, is there a risk that the rule, if adopted, would dampen innovation and the delivery of the innovation technology type

devices that would substantially benefit consumers?

Mr. Brake. Absolutely. I think this rulemaking has potential to dampen innovation across the board, both in the Internet of things and obviously on the action-size piece. I think the rules governing the treatment of personally identifiable information are incredibly overbroad and will have reverberating impacts throughout the ecosystem. Yes.

Mr. Latta. You know, when you talk about -- we are looking at how much that impact would be. How large would that be on that innovation? You know, because we have had so much testimony on this committee through the years as to what the -- as the chairman started off with this morning, talking about how much innovation it had brought and the amount of money that has been spent. Do you have any kind of a clue what we could see happen if that innovation is dampened and how much that would be?

Mr. Brake. There are all sorts of specific practices that we think are beneficial to overall economy. I think it is worth noting in a lot of the privacy conversations, it is taken as a given that all the uses of data are necessarily scary or a bad thing. But to my mind, targeted advertising a potential business practice that ISPs have been exploring can very much be a good thing, can enhance consumer welfare, giving them less intrusive, more helpful advertisements and overall enhance economic activity

on the Internet.

There are practices such as ISPs exploring, offering free WiFi services based on offering target advertisements that I don't see how those could possibly operate on an opt-in only basis and not conditional on the provision of the service as is proposed by the rules. It seems to me that the rules would outlaw that type of service.

I think there are a number of ways in which the basic infrastructure of telecommunications is shifting towards software, away from hardware and more provision in software. And all of that is going to be largely dependent on availability of data. Much of that is, granted, providing the communication service, but I am worried that these rules could dampen ISPs' ability to either internalize those functions or outsource them to third-party companies without extensive compliance procedures. Those are just a few, a large impact.

Mr. Latta. Thank you. Moving on, Mr. Leibowitz, I would like to ask in the FTC's 2012 privacy report, the agency asserted that the operating systems and browsers may be in a position to track all or virtually all of the consumers' online activity to create highly detailed profiles. Should consumers' privacy protection related to their online activity be different because operating systems and browsers subject to the FTC's jurisdiction,

but because of the FCC's Open Internet Order Internet service providers are subject to the FCC's jurisdiction.

Mr. Leibowitz. I am not sure I caught all of that question, Mr. Latta. Let me try to answer it and you can direct me. So this is our 2012 privacy report and it looked at large platform providers. There is a section in it. And large platform providers included ISPs and it included other big data collectors like Facebook and Google. And what we said was that with respect to large platform providers who collect data, perhaps there should be heightened scrutiny. But what we also said is that it should be consistent across the board.

And the FTC held a workshop after we released this report on large platform providers and at that hearing a number of consumer groups also raised the point, and by the way, this report was criticized by many in business including I believe the ITIF actually for being too pro consumer. I don't mean to mischaracterize it, but I think that is accurate.

And a number of consumer groups actually at the hearing, and I will put those quotes in the record, actually argued that you have to have similar rules across industries for all data collection. They called for technology-neutral standards.

Mr. Latta. Thank you very much, Mr. Chairman. My time has expired and I yield back.

Mr. Walden. The gentleman yields back. The chair recognizes the gentlelady from California, Ms. Matsui, for questions.

Ms. Matsui. Thank you, Mr. Chairman. We just learned this morning that the FCC's legal authority over broadband was upheld in net neutrality case and it was clear that the FCC has oversight and consumer protection authority for broadband.

My questions are about how to best exercise its authority on behalf of consumers. With this decision, it is more important than ever that the FCC get these privacy rules right.

Now consumers need to have confidence in the safety and security of their information. Today, that means more than just logging on to a desktop computer connected to your home broadband provider. The devices that Americans are using for financial transactions or communicating healthcare information are often connected to a wireless network.

Professor Ohm, can you elaborate on the information collection practices that Internet service providers are using today over wired and wireless networks and to what extent are consumers aware of the amount of personal information shared with their ISP?

Mr. Ohm. Yes. I am happy to do so. I should say in the obnoxiously long, nine page CV that I submitted, we haven't

mentioned yet that I have an undergraduate degree in computer science and I worked for 2 years as a systems network programmer and systems administrator. And so although that experience is a little dated, I still keep up with quite a bit of this information.

Ms. Matsui. I am sure you do.

Mr. Ohm. So there is a fundamental technology called NetFlow. NetFlow, you can think of it as the kind of permanent record that you were always warned about in high school, but this isn't a record of how many times you chewed gum in school. This is a permanent record of these individual transactions, right, what website you are visiting, the address you are visiting and that is stored. Now I will be the first to concede that the way that is stored right now, it would require some engineering to extract it and then to start advertising based on it. But I think it is exactly that engineering that the ISPs are hoping to achieve and are worried that the privacy world might prevent them from doing. But that record is there. That record is being created.

Ms. Matsui. Okay. Okay. Now all witnesses, are there different risks that mobile broadband consumers face and how should privacy rules account for this?

Mr. Leibowitz?

Mr. Leibowitz. Look, I think you have asked two really good

questions. I think with respect to mobile broadband, first of all, there is quite a bit of competition. All you have to do is turn on the TV and you will watch the advertisements of mobile broadband providers.

What do we think? We think at the 21st Century Privacy Coalition that there should be -- that if there is going to be an opt in, it shouldn't be for everything. It shouldn't be for commonplace sort of business, commonplace information. It should be for sensitive information. And that is what the FTC called for in its privacy report and that is what it called for in its comment. And if you look closely at that comment and if the FCC looks closely at that comment and I am sure it will, it could dramatically improve its rule because there is a lot of good advice in it.

Ms. Matsui. Okay. Professor Ohm, quickly, yes.

Mr. Ohm. Yes, I so appreciate the question because it gives me the opportunity to talk about one aspect of mobile broadband that has been raised only obliquely which is you often hear this number thrown around in this debate that the average American has 6.1 devices, right? I think the average D.C. telecom lawyer may have 6.1 devices, but for many people in more modest circumstances for many minorities, they have one lifeline to the Internet and that is their mobile phone.

Ms. Matsui. Right.

Mr. Ohm. It is how they find jobs, how they communicate, how they find dates. And so that one thing, right, has become an essential part of this entire debate about the FCC and I don't want to lose sight of those people when we are talking about these privacy rules.

Ms. Matsui. Okay. Mr. Brake.

Mr. Brake. Yes, I agree with Mr. Leibowitz. I think that the number of mobile providers dramatically increases the number of choices that consumers have and beyond that, offering a simple opt-out that is already available to consumers, I don't see that as being a particularly different situation as with fixed providers.

Again, I return to you want to have an overarching framework that can apply to any actors in the ecosystem and you want this for reasons other than the particular information that is collected by any other -- any particular actors.

Ms. Matsui. You had a quick comment?

Mr. Leibowitz. Yes. I just wanted to say one thing and it goes back to a point you made or Mr. Ohm made and Ms. Eshoo made about consumer choice. So there is one area where the FCC particularly gives consumers no choice. You mentioned one device. If I have one device, if I am a family of four and I make

$40,000 a year, and I would like to allow an ISP to collect information, not necessarily disseminate it, but to collect aggregated information or de-identified information and they are offering me a $250 a year discount, as long as they explain that to me, I should be able to make that choice. That is the concept of notice and choice which is embedded in the FTC's approach, embedded in the FTC's recommendation. And the FCC would say you can't make that choice, an ISP isn't allowed to do that.

Now, if the ISP were collecting identified data like a data broker and then selling it, that would be a real problem. And most of us in the room today probably might pay that extra $20 a month. But if someone wants to make that choice themselves, they should be given the opportunity to make that choice.

Ms. Matsui. I am sorry, I have run out of time.

Mr. Walden. The gentlelady's time has expired. The chair now recognizes the vice chair of the full committee, Congresswoman Blackburn from Tennessee for 5 minutes.

Ms. Blackburn. Yes, thank you all. Mr. Leibowitz, I am going to stay with you. I appreciate your perspective always and your spending some time with us.

The rules, the data security rules proposed by the FCC also seem much more stringent and prescriptive than the standard that is there at the FTC and I wanted to know if you could just briefly

give what you think would be a justification for that.

Mr. Leibowitz. For the FCC's rule?

Ms. Blackburn. Yes.

Mr. Leibowitz. Well, look, I think once it made the decision to do Title II net neutrality, then you needed to have a cop on the beat. And so it makes sense for the FCC to do a re-think. But the truth is that the FTC rules could actually incorporate the FCC's approach that is an enforcement-based approach plus the suggestions in the privacy report about where you should have an opt-in which is for sensitive data, vulnerable populations like kids. We worked on the Children's Online Privacy Protection Act. And they could do that and it would be much more balanced.

Now, it still wouldn't be entirely technology neutral, but I think it would go a long way towards making the 21st Century Privacy Coalition members to bringing down sort of the decibel level of their concerns which are legitimate concerns and towards taking a better and more balanced approach that both protects privacy which is critically important, but also allows for innovation.

Ms. Blackburn. Thank you. You know, one of the things is we have looked at what the chairman, Chairman Wheeler, has had to say. I feel like he has almost done an about face, if you will, in the first couple of years when it comes to addressing network

security and data security. Because a couple of years ago and here is a quote that he said and I am quoting him, "The Commission cannot hope to keep up if we adopt a prescriptive regulatory approach." And as you said, that is what they are doing as much for prescriptive. And that he also followed that with a statement that "The FCC should rely on industry and market first to develop business-driven solutions to the security issues." I wish that is

where we were. I wish that is what we saw coming up.

Mr. Brake, coming to you for a minute, I want to go back to your testimony, page four, where you talk about the gatekeeper model when thinking about the broadband providers' relationship to the consumer data. Can you elaborate as to why you think that is the wrong way to think about the relationship and why you think it leads to confusion with the consumers?

Mr. Brake. Absolutely. So Professor Ohm spoke about this earlier, the issue of choice, the fact that consumers only have so many choices when it comes to ISPs. So I think this issue of choice is often misrepresented. Just as a factual matter, consumers often have more than two fixed, and of course, we have four mobile countrywide carriers. And there is a general trend towards more, new entrants in this space. Switching costs are, of course, not unique to broadband and especially in mobile.

Switching costs are going down dramatically. We have carriers offering to pay consumer switching costs.

And also some of the statistics from Professor Ohm, I think, are misrepresented from the FCC's relatively arbitrary definition of broadband at 25 megabits per second. When you change that to 10 megabits per second, the numbers go dramatically up, over I think 78 percent have a choice of two fixed.

And so beyond that, I think the visual metaphor of broadband providers as intermediaries in the middle is misleading and it is far better to think of them as one platform in concert with a number of other large platforms. This is exactly how the FTC recommended that we think about this issue in its 2012 privacy guidelines, mentioned that it was important that we recognize technology-neutral frameworks and that these are one type of platform among many.

And again, I have to return to -- even if this is a particularly large platform, when consumers have the ability to opt-out as is available now or even if the FCC wanted to go with the FTC's guidelines and offer opt-in only for sensitive information, that would be a tremendous improvement over the other rules as proposed.

Ms. Blackburn. Well, I am one of those that appreciates some notice and choice and I prefer being able to opt-in as opposed

to having to opt-out. I think the opt-in is less confusing and brings more clarity because people understand what they are getting into on the front end and appreciate that. Thank you, all and I yield back.

Mr. Shimkus. [presiding] The gentlelady yields back her time. The chair now recognizes the gentleman from California, Mr. McNerney, for 5 minutes.

Mr. McNerney. Well, I thank the chairman. I want to commend the panel. It is a very lively discussion. I appreciate it. It is very informative as well.

Mr. Leibowitz, as chairman of the FTC, you testified before the Senate Commerce Committee that the common carrier exemption to the FTC Act should be lifted. There is a quote here I can give you, but I will pass on that. At the hearing in this committee earlier, this Congress, Ranking Member Pallone asked if you supported lifting the exemption without preempting any other part of the Communications Act. You unequivocally said yes. Do you still hold this position today in your role as chairman of the 21st Century Privacy Coalition? Should the FTC lift --

Mr. Leibowitz. I certainly hold that as my personal position is that the common carrier exemption should be eliminated, absolutely.

Mr. McNerney. So is your personal position -- what about

your position as chairman of the --

Mr. Leibowitz. Of the 21st Century Privacy Coalition, I think a number of the carriers, I haven't gone back and polled them, but I think a number of the carriers would support lifting the common carrier exemption. Now they would prefer and this was the White House position, that the FTC have sole jurisdiction for privacy enforcement.

Mr. McNerney. Thank you. Mr. Brake, in your testimony, you argue the ISPs don't actually have much access to consumers' data because so much of the data is now encrypted, yet ITIF's unlocking encryption report released earlier this March notes that even when information is encrypted, law enforcement can have a lot of that information from analyzing users' metadata. If law enforcement can draw important insights from analyzing metadata, wouldn't an ISP also have the ability to benefit from analyzing users' metadata?

Mr. Brake. That is absolutely true. I mean we are not denying that metadata is still available. The high-level URL, the web address is still available to ISPs.

Mr. McNerney. And a lot of information can be gleaned about users from that metadata.

Mr. Brake. That is correct. And to the extent that that can be used under an appropriate privacy framework such as that

offered by the FTC, we think that is a good thing. We think that that offering ISPs the opportunity to enter into target advertising allows for other innovations. And so we wouldn't deny that there is still available metadata. But I think it is important to look back at how unpredicted and unprecedented the rise of encryption is and how dramatically this changes both the scope and the type of information that is available to ISPs.

It was not that long ago that very respective privacy scholars expected, predicted that ISPs would deploy DPI, Deep Packet Inspection, scale based on trends and Moore's Law, as process and power increases, that would become cheaper and more available. That turned out not --

Mr. McNerney. But the metadata is still a big deal.

Mr. Brake. But what happened was widespread rise of encryption and so I think that this sort of -- the ways in which technology can shift the ground under our feet with regard to these sorts of practices should caution us towards flexible, ex post enforcement guidelines rather than --

Mr. McNerney. The same goes true with the amount of information that is available for metadata, the same argument.

Professor Ohm, would you comment?

Mr. Ohm. This is such an important point and I think it is something to really underscore, right. So in my misspent youth,

along with being a systems administrator, I was also a computer crimes prosecutor at the Justice Department.

Ms. Eshoo. Which job did you not have?

Mr. Ohm. And I will say that there is a richness to metadata that is useful to the FBI. This has come up time and time again. And I commend the ITIF for acknowledging that in the report you reference.

I will also say this is something to consider when you think about the spread of encryption. There is an intrinsic relationship between is data useful for advertising? Is data useful for the FBI? Is data potentially privacy invasive? Right? We have not yet invented the magic wand that allows us to wave it over a database and remove only the privacy violation, but retain the law enforcement utility and the advertising utility. It is a really, really vexing relationship of data.

So if the Swire report, right, and I don't think he goes this far, but if it is read to say that encryption is literally blinding ISPs, that it means that ISPs have very little revenue to make from the stream of data that they are being deprived. The benefit that is lost is very small. You can't have it both ways. Right? Either the data continues to be valuable for advertising which is exactly why it continues to be a potential privacy violation or the data is blinded through encryption which saves us from

privacy violation, but it also makes it nearly worthless to the ISP.

Again, I wish we have the magic wand that would allow us to have the optimal results of both of those things, but I am sorry to say it just doesn't exist.

Mr. McNerney. Mr. Ohm, does this proposal also result in increased confusion to consumers?

Mr. Ohm. No, I mean so the consumer confusion point has been made repeatedly in this debate. The entire essence of the FTC framework which has been lauded by everyone is that consumers somehow will read hundreds of privacy notices, become informed about the different choices and make intelligent choices all along. This is the premise of the FTC model.

We are talking about adding a few more privacy notices. I don't understand why this is going to increase consumer confusion in the ways that it has been argued. That argument, I will be quite honest, I have thought a lot over the last 4 days about what that argument even means. And if we believe in the FTC model, it is hard to say that this is going to increase consumer confusion.

Mr. McNerney. Mr. Chairman, I yield back.

Mr. Shimkus. The gentleman yields back his time. The chair now recognizes himself for 5 minutes for questions. This is

actually a great hearing. I appreciate your time. It is very difficult. I wish the Johnson clan was still here because they are like most -- you have got smart people, obviously, behind you that are watching this very closely, but they are average Joes, right? They are just trying to figure out. They are dealing with FTC, FCC, ISP, browsers, and all this world that you are digging deep into where everybody else's head is kind of spinning. That is why I am a former infantryman. We had the KISS principle, Keep It Simple.

How many of you think it is time to rewrite the Telecom Act? Mr. Brake? Mr. Leibowitz? Mr. Ohm? Come on, join the movement here.

Mr. Ohm. I think laws are meant to be reassessed.

Mr. Shimkus. Very good, I do, too. And the '96 Telecom Act is great. It did things that hadn't been done before. It dealt with Internet issues. But it really was and tried to bring competition into the market and it also did voice and video delivery. It wasn't in this data world. I mean it is 20 years now. There was no Facebook, Instagram, Pinterest, Twitter, Snapchat, YouTube, BuzzFeed. None of those. We are in a different world, so that is why I am all in. It is time to do the hard work and really to keep it simple, so we don't have this fight. We have this fight, FTC, FCC. We need to simplify this

process.

And there is historical activities that have been done, that have been proven correct. But I don't know if people are going to just count the other aspects of this whole privacy security and the stuff my colleague, Mr. McNerney talked about. Right? Especially on security. I have been pretty vocal on Apple and encryption and shouldn't there be a way that they give it back to Apple, get the information so we can do our security issues?

You have a staffer behind you that keeps shaking his head yes or no on everything that is being said. And I don't appreciate it. So I think we really need to open up the debates again.

I also do some European issues, Eastern European, National Security, NATO, E.U., so I have been following this safe harbor stuff now turned into U.S.-E.U. Privacy Shield debate. And the European Commission, Commissioner Vera Jourova confirmed yesterday, which means today, that they should be close to an agreement. What is that agreement based upon, FTC or FCC?

Mr. Leibowitz, why don't you give me a --

Mr. Leibowitz. Well, I mean I think that the Executive Branch is holding up the FTC approach as the approach that protects privacy including the privacy of European consumers. That is the privacy shield. And my concern and I think the Executive Branch's concern, but I won't speak for them, is that if you are criticizing

the FTC approach as too weak, and actually, I think in many ways the FTC is stronger than the FCC approach --

Mr. Shimkus. Quickly, quickly.

Mr. Leibowitz. It puts the American Government in a potentially complicated position as it is negotiating that privacy shield.

Mr. Shimkus. Let me go to Mr. Brake. What signal are we sending to the European Union?

Mr. Brake. I absolutely agree with Mr. Leibowitz. I think this undermines our stance that the FTC approach and in a true fact, the FTC approach has been successfully applied to a number of different Internet actors all across this ecosystem.

If I may very quickly jump back to your earlier point about the history of legislation. I think it is important to point out Professor Ohm has stated that it is unambiguous that 222 authorizes the FCC to regulate here. I think that that is questionable. This statute, this section of the statute was written, the '96 Act was written to introduce competition in telephone networks. So this was a different type of network, different actors, and is largely focused on competition, not pulling information from rival networks as competition was introduced to telephones, was not focused on privacy.

Mr. Shimkus. Thank you. So let me continue to make this

as confusing as possible.

Mr. Ohm, does it seem contradictory to you that the FCC is seeking to impose stringent regulations or more stringent on the ISPs, while at the same time opening up consumer viewing habits for anyone to track in the FCC's current proceedings on set-top boxes?

Mr. Ohm. Set-top box privacy is something that we should be concerned about as well. I completely concede that. I think the ability to track websites is richer data and more likely to cause privacy harms. I absolutely think that is true, too.

The other thing I will say in response to your question is there has been the specter throughout this entire hearing that the FCC somehow is prohibiting conduct when in my reading of the NPRM they are actually just shifting to an opt-in consent model. And so they are still giving you the ability to be very, very innovative in your business models, as long as you tell the consumer what you want to do and get their permission to do it. I mean that seems a far cry from a blanket prohibition.

Mr. Shimkus. Excellent, excellent. Thank you for your time and I will now yield back my time and turn to my colleague from Kentucky, Mr. Yarmuth, for 5 minutes.

Mr. Yarmuth. Thank you, Mr. Chairman. I also want to commend the panel. It has been a very interesting discussion and

everyone makes very good cases, I think. I will disagree -- agree with Mr. Shimkus and in doing so disagree with Mr. Ohm. 1996 is the Dark Ages in terms of where we are. And one of the things that I constantly obsessed about is how we as a Congress which moves at its optimum efficiency at 10 miles an hour, probably these days 2 or 3 miles an hour, and in a world that is moving at 100 miles an hour, and how do we possibly keep pace in making policy?

I am one who is willing to sign on right now to Mr. Shimkus' idea of rewriting the Telecommunications Act. I think it is negligent that we don't consider doing that.

I am concerned about a couple of things. One is I personally would prefer one agency to deal with one subject, philosophically, generally speaking. I also think it is important that we not only have an enforcement facility, but we also have a rulemaking facility. I think we can't just say go out and do whatever you want and then we will clamp down on you. I don't think that makes sense.

I also don't think it is useful in a rule or in statute to distinguish between the participants in this world. I look at the cross media ownership rules and how silly they are in today's world when every broadcast facility is also doing print. They are doing it online, but they are doing print. And every newspaper is doing broadcasting. I mean there is no distinction

any more between those functions. And certainly the public doesn't get them. So I am sure Google -- my district of Louisville, Google is coming in right now with putting up high speed capacity, competing with the existing Internet service providers. Those worlds are going to merge as well. And ISPs are not going -- 5 years from now are not going to be what ISPs are now.

I also understand very clearly the need to maintain this advertising capability online. I was involved for many years and now my son is involved in a free media publication that only survives because advertising is in there. As a matter of fact, the entire history of commercial broadcasting in this country involves advertising that consumers accept. They accept the intrusion. Now they can record and fast forward them, but there wouldn't have been broadcast television, commercial television, nor would there be radio without advertising. So I accept the fact that we need to accommodate those.

All that being said, I am not really sure where I come out on this. I suspect that again, I think we do need rules going -- the rules of the games, as well as an enforcement capability.

But would you comment, Mr. Ohm, on this whole question about edge providers and that broadband providers sit in a privileged place and at the bottleneck? Can you explain what that means

being in a privileged place?

Mr. Ohm. Sure, absolutely. And if I may follow and connect that to some of the things that -- the excellent points that you have just brought. So you have compared the advertising ecosystem of our online world and let me be clear. In 1996, there was a different Internet. I first signed on in 1991 and it was a very empty, lonely place at the time.

But advertising, as it existed in the radio and television markets that you talked about, was not behavioral advertising, right? It was keyed to the television show you were watching or the radio show.

There is a lot of advertising on the Internet that is contextual in the same way and it makes a lot of revenue for a lot of people and creates all sorts of innovation. So we are talking about the slim layer at the top which is how many extra pennies can we extract from a consumer if we know this digital dossier about them? Right? So it is not enough to say you are on a travel website, I am going to show you a travel ad. The move is yes, but we want to know when you are going to Cabo San Lucas and we want to know whether you would like an aisle seat or not. This is the extra stuff we are talking about.

We are not talking about getting rid of advertising. We are certainly not talking about getting rid of contextual

advertising. We are talking about the advertisers' ability to pry essentially into your habits, into your mind, into your experiences, into your preferences, and build a virtual version of you in their server that they can then use to serve you after.

Mr. Yarmuth. Every third paragraph of a political story I read now has a golf-related ad.

Mr. Ohm. Yes, right. It happens to all of us. You look at a pair of shoes and it haunts you for the next month. Maybe I should buy the shoes.

So what we are really talking about here is that thin behavioral layer. And by the way, one of the things that has been criticized is that there is disparate treatment. The disparate treatment means there will be online behavioral advertising throughout the Internet ecosystem, in fact, also by ISPs, because the ISPs no doubt will convince some of their customers to opt-in based on whatever benefit they are going to give them and they will be able to take part in this ecosystem, too.

Nothing in the proposed rules stops an ISP for competing directly with a search engine or with some other service, a social network, right?

Mr. Leibowitz. Let me just add --

Mr. Yarmuth. My time is up. I would love for you to answer, but --

Mr. Leibowitz. If I could just add to your point and I agree with most of what Professor Ohm said and I agree with most of what you said. First of all, those golf ads that you are getting, those are invisible cyberazzi who are collecting information. They are not touched by this. The people who put cookies in your computer, they are not touched by this proposed rule.

Second of all, 1996 was the Dark Ages when it came to the Internet, and that is why I think all of you, and you are the policy makers, believe that there should be -- seems like there is bipartisan support for a rethink of the Telecommunications Act.

When we did our rethink of privacy, protecting consumer privacy in an era of rapid change in 2012, I want to make a process point. We took 450 separate comments. We took 2 and a half years. We did three workshops. We did a workshop after we put out a draft report. This is really important stuff and you can't do it in a quick, 6-month turnaround under the APA. You need to get it right. And this rulemaking, this proposed rulemaking and it can improve, doesn't get it right.

Mr. Walden. [presiding] All right, I need to go now to Mr. Johnson from Ohio for questions.

Mr. Johnson. Thank you, Mr. Chairman. Mr. Leibowitz, do you think the FCC's proposed rules could interfere with the routine business operations?

Mr. Leibowitz. Well, I think they encompass routine business operations so that, for example, the FTC approach, the FTC said in its comment to the FCC, you know, you should have an opt-in for sensitive data, perhaps for Deep Packet Inspection. That is not actually being reviewed right now. But not for routine information. That benefits consumers. There is no harm to --

Mr. Johnson. Okay, all right. Well, following on with you, Mr. Leibowitz, I am concerned about the huge scope of data covered by the FCC's rules. There seem to be many data elements, for example, IP addresses, device identifiers, domain information that cannot on their own identify a specific person, but are nonetheless defined as customer proprietary information under the proposal.

I understand that a number of commenters that are not ISPs, IT companies, network engineers, security specialists, etcetera, have expressed concern about the unprecedented scope of the data being covered here, and its potential impact on how the Internet works and how consumers experience the Internet today. Are you concerned about that as well, the data that is covered?

Mr. Leibowitz. I do share those concerns.

Mr. Johnson. Okay, well, I am particularly concerned with the number and complexity of the issues raised in this proceeding

and the potential for unintended consequences. As I understand it, before the FTC adopted its framework, your agency spent over 15 months working through various practical applications and quote unquote use case scenarios to try to minimize the potential for unforeseen adverse facts, But the FCC seems determined to get an order out by September or October no matter what.

Isn't rushing the process incompatible with the agency's imperative to think through all of the potential consequences of this kind of regimen?

Mr. Leibowitz. Well, you know, I think the agency is operating, the FCC is operating under the APA, but to do this rule properly, you need to think about it carefully. And I will say, going back to Mr. Yarmuth's point, I was with -- after we had that 15-month process, we did an event at the White House where the Obama administration rolled out its consumer bill of rights, privacy rights. And it called for the FTC to have sole jurisdiction, only jurisdiction over privacy issues, consistently across every industry.

And so going back to Mr. Yarmuth's point, if you are going to have one -- the FTC shouldn't be doing spectrum allocation. And I am not so sure the FCC should be doing privacy.

Mr. Johnson. Okay, all right. Thank you. Mr. Brake, one of the major flaws we have heard about today in the FCC's proposed

rules is the lack of uniformity for the rules. What does this mean for consumers and their data as they use the Internet and how does privacy protection change, depending on what services or products they may have using?

Mr. Brake. Thank you for the question. I think one of the important reasons that we want to have uniform rules is to allow for industries to explore different parts of the Internet ecosystem unimpeded by particular regulatory restrictions. So I think that is my overwhelming goal is to allow companies to innovate across different sector lines.

To my mind, I think that the distinction between edge and broadband provider is going to be increasingly blurred over time and so to be going back to this model of creating sector specific regulatory silos is just taking a step backwards in time.

So I think over the long term it affects consumers in that we would see less innovation, less flexibility in different business models throughout the entire Internet ecosystem, the more that we build up these specific sector rules.

I also agree with the point made by Mr. Leibowitz earlier that I think this will continue to confuse consumers to think that information, as it is treated by particular industry actors would be different depending on whether they want to opt-in or opt-out, could be different depending not on their expectation of privacy

or what the actual data is, but on the specific actor that they are interacting with.

Mr. Johnson. Okay, well, great. Thank you, Mr. Chairman. I yield back.

Mr. Walden. The gentleman yields back. The chair now recognizes Ms. Clarke for her opportunity to ask questions. Please go ahead.

Ms. Clarke. Thank you, Mr. Chairman. I thank our ranking member. I thank our panelists today for lending their expertise on this very complex issue of privacy and innovation.

Mr. Ohm, the rise of mobile broadband, you alluded to this in one of your answers earlier, has ushered in a new era of convenience in the terms of access to the Internet. But it has also created highly detailed portraits of the user's life.

The information gathered from a cell phone, particularly real time location data is far more sophisticated than information gathered from wired connection. Can we really expect an industry framework to protect this sensitive information when it represents such a significant marketing opportunity?

Mr. Ohm. That is right. Some describe kind of the great untapped part of the advertising market to be local advertising. So the idea is if you are walking by -- I was going to say Circuit City. I am not sure they exist in large numbers any more.

Ms. Clarke. They don't.

Mr. Ohm. But if you walk by a particular retailer, they will notice you are there and send you an advertisement. So there is a lot of competition to figure out where you are on a minute-by-minute basis to fix your location.

I have written an article in the Southern California Law Review about sensitive information. And in that article, I have gone on the record saying Congress really ought to have a location privacy protection act in 2016 for exactly the reasons that you are suggesting. This is deeply sensitive information. There are many stories about women entering battered women shelters and the first they are told to do is take their battery outside of their telephone, right, because there are so many different ways that not only corporations, but maybe even other individuals can track your location using a tracking device that we all carry with us. It is something to be quite concerned about.

Ms. Clarke. There is also the concern now with even automobiles and --

Mr. Ohm. That is right. Smart Cars and autonomous cars and one other thing I will say on this because I could not agree more and I have not had the opportunity to say that the FTC report is a towering achievement for an agency. They recognize -- and I didn't work on it. This actually predated my time there. They

recognize in the report that location information does belong in the categories of sensitive information for exactly the same reasons.

Ms. Clarke. A recent story regarding Cable One, an Internet service provider, illustrates the fears that I think many have about Internet ecosystem without sufficient privacy protection. According to their CEO, the company was able to determine which customers were high value and low value based on their credit scores. As a result, some customers received better service from Cable One than others simply because their personal information was available.

Are you concerned that customers' data could potentially be used to discriminate against them as in the case of Cable One?

Mr. Ohm. Yes, and not only am I concerned, this is where the pessimism really starts to come out, I am sorry to say. Study after study has shown that there is data that someone can use to guess your FICO score with great accuracy, even if they promise to never look at your FICO score, right?

And so there is one story that is documented, although I didn't do the research, that a Canadian bank asked a single question which was is this person applying for a loan the type of person who buys the rug protectors on the bottom of their furniture? And if they doled out loans based only on that one

piece of information, they basically make about the same in terms of defaults and returns.

So the idea here that I am trying to get to is if we let ISPs have unrestricted access to the domain data that we have been talking about this entire day, this Cable One story may not be an outlier, right? It may be that what they are doing is using big data techniques to infer that you are not a good credit risk, even if they promise never to look at your FICO score. So this relates absolutely to the need for the FCC rule.

Ms. Clarke. Mr. Leibowitz, did you want to respond?

Mr. Leibowitz. I was going to say, it definitely should concern all lawmakers. It is an important policy issue and the FTC has done multiple workshops; one when I was there; some since I have left, about this very issue and what it does to expand the already troubling digital divide. So it is an issue.

Now I also would say that there are some other areas within the FCC proposed rule that would potentially expand that digital divide and make it worse. So take, for example, a 23-year-old who lives in Crown Heights, or a family of four that lives there and is on $40,000 a year. If it wanted discounted Internet service in exchange for collection of data, maybe not the dissemination of data, by name, it could be de-identified and it may not be disseminated at all, that person wouldn't have the right

to make a choice because it would be banned by the FCC's proposed rule.

It just seems to us, the people and consumers ought to have choice, particularly when the choice is maybe some modest collection of data against savings of hundreds of dollars a year. That could be important to people.

Ms. Clarke. Mr. Brake, did you want to respond?

Mr. Brake. On the Cable One point, I think there is general agreement that nobody wants to see anyone denied service or offer particularly bad service based on any sort of collection of information, but it seems to me that if companies want to address issues like churn or decide who to up sell based on particular data sets, that seems entirely consistent with other areas of the economy and can make the overall system more efficient.

And moreover, I think it is important that data sets like that can be more accurate and better than other proxies that could have been used in the past.

Ms. Clarke. My time has expired, but I thank you for your responses and I yield back, Mr. Chairman.

Mr. Olson. [presiding] The gentlelady's time has expired. The chair recognizes the gentleman from Kentucky, Mr. Guthrie, for 5 minutes.

Mr. Guthrie. Thank you, Mr. Chairman, and thank you all for

testifying today. Congress should pay close attention to how agencies use and perhaps misuse statutory authority.

But Mr. Leibowitz, I have a question first for you. The FCC is intending to apply a statute written to cover information about telephone calls to information about consumers' online activities. In doing so, the FCC has broadly, perhaps too broadly, interpreted what information is included in the statutory requirement. And my question is do you think Congress intended information such as IP and Mac addresses to be subject to Section 222?

Mr. Leibowitz. Well, I was a staffer in the Senate during the '96 Act. People on this committee were there in the '96 Act. I will leave it for others to -- I will leave it for members of this committee to make that determination and perhaps for the courts.

I would say it is certainly not clear from Section 222 that the Telecom Act, at least in my reading, was supposed to be quite so expansive. I am sure there is going to be more discussion about that going forward.

Mr. Guthrie. I have a second question and I will lead up to it, but I have concerns about -- I do have concerns about FCC's treating ISPs' use of data differently than other businesses who use online data. For one, I believe that consumers are more

likely to have questions about how other online companies out there are mining their online data for ads and targeted marketing and other uses as opposed to how service providers are using it.

But as we have discussed at length today, the Commission has focused on treating two parts of the same industry very differently which also raises constitutional questions.

So for Mr. Leibowitz, I guess three questions, and I will ask them all and I will let you answer. Can you elaborate on the constitutional concerns that have been raised about the FCC's proposal? And second, do you consider the FCC's proposal to be the least restrictive means of protecting consumer privacy as required under the test in the Central Hudson case?

Mr. Leibowitz. Well, that is one of the prongs in the Central Hudson case and I think there is an argument to be made that by not using the least restrictive means, that to address a problem which may or may not be a problem under one other prong of the Central Hudson test, that the FCC may exceed its constitutional authority.

Don't take my word for it. No one less than Larry Tribe has put a comment into the FCC that suggests that under the Central Hudson test, whether the asserted governmental interest is substantial, whether the regulation directly advances the government interest asserted, and whether it is more extensive

than necessary, and I would certainly, based on my experience, not as a constitutional lawyer, but as an FTC official think that it is more extensive than necessary whether it fails the Central Hudson test.

Mr. Guthrie. One more final question for Mr. Leibowitz. Can the FCC's approach really achieve its intended goal when it applies only to a subset of the online ecosystem?

Mr. Leibowitz. Well, it sort of depends on what its goal is at the FCC. I think the FTC's approach, when we were doing a deep think about privacy in 2010, '11, and '12, was that it should be technology neutral and when we held a special workshop to look at the issues of what we call large platform providers, that is, collectors of big data which include ISPs, Google, Facebook, various others, there was a general consensus at the workshop from consumer advocates, from businesses, from the Commission, that any restrictions ought to be content -- I am sorry, ought to be technology neutral and apply across the board. The FCC doesn't have the authority, it believes, to do that.

Mr. Guthrie. Thank you, and that finishes my questions. I will yield back a minute and 11 seconds.

Mr. Olson. The gentleman yields back. The chair recognizes the gentleman from New Jersey, the ranking member of the full committee, Mr. Pallone, for 5 minutes.

Mr. Pallone. Thank you. I wanted to start with Chairman Leibowitz. When you were chairman of the Federal Trade Commission, you testified before this committee that the FTC ought to have APA rulemaking authority. And last year, you testified you still held that position. So just stepping away from the FCC's specific proposals for a minute, do you continue to believe that the FTC should have APA rulemaking authority? You just have to answer yes or no, if that is okay.

Mr. Leibowitz. In my personal capacity, I do.

Mr. Pallone. Thanks. And then I wanted to ask you, you have talked about the amount of good work the FTC has been able to do for consumers even without rulemaking authority. And I know that one of the tools the FTC uses in negotiated consent decrees that last for 20 years, another tool is its ability to find practices unfair even without a finding of economy injury.

Can you just elaborate on what tools the FTC used during your time there a bit?

Mr. Leibowitz. The FTC used a variety of tools when I was there including strong orders, including policy papers, like this one on privacy, including rulemaking which we have for children and Paul Ohm was a critical part of the update we did for the Children's Online Privacy Protection Act to make parents the gatekeepers for protecting their children's privacy, but also

allow businesses some flexibility. So the FTC has all those tools and it continues to use all those tools.

Mr. Pallone. All right. Thanks. So I wanted to ask Professor Ohm, some claim the FCC's proposal will make consumers worse off because having new rules will be too confusing. They argue that the FCC would be better off using only the after-the-fact enforcement that the FTC has traditionally used for websites.

Now I have seen data that shows that two thirds of Internet users say that they would prefer more regulations than the ones that we are using today. Have you seen any independent research that shows whether consumers are confused if they are faced with these differing privacy regulations or policies?

Mr. Ohm. Thank you for the question. Survey after survey has demonstrated that consumers desperately want more privacy. And to be quite honest, I am not sure if they care if they get it from companies being beneficent or from the government imposing rules. They want more privacy, right?

And I have never, except with one odd question that was reported out last week, I have never seen a survey that said okay, which of the entities should owe you privacy and which shouldn't? This goes back to my earlier point about consumer confusion. A lot of our approach in privacy is that we give the consumer a lot

of credit. We treat them like a sophisticated individual with autonomy and intelligence and an awareness and incentives to worry about things like their privacy. This is kind of a bedrock underpinning of notice and choice.

And so once again, it really does confuse me to hear so many people say that the FCC rules are going to be the last straw that are going to kind of befuddle our poor consumers. I have a lot more faith in the consumers, right? I think it is not just a legal fiction that notice and choice works. I think it actually has been proved in survey, and research report after research report, but also in kind of just our lived experience. We actually have recognized that people can make good choices for themselves when they are armed with the right information. And that is all the FCC report does. There is no prohibition. It is opt-in consent and opt-out consent and actually some implied consent where consent isn't even necessary. Three simple categories, very easy to understand.

Mr. Pallone. All right. Thanks so much. Thank you, Mr. Chairman.

Mr. Olson. The gentleman yields back. The chair recognizes the gentleman from Missouri, Mr. Long, for 5 minutes.

Mr. Long. Thank you, Mr. Chairman. And Mr. Leibowitz, it is my understanding that the FTC has conducted more than 35

workshops, townhalls, and roundtables that have focused on emerging issues in consumer privacy and security. Have these sessions helped inform the FTC's protection of consumer privacy?

Mr. Leibowitz. Absolutely. Absolutely.

Mr. Long. Would the FCC perhaps benefit from a comparable process and series of events before adopting final rules?

Mr. Leibowitz. Certainly taking a modest step in that direction might be useful in understanding where they might find consensus.

Mr. Long. Can you pull your mic a little closer? When you turn your head, I lose you.

Mr. Leibowitz. I am sorry. No one is asking them to take 450 separate comments or to do 2 and a half years, to take 2 and a half years to go through a workshop and put out a draft rule and take 2 and a half years as we did to finish our report. But I think a little bit of additional thinking in that direction might be a very useful thing to moving towards a more balanced rule at least from the 21st Century Privacy Coalition.

Mr. Long. Okay. Mr. Brake, will the FCC's proposed rules promote competition in the online ecosystem?

Mr. Brake. No. I think that the FCC's rules insofar as they are explicitly structured around specific business models that broadband providers are currently engaged in and placing

limitations on any experimentation outside of that, I think it would greatly limit the possibility of broadband providers engaging in particularly new business models around target advertising that is most obvious. I think it is explicitly designed -- this is a common carriage of the 19th and the 20th century that is designed to lock in broadband providers into the historic business models that they have been engaged in.

Mr. Long. So I am assuming that you think FCC's proposed rules ignore the economic and technological realities of Internet ecosystem?

Mr. Brake. Yes. I think so. I think they do, yes.

Mr. Long. Thank you. And Mr. Leibowitz, the Notice of Proposed Rulemaking proposes that a person's physical address and telephone number be included among protection information, even though that is not the case under the agency's consumer proprietary network information rules for voice providers. So a phone company can share name and address and what is called a phone book. A lot of people might not remember those, but they can share a name and address in a phone book, but if the broadband provider were to share the same information, it would be on the hook for even an inadvertent action such as a bill mailed to the wrong address. Why the change in policy?

Mr. Leibowitz. Right, I mean look, there is a lot of

additional thinking that might be done to smooth out some of those inconsistencies. And I just want to make a point because I have heard a lot today about either -- it is like binary. Either there is nothing anyone can do or you have to take the FCC's NPRM as it is and just go forward with it. And that is just not the truth.

The truth is that you can create some limits on ISPs and protect privacy at the same time without making everything opt-in. I would just, if I have one suggestion for the FCC which is really the decider here, it would be take a look at the FTC's comment. I know they are going to do this. And be responsive to it. Because if that happens, and I hope it will and I believe it will, because I believe in agencies doing the right thing in rulemakings, they are going to make their rule much more balanced, still very privacy protected, but also flexible to allow the innovation, I think that all of us on the panel, all of us on the dais would like to see.

Mr. Long. Thank you. I have a little bit less than a minute, but Mr. Ohm, when you talk about intellectual privacy rights, can you kind of define what you are talking about and how that works?

Mr. Ohm. Sure. This comes from Professor Neil Richards at Washington University in St. Louis. The theory is that in many ways we are composed and we are kind of in a central core of us

is what we read and say, and that there should and ought to be additional privacy protections.

Professor Richards is a First Amendment scholar who by the way couldn't disagree with Professor Tribe's analysis of this more. We have been trading some emails. But Professor Richards says that when someone implicates your ability to read and chills your ability to read what you want to read, that should be a heightened privacy concern.

If I may, since we are almost out of time and on a moment of agreement here, I think it is a wonderful thing about the American system that the FCC is doing this public notice and comment process. Nothing is final. They are going to reassess it as they go along. They have, the last time I checked, more than 50,000 comments filed in this proceeding, and they are going to have to talk about those comments. So we are going to know whether they took these concerns, and there are a lot of concerns, seriously. And if they don't, they will be held to account by this body and others.

Mr. Long. Thank you. I am out of time, Mr. Chairman.

Mr. Olson. The gentleman yields back. The chair recognizes himself for 30 minutes, 5 minutes. Just making sure you are paying attention.

Okay, the chair yields to the gentlelady from Illinois, Ms.

Schakowsky, for 5 minutes for questions.

Ms. Schakowsky. First of all, I want to thank the chairman and ranking member so much for allowing me to be here today and to ask a question. I am not on this committee, but I have great interest. So let me start out. Mr. Leibowitz, you noted, not that I heard it, but I read it, that privacy is an important part of the Federal Trade Commission's consumer protection mission and you praised the FTC's proven track record of success on privacy enforcement actions.

Last week, the Subcommittee on Commerce, Manufacturing, and Trade, where I am the ranking Democrat, held a mark-up on a bill to change the FTC's enforcement authorities. Given your experience as chairman of the FTC, I would like to ask you some questions about how the FTC protects consumers.

Let me ask this one. Currently, a company can use evidence of compliance with guidance as evidence of good faith, but a company cannot use evidence of compliance with guidance as evidence of compliance with law. Do you agree with Professor David Vladeck's testimony from a couple of weeks ago that allowing a company to use evidence of compliance with guidance to prove compliance with the law would create a significant loophole in the FTC enforcement actions and make it more difficult for the FTC to protect consumers?

Mr. Leibowitz. Well, let me say two things. First of all, I am testifying for the 21st Century Privacy Coalition which does not have a position -- I have not polled them on these 17 proposed bills that are coursing through your committee. I would have, and I haven't read this bill particularly, but I would have concerns with that bill in my personal capacity, absolutely.

Ms. Schakowsky. As you know, the FTC can only make allegations that a person has violated a law. Did the Commission ever bring cases against a company simply for its failure to comply with guidance?

Mr. Leibowitz. Guidance is different, as you know. And we worked so closely together when I was at the FTC and you were ranking on the Consumer Protection Subcommittee.

The FTC brings cases based on violations of the law, not violations of guidance. Now the guidance are there for businesses and consumers so that they understand what is and what is not permissible.

Ms. Schakowsky. Just like the companies you represent, the FTC filed comments in response to the FCC privacy proposal. Is that something the FTC commonly does, provide comments to other agencies?

Mr. Leibowitz. It does it from time to time. I am particularly pleased that my former agency did it here because

my sense is that it reads -- if the FCC closely reads, and I believe it will, the FTC's comment which is based on our 2012 privacy report which you know about, it will dramatically improve its draft rule.

Ms. Schakowsky. Would such comments include an economic analysis? Would the FTC be able to do a meaningful economic analysis within the time a comment period is typically open?

Mr. Leibowitz. Would the FCC be able --

Ms. Schakowsky. No, would the FTC be able to do a meaningful economic analysis?

Mr. Leibowitz. The FTC always thinks about the cost benefits of privacy protections as it writes its report, but if you mean some sort of cost benefit as you do with a major rule, I don't think the FTC would have time to do that and submit it with respect to the FCC rule, unless the FCC takes some additional time to think through its rulemaking. And given the complexities of that, they might decide to do that and it might be an appropriate thing to do.

Ms. Schakowsky. While you were at the FTC, I presume the FTC made at least one allegation using its unfairness authority, right?

Mr. Leibowitz. Many allegations and in a bipartisan way, too.

Ms. Schakowsky. The Commission used the unfairness statement issue in 1980, correct?

Mr. Leibowitz. Yes, it did.

Ms. Schakowsky. And should we be selectively codifying the statement so that unfairness claims can only be made if there is a substantial economic injury or should we be concerned about cases like the designer where in-home computer cyber-peeping case or concerned about that kind of invasion of privacy?

Mr. Leibowitz. I think you know what my position would be in my personal capacity and I would be concerned about any rules that hamstrung the FTC which is an agency that I think that clearly I hear today, really from both sides of the aisle is one that has done a great job of protecting consumers. I would have to look at the legislation some more, but it sounds to me like it is concerning.

Ms. Schakowsky. Thank you. I really thank the committee for allowing me to speak. Thank you.

Mr. Olson. The gentlelady yields back. The chair would now recognize himself for 5 minutes for questions. First of all, thank you, Chairman Leibowitz, Mr. Ohm, and Mr. Brake for coming this afternoon.

Having worked for Phil Gramm for his last 4 years as our Senator from Texas, I have learned some pearls of Texas wisdom.

One is, and I quote, "It is easier to kill a vampire than a bad law or an over-reaching federal rule."

In my humble opinion, FCC's NPRM contains tentative conclusions that may be harder to kill than Count Dracula. My first questions are for you, Mr. Brake, and you, Chairman Leibowitz. In your opinion, are there tentative conclusions in the NPRM and how hard would they be to overcome, those conclusions in the record?

Mr. Brake, you first.

Mr. Brake. Absolutely. The Notice of Proposed Rulemaking, obviously a long, complex document that makes a number of tentative conclusions, a number of tentative proposals that I think sets the framework in the wrong direction. So I think a course correction, something more into the FTC approach.

And if I can narrow down on this issue because I think Professor Ohm hit on it that is really the heart of the question is the choice of architecture framework of the opt-in versus the opt-out. And so the FCC proposes to require an opt-in for any non-communications related use of data. We think that the correct approach to promote innovation would be to require only an opt-out.

Here, you are asking consumers, many of which are very happy to make tradeoffs around their privacy and do not have as deep

a concern about privacy as Professor Ohm or some of the other privacy advocates in the proceeding, to take the extra step and opt-in. And so fundamentally, any consumer who really cares about their privacy can take the extra step and find that opt-out and that is also a problem. I think just correcting that choice of architecture could do an awful lot of good.

Mr. Leibowitz. So just a followup.

Mr. Olson. Yes, sir.

Mr. Leibowitz. You know, I think the draft at least overshoots the mark. It creates, going back to your Phil Gramm analogy, it creates sort of a Boogie Man among ISPs. They are not collecting Deep Packet Inspection information of web browsing history now. And they are not collecting more information than others in the Internet ecosystem. You ought to treat them, if you want to do privacy, if you want to enhance privacy protections for consumers by rule, you ought to do it with respect to sensitive information.

Mr. Olson. One more question to you Chairman Leibowitz and you, Mr. Brake, as well. Does the FCC proposal set the stage for double jeopardy? Is there potential for subjecting alleged violators to sanctions from two separate agencies or one agency, but not the other? Is that a real possibility?

Mr. Leibowitz. You know, that is an interesting question.

I think with respect to ISPs, no, because by using Title II for net neutrality, it is just taking jurisdiction away from the FTC. Now, if the FCC tries to reach beyond that jurisdiction, then you could have two agencies doing privacy protection for the same company. But I will also say this, in the 8 and a half years I have served on the FTC, both as a commissioner and then as chairman, there was never an instance where almost all of the privacy protection was ceded to the Federal Trade Commission, even as it came to ISPs. And ISPs were subjects of some privacy cases involving the FTC.

Mr. Brake. Certainly, so I would say on the first point the question of the exact reach of the FTC's exemption, and the FTC experts can correct me if I am wrong, but my understanding is that is something of an open question as to whether or not the commentary exemption applies on a matter of status whether or not a common carrier is a common carrier or whether or not it is activities based, whether or not they are engaged in particular common carrier, classic common carrier activities. And frankly, to my mind, I think it is a question of whether or not privacy falls under the common carrier status or as an activity whether or not that is more a private carrier activity or common carrier activity.

I know it is commonly accepted that the common carrier

exemption has been triggered, but to my mind if the FTC and FCC wanted to agree that this is a matter of -- that privacy is a matter of private carriage, to my mind it would be lawful for the FCC to leave this matter to the FTC entirely. And that is what we have advocated.

On the second point, I think Mr. Leibowitz is correct that if the FCC wanted to expand its reach to look under 706 under regulating edge providers, that would certainly throw all this into great confusion.

Mr. Olson. Well, thank you. My time has expired. And seeing no further members here, the chair announces to all the members you have 5 days to submit questions for the record.

I want to thank all of the witnesses for coming and remind everybody that today is the Army's birthday. The United States Army is 240 years old, but the birthday present they will get from Navy is a victory at the football game. The committee stands adjourned.

[Whereupon, at 12:20 p.m., the Subcommittee was adjourned.]