

FCC OVERREACH: EXAMINING THE PROPOSED PRIVACY RULES

HEARING BEFORE THE SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY OF THE COMMITTEE ON ENERGY AND COMMERCE HOUSE OF REPRESENTATIVES ONE HUNDRED FOURTEENTH CONGRESS SECOND SESSION

JUNE 14, 2016

Serial No. 114-154



Printed for the use of the Committee on Energy and Commerce
energycommerce.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE

21-417 PDF

WASHINGTON : 2016

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

COMMITTEE ON ENERGY AND COMMERCE

FRED UPTON, Michigan

Chairman

JOE BARTON, Texas

Chairman Emeritus

ED WHITFIELD, Kentucky

JOHN SHIMKUS, Illinois

JOSEPH R. PITTS, Pennsylvania

GREG WALDEN, Oregon

TIM MURPHY, Pennsylvania

MICHAEL C. BURGESS, Texas

MARSHA BLACKBURN, Tennessee

Vice Chairman

STEVE SCALISE, Louisiana

ROBERT E. LATTA, Ohio

CATHY McMORRIS RODGERS, Washington

GREGG HARPER, Mississippi

LEONARD LANCE, New Jersey

BRETT GUTHRIE, Kentucky

PETE OLSON, Texas

DAVID B. MCKINLEY, West Virginia

MIKE POMPEO, Kansas

ADAM KINZINGER, Illinois

H. MORGAN GRIFFITH, Virginia

GUS M. BILIRAKIS, Florida

BILL JOHNSON, Ohio

BILLY LONG, Missouri

RENEE L. ELLMERS, North Carolina

LARRY BUCSHON, Indiana

BILL FLORES, Texas

SUSAN W. BROOKS, Indiana

MARKWAYNE MULLIN, Oklahoma

RICHARD HUDSON, North Carolina

CHRIS COLLINS, New York

KEVIN CRAMER, North Dakota

FRANK PALLONE, Jr., New Jersey

Ranking Member

BOBBY L. RUSH, Illinois

ANNA G. ESHOO, California

ELIOT L. ENGEL, New York

GENE GREEN, Texas

DIANA DeGETTE, Colorado

LOIS CAPPS, California

MICHAEL F. DOYLE, Pennsylvania

JANICE D. SCHAKOWSKY, Illinois

G.K. BUTTERFIELD, North Carolina

DORIS O. MATSUI, California

KATHY CASTOR, Florida

JOHN P. SARBANES, Maryland

JERRY McNERNEY, California

PETER WELCH, Vermont

BEN RAY LUJAN, New Mexico

PAUL TONKO, New York

JOHN A. YARMUTH, Kentucky

YVETTE D. CLARKE, New York

DAVID LOEBSACK, Iowa

KURT SCHRADER, Oregon

JOSEPH P. KENNEDY, III, Massachusetts

TONY CARDENAS, California

SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY

GREG WALDEN, Oregon

Chairman

ROBERT E. LATTA, Ohio

Vice Chairman

JOHN SHIMKUS, Illinois

MARSHA BLACKBURN, Tennessee

STEVE SCALISE, Louisiana

LEONARD LANCE, New Jersey

BRETT GUTHRIE, Kentucky

PETE OLSON, Texas

MIKE POMPEO, Kansas

ADAM KINZINGER, Illinois

GUS M. BILIRAKIS, Florida

BILL JOHNSON, Missouri

BILLY LONG, Missouri

RENEE L. ELLMERS, North Carolina

CHRIS COLLINS, New York

KEVIN CRAMER, North Dakota

JOE BARTON, Texas

FRED UPTON, Michigan (*ex officio*)

ANNA G. ESHOO, California

Ranking Member

MICHAEL F. DOYLE, Pennsylvania

PETER WELCH, Vermont

JOHN A. YARMUTH, Kentucky

YVETTE D. CLARKE, New York

DAVID LOEBSACK, Iowa

BOBBY L. RUSH, Illinois

DIANA DeGETTE, Colorado

G.K. BUTTERFIELD, North Carolina

DORIS O. MATSUI, California

JERRY McNERNEY, California

BEN RAY LUJAN, New Mexico

FRANK PALLONE, Jr., New Jersey (*ex*

officio)

C O N T E N T S

	Page
Hon. Greg Walden, a Representative in Congress from the State of Oregon, opening statement	1
Prepared statement	3
Hon. Anna G. Eshoo, a Representative in Congress from the State of Cali- fornia, opening statement	5
Hon. Marsha Blackburn, a Representative in Congress from the State of Tennessee, opening statement	6
Hon. Frank Pallone, Jr., a Representative in Congress from the State of New Jersey, opening statement	7
Prepared statement	8
Hon. Fred Upton, a Representative in Congress from the State of Michigan, prepared statement	69

WITNESSES

Jon Leibowitz, Co-Chair, 21st Century Privacy Coalition	10
Prepared statement	12
Answers to submitted questions	86
Paul Ohm, Professor, Georgetown University Law Center, and Faculty Direc- tor, Georgetown Center on Privacy and Technology	22
Prepared statement	25
Answers to submitted questions	91
Doug Brake, Telecommunications Policy Analyst, Information Technology and Innovation Foundation	34
Prepared statement	36
Answers to submitted questions	96

SUBMITTED MATERIAL

Letter of June 1, 2016, from Mr. Upton, et al., to the Honorable Tom Wheeler, Chairman, Federal Communications Commission, submitted by Mr. Wal- den	71
Letter of June 13, 2016, from Matthew M. Polka, President & CEO, American Cable Association, et al., to Mr. Walden and Ms. Eshoo, submitted by Mr. Walden	75
Letter of June 13, 2016, from the American Advertising Federation, et al., to Mr. Walden and Ms. Eshoo, submitted by Mr. Walden	78
Letter of June 14, 2016, from Steven K. Berry, President & CEO, Competitive Carriers Association, to Mr. Walden and Ms. Eshoo, submitted by Mr. Walden	81
Letter of May 25, 2016, from Mr. Rush, Mr. Olson, et al., to the Honorable Tom Wheeler, Chairman, Federal Communications Commission, et al., sub- mitted by Mr. Walden	84

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, DC.

The subcommittee met, pursuant to call, at 10:18 a.m., in room 2123 Rayburn House Office Building, Hon. Greg Walden (chairman of the subcommittee) presiding.

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

Also present: Representative Schakowsky.

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

OPENING STATEMENT OF HON. GREG WALDEN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OREGON

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 own 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.

[The prepared statement of Mr. Walden follows:]

PREPARED STATEMENT OF HON. GREG WALDEN

Good morning. I'd like to thank our witnesses for joining us today to offer their expert counsel.

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 the Internet and on consumers. The Commission shortsightedly looks at one 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 shortsightedly 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 hasn't changed everything.

The Internet has long been known for being disruptive. Rare is an industry that the Internet hasn't changed. 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 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's 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's consumers who will pay the price. The FCC has proposed a set of regulations that would not only single out ISPs based on 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 this 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, and most importantly, what best serves American consumers. The Internet has helped to shape our economy in ways we could have never imagined, we must work together to preserve the competition and innovation the Internet embodies. Thank you to our witnesses for being here and I look forward to hearing your testimony.

Mr. WALDEN. I yield the balance of my time to the ranking—or the vice chair of the 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 removed 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 proposed 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 hearing 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 and retail associations 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.

[The information appears at the conclusion of the hearing.]

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.

OPENING STATEMENT OF HON. ANNA G. ESHOO, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

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 Web sites 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 Web sites 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 the 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.

OPENING STATEMENT OF HON. MARSHA BLACKBURN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TENNESSEE

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 that 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.

OPENING STATEMENT OF HON. FRANK PALLONE, JR., A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW JERSEY

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 DC 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 Web sites 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 Web sites. That would allow the FTC to craft privacy rules for Web sites 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.

[The prepared statement of Mr. Pallone follows:]

PREPARED STATEMENT OF HON. FRANK PALLONE, JR.

Thank you Mr. Chairman and Ranking Member Eshoo. And thank you to our three witnesses for being here today.

Today, we're just learning that the DC Circuit Court of Appeals has upheld the FCC's Open Internet Rules. 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, it seems this was a big win for consumers. This decision 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. 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's very important to them that they have control over who has access to their information.

It's important that we take these opinions and concerns into account as we move forward with this hearing today.

It's 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 Web sites 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—not less.

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 Web sites. That would allow the FTC to craft privacy rules for Web sites 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'm talking about would effectively gut the FTC.

It's 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. 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. When consumers are safe, we are all better off.

I look forward to today's discussion.

Mr. PALLONE. 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 time. 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 great 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 JON LEIBOWITZ, CO-CHAIR, 21ST CENTURY PRIVACY COALITION; PAUL OHM, PROFESSOR, GEORGETOWN UNIVERSITY LAW CENTER, AND FACULTY DIRECTOR, GEORGETOWN CENTER ON PRIVACY AND TECHNOLOGY; AND DOUG BRAKE, TELECOMMUNICATIONS POLICY ANALYST, INFORMATION TECHNOLOGY AND INNOVATION FOUNDATION

STATEMENT OF 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 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 could 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 because it is framed diplomatically, there are more than 25 separate instances where it raises concerns about the FCC's approach. Twenty-five. More than 25. There is no need for the FCC to embark on this dangerous path.

And by the way, after today's DC 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 Mr. Leibowitz follows:]

Testimony of
Jon Leibowitz
Co-Chairman, 21st Century Privacy Coalition
on
“FCC Overreach: Examining the Proposed Privacy Rules”
before the
House Energy & Commerce
Subcommittee on Communications and Technology
June 14, 2016

Chairman Walden, Ranking Member Eshoo, other distinguished Members of the Subcommittee, thank you for inviting me to testify at this important hearing. My name is Jon Leibowitz and, along with former Representative Mary Bono, I serve as co-chair of the 21st Century Privacy Coalition.

Our group is comprised of the nation's leading communications companies, which have a strong interest in bolstering consumers' trust in online services and confidence in the privacy and security of their personal information. We believe that consumers should enjoy the same robust protections throughout the internet ecosystem. I offer testimony today regarding the FCC's ongoing broadband privacy rulemaking on behalf of our group.

As consumers' online activity grows in size and scope, it is more important than ever for internet companies to protect us against hackers and disclose how they use our personal data. Since the internet's inception, the Federal Trade Commission ("FTC") has been the main privacy cop enforcing these essential consumer protections. But last year, the FTC's sister agency—the Federal Communications Commission ("FCC")—reclassified Internet Service Providers ("ISPs") as common carriers subject to Title II of the Communications Act, removing ISPs from the FTC's jurisdiction. Having assumed sole jurisdiction to protect consumer privacy in the ISP market, the FCC is currently engaged in a rulemaking to set out a privacy framework for ISPs.

The 21st Century Privacy Coalition was encouraged by FCC Chairman Wheeler's stated aim to craft the proposed broadband privacy rules in a manner "consistent with [the] FTC's thoughtful, rational approach," and with the core principles of the 2012 FTC Privacy Report: privacy-by-design, choice, and transparency. Our group believes that an FCC rulemaking consistent with the FTC's privacy framework would ensure that privacy enforcement remains both robust and technology neutral—that is, based on the sensitivity of data collected and how that data is used, rather than on the type of entity collecting the data.

Unfortunately, while some parts of the FCC's proposed rules are consistent with the FTC approach, in many important areas, the rules deviate sharply from that approach. The FCC has proposed regulations for broadband providers that go well beyond those imposed upon the rest of the internet economy, and which, if adopted, would undercut benefits to the very consumers such rules seek to protect. Yet the FCC has failed to identify any harms or particular problems posed by ISPs that necessitate a divergence from the effective privacy framework that has applied to ISPs for years.

The FCC's proposed rules do not reflect the economic and technological realities of the internet ecosystem, in which myriad entities have access to and use consumers' online information to provide advertising-supported content and services and a wide array of customized capabilities and offerings. Data-driven insights and offerings are a key driver of the growth of the internet economy and the source of considerable innovation and benefits for consumers, but the FCC's proposed rules will make it much harder for ISPs to deliver these benefits, particularly compared to other online entities.

In fact, ISPs are new entrants in the online advertising market, where ten companies hold seventy percent of the market. The proposed rules would curtail ISPs' ability to enter that market and provide sorely needed competition.

The proposed rules also threaten to create not only consumer confusion, but also frustration and disruption of their online experiences. And, as a recent survey from the Progressive Policy Institute demonstrates, consumers overwhelmingly agree that "[a]ll companies collecting data online should follow the same consumer privacy rules so that consumers can be assured that their personal data is protected regardless of the company that collects or uses it." In addition, because the United States has highlighted the FTC's approach to privacy in its negotiations with the European Union regarding cross-border data transfers, including the so-called Privacy Shield, there are concerns on both sides of the Atlantic that FCC divergence from the FTC privacy framework could undermine the Privacy Shield in the European Court of Justice as well as other US international privacy negotiations.

A truly consistent approach is critical to the continued growth of the internet, to avoiding consumer confusion and misunderstanding regarding the uses of their data, as well as to permitting innovation to continue to flourish. The FCC's approach, as currently drafted, fails to achieve these goals.

The FTC Approach

Privacy has long been a cornerstone of the FTC's consumer protection mission, and all of us who worked at the FTC are proud of the work we did to both protect consumer privacy and ensure that consumers continue to benefit from the high-tech innovation and competition that has revolutionized modern life. As consumers continue to migrate more and more of their lives online, the FTC has worked to ensure both that consumer privacy is safeguarded while providing companies with the flexibility to use data in ways that benefit consumers and foster competition and innovation.

The FTC has a proven track record of success, built on robust enforcement, including over 400 successful privacy enforcement actions; occasional regulation such as the initial 1999 and subsequent 2010 rulemakings on the Children's Online Privacy Protection Act; and thoughtful policy initiatives like the 2012 Privacy Report, "Protecting Consumer Privacy in an Era of Rapid Change," a multi-year endeavor that incorporated the findings of iterative policy workshops beginning in 2006, a draft Privacy Report in 2010, and over 450 comments from consumer and industry advocates, technology and policy experts, and the public. Indeed, when the FTC published its comprehensive Privacy Report in 2012, its approach received praise from many consumer and privacy groups and some criticism from businesses. For example, the privacy organization Electronic Frontier Foundation praised the FTC for "creat[ing] strong guidelines for protecting consumer privacy choices," while the Information Technology and Innovation Foundation criticized the FTC, raising concern about "important trade-offs and costs" associated with the FTC framework.

In the four years since the publication of the Privacy Report, in which there have been continued developments in the way consumers access and use the internet itself, the FTC has held more workshops and issued additional reports and guidance tailored to specific sectors, technologies and practices to account for changes in the services offered over the internet, and in the data collection and tracking technologies used by various entities within the internet ecosystem. Despite these changes, the framework established in 2012 and the principles within the framework not only remain the same, but are even more resonant.

The 2012 Privacy Report presents a single, comprehensive framework that companies should consider and implement when collecting, using, and maintaining consumer data. These principles are:

- 1) *Privacy by Design*: calling on companies to provide reasonable security for consumer data, to limit the collection of consumer data to what is consistent in a context of a particular transaction, to implement reasonable data retention and disposal policies, and to maintain reasonable accuracy of consumer data;
- 2) *Consumer Choice*: encouraging companies to offer consumers the ability to make decisions about the collection and use of their personal data in a timely and contextual manner; and
- 3) *Transparency*: encouraging companies to increase the transparency of their information collection and use practices through easily-readable privacy statements and consumer education.

The FTC furthers these principles through robust enforcement rather than prescriptive regulation. It goes after companies when they break their privacy commitments to consumers or take actions that cause consumers real harm. This approach is flexible and promotes high-tech innovation, and it has held hundreds of companies, large and small, accountable when they cause real harm to consumers without countervailing benefits to consumers or competition.

Importantly, in addition to creating a comprehensive framework for both online and offline data collection and use, the FTC Report highlighted the importance of a technology-neutral approach to privacy: “Any privacy framework should be technology neutral.” In other words, privacy enforcement should not depend upon the type of company using or collecting consumer data or the particular technology being used to do so. Indeed, the FTC specifically examined the question of whether large platform providers – a category that includes, but is not limited to, ISPs – should be subject to more stringent privacy obligations and, after a comprehensive inquiry, declined to take such a step. Instead, the FTC framework focuses on the sensitivity of the data collected and how those data are used. Consistent application of the principles is designed to provide consumers with clear and uniform privacy and data security protections, regardless of the particular product or service being used. The Administration has supported the FTC’s policy of technology neutrality for privacy and the goal of a harmonized privacy framework for the entire internet ecosystem.

Finally, it is worth noting that the comments the FTC filed last week in the FCC's privacy proceeding, based on its 2012 Privacy Report, were unanimously supported by all three sitting commissioners. There is more legitimacy, and more enduring impact, from bipartisan regulatory action.

The FCC's Proposed Rules

The FCC's stated principles of transparency, consumer choice, and data security are framed as matching the principles at the heart of the FTC's framework and other privacy regimes in the United States and globally. Certain specific proposals in the NPRM are also consistent with the FTC approach. For example, the proposal for broadband providers to take reasonable measures to protect customer data is similar to FTC guidance and enforcement. The FCC's goal of standardizing the delivery of broadband privacy notices echoes goals set by the FTC. Likewise, the FCC's call for notice and consent to consumers of retroactive material changes to data collection and use is consistent with the FTC's framework and enforcement.

But, as the FTC staff noted in its comments last month on the FCC's proposal, which was approved by a unanimous, bi-partisan vote of the Commissioners, "the FCC's proposed rules, if implemented, would impose a number of specific requirements on the provision of [broadband] services that would not generally apply to other services that collect and use significant amounts of consumer data. This is not optimal."

In effect, the FCC proposal amounts to a *de facto* rejection of the FTC's determination that ISPs should not and need not be governed by a different set of standards with regard to how they handle broadband customer data. Instead, the FCC's proposed rules require a broad default opt-in requirement for the use and sharing of customer data, with limited exceptions, rather than narrowly tailoring its opt-in to the collection and use of sensitive customer data. The FCC is also much more restrictive with regard to first-party uses of information, which enable companies to improve their service and apprise their customers of offers and products of interest to them.

The breadth of data covered by the proposal, and the highly restrictive nature of the permissions regime employed by the FCC, creates a serious risk of unforeseen consequences that could adversely affect Internet capabilities and operations and disrupt consumer expectations. During the development of the 2012 Privacy Report, FTC staff addressed the potential impact of various proposals and ideas through extensive "stress testing," whereby staff held scores of meetings with industry and consumer groups alike to test particular components in order to determine whether the desired outcome would be achieved. The FCC should conduct similar meetings to fully understand the effects of its proposed requirements, which have the potential to disrupt not only the broadband industry, but the entire internet ecosystem, including competition in the online advertising market. What follows is a discussion of specific differences between the FCC proposed rules and the FTC approach.

Scope

The FCC's Notice of Proposed Rulemaking ("NPRM") applies onerous privacy and security requirements to sweeping a range of information that is not sensitive, such as IP or MAC addresses, as well as any other information that is "linked or linkable to" a user. This differs from the FTC approach, which sought to calibrate the framework's obligations to incentivize the strongest protections for the most sensitive data.

The FCC's treatment of de-identified data is particularly problematic. Because de-identified data does not present a risk to consumer privacy or security, the FTC framework does not govern the notice, use, disclosure, security, or notification of breach of anonymized or de-identified individual data, as long as such data cannot be reasonably linked to a particular consumer, computer, or device. The FCC's proposal appears to confuse the FTC's guidance on the "reasonable linkability" standard and the appropriate steps companies can take to minimize such linkability with a standard for aggregation, which is but one way to de-identify data. The NPRM would limit the exception for de-identified data only to data that is *both aggregated and de-identified*. By discouraging companies from investing in resources and tools to de-identify data, the FCC's proposal actually exacerbates – rather than mitigates – risks to consumer privacy.

Application

As noted above, in the 2012 Report, the FTC stated: "[A]ny privacy framework should be technologically neutral." There is widespread agreement on this point among consumer and industry advocates alike. At the FTC's December 2012 workshop, "The Big Picture: Comprehensive Online Data Collection," Maneesha Mithal, Associate Director of the Privacy Division at the FTC noted this consensus in her closing remarks, describing "the need for tech neutrality" as an area of consensus and emphasizing that "[w]e can't be picking winners and losers in this space."

Moreover, since 2012, the precipitous rise of encryption and the proliferation of networks and devices have limited the scope of customer data available to broadband providers, while other companies operating online have gained broader access to consumer data across multiple contexts and platforms. For example, today, nearly half of Internet traffic is encrypted, dramatically limiting the information visible to ISPs, and an estimated 70% will be encrypted by the end of this year. This sea change in only four years' time drives home the importance of technology neutral privacy frameworks. Because the FCC is not in a position to dictate privacy rules for the entire Internet ecosystem, it should strive to harmonize its proposed rules with the FTC framework, and carefully consider the consequences of failing to do so.

Choice and Context

In its comments, FTC staff leveled criticism at the FCC's proposed consumer choice rules and recommended "that the FCC consider the FTC's longstanding approach, which calls for the level of choice to be tied to the sensitivity of data and the highly personalized nature of consumers' communications in determining the best way to

protect consumers.” The FCC’s proposed restrictive choice mandates that selectively target broadband providers prevent consumers from accessing new products and services and provide them no benefits, as well as potentially confuse them. They also, constrain ISPs’ ability to compete with edge providers, and may discourage broadband investment in a manner contrary to the FCC’s mandate to promote such investment.

Under the FTC framework, when a consumer does business with a company, there are certain uses of the consumer’s information by the company for which consumer choice is implied because such use is consistent with “the context of interaction between a business and the consumer.” This implied consent covers uses and disclosures for product or service fulfillment, internal operations, most first-party marketing, and more. Opt-in consent is limited to truly “sensitive data” and technologies that use “all or substantially all” customer data. The FTC framework calls for a consumer opt-out for almost all online tracking, not an opt-in. The FCC proposal is a vast departure from this guidance.

Rather than narrowly tailoring a requirement for opt-in consent to truly “sensitive data,” the proposed rules would impose a broad opt-in requirement upon broadband providers for the use or disclosure of a wide swath of consumer data for an extensive range of practices – including practices for which the FTC requires no choice at all because consent is implied. In doing so, the FCC’s proposed rules disregard the context of the interaction between the consumer and the service provider. In today’s economy, a company’s relationship with its customers involves more than just providing service, but also requires understanding the ways in which services are used, identifying areas for improvement, and making consumers aware of product offers and enhancements that may interest them. By ignoring the balance between privacy and data-driven insights and innovation, the FCC’s approach actually makes consumers worse off.

The FTC does not require companies to provide any choice to present advertising to their own customers, except where that advertising was presented by tracking a user’s online activity across other companies’ websites or intentionally using sensitive information collected from its customers. Under the FCC’s proposal, however, any use of customer information that is not relevant to marketing a communications-related service would require opt-in consent from the customer. Indeed, under one reasonable reading of the proposed rules, a broadband provider would not be able to market its own non-communication-related products—like a home security system, cloud services, or music streaming—to its own customers without their prior opt-in consent, regardless of the marketing channel used and despite the fact that this type of first-party marketing is certainly consistent with consumer expectations.

The FCC’s overbroad opt-in proposal has the potential to stifle innovation and competition in the online advertising marketplace and undermine benefits to consumers. As the FTC has recognized, the ability to effectively monetize online data has yielded astounding benefits to consumers. Consistent with the FTC’s technology-neutral approach, broadband providers should be able to use information in a manner consistent with consumer expectations and in a way that correlates to how the rest of the internet ecosystem provides choice. Requiring over-inclusive opt-in choice would unduly restrict

broadband providers from participating in the same internet marketplace the FTC has found to provide benefits to both consumers and competition.

The FCC's NPRM also departs fundamentally from FTC guidance and questions the core principle of customer notice and choice by suggesting that it could be appropriate to prohibit broadband providers from offering discounted services in exchange for greater access to consumer data. Many of us may decide that the price to pay to avoid personalized advertising is worthwhile, and so long as broadband providers provide sufficient information to enable an informed choice, consumers should be able to choose for themselves how to value privacy.

The application of a broad opt-in for non-sensitive information as proposed by the FCC would create an isolated privacy regime for ISPs that bears little correlation with consumer data practices used in virtually every other sector. Deviating from the FTC's privacy framework overall, but especially from the FTC's emphasis on determining consumer choices based upon the sensitivity of the information, the context of a consumer's interaction with a company, and the consumer's expectations, will inevitably result in consumer confusion over illogical, disparate standards applied to the same set of data. Ultimately, while the FCC Privacy NPRM purports to be based significantly on the FTC privacy framework, it is far more restrictive in all of the above respects, without providing clear benefits to consumers.

Data Security and Breach Notification

The FCC's proposed data security provisions, requiring broadband providers to take reasonable measures to protect customer data, are consistent at a high level with the approach set out in the FTC Report. However, their prescriptive and static nature are at direct odds with the Administration's Cybersecurity Framework, which has been voluntarily adopted by a wide swath of industry and reflects flexible and reasonable standards that emphasize business-driven responses and solutions to cyber threats over prescriptive regulatory measures. In addition, these requirements should be more narrowly tailored to apply to customer information that carries a risk of harm in the event of a breach.

The proposed FCC breach notification rules would require broadband providers to notify consumers of a breach of a very broad new definition of "customer proprietary information," much of which includes categories of data that do not pose a risk of harm to customers in the event of a breach, such as IP and MAC addresses and de-identified data. While the concept of breach notification is consistent with the approach the FTC and most states have taken, the proposed implementation by the FCC for innocuous data and to notify only ten days after discovery of the breach is very different and far more cumbersome.

The FTC has long supported requirements for companies to notify consumers of security breaches in appropriate circumstances, such as when information has been compromised that can lead to harms such as financial loss or identity theft. The FTC has advocated that "any trigger for providing notification should be sufficiently balanced so

that consumers can take steps to protect themselves when their data is at risk, while avoiding over-notification, which may confuse consumers or cause them to ignore the notices they receive.”

The proposed rules, as currently drafted, would mandate over-notification. As the FTC staff notes in its comments on the proposed rule, the FCC should limit its notification requirement to a “narrower subset of personal information than ‘customer proprietary information’” as the FCC has proposed that term to be defined in order to avoid over-notification to consumers. As the FTC staff asserts, “when consumers receive ‘a barrage of notices’ they could ‘become numb to such notices, so that they may fail to spot or mitigate the risks being communicated to them.’” That is an outcome that the NPRM states that the FCC intends to avoid, but major changes are required to the breach notification provision to achieve this goal.

The proposed rules also contain an unrealistic timeline for customer notification. The FTC’s Health Breach Notification Rule requires companies to notify affected consumers “without unreasonable delay” and within 60 calendar days after the breach is discovered. Under the most restrictive time requirements among the general state breach notification laws – there is currently a patchwork of 47 state laws – an entity is required to provide notice “as expeditiously as practicable and without unreasonable delay but no later than 30 days after determination of breach, consistent with time necessary to determine scope of the breach, identify individuals affected, and restore the reasonable integrity of the system,” and with a 15-day extension granted for “good cause shown.” The FTC staff comments suggest an outer limit of between 30 and 60 days, which it views as “adequate for companies while protecting consumers.” When finalizing its breach notification rules, the FCC should take these realities into consideration.

Conclusion

Mr. Chairman, thank you for holding this hearing today. Our Coalition commends you for devoting the Subcommittee’s attention to this critically important issue. It is through the exercise of your crucial oversight authority that Congress can right the course of agency rulemakings that have veered away from mainstream policy goals.

As the FCC formalizes its privacy and data security rules, the agency should hold broadband providers to the same robust privacy standards to which the FTC successfully held them for many years—and to which the FTC still holds the rest of the internet ecosystem.

A truly consistent approach will ensure a comprehensive, technology-neutral privacy framework that provides consumers the strong protections and choices they need and deserve, while reducing consumer confusion regarding what protections apply. At the same time, a consistent approach will promote the types of competition and innovation that fuel our economy. Such an approach will also demonstrate that the United States views the FTC approach to privacy as the preeminent model for consumer

protection, which will help provide confidence to our trading partners that their own consumers will enjoy robust privacy protections under U.S. law.

As someone who was involved in more than a handful of rulemakings, it is important to point out that final rules are often more balanced than proposed ones. But the FCC's current proposal fails to achieve its own goals. Instead, it would create inconsistent standards across the internet, harm and confuse consumers, and undermine innovation. 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.

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 DC 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 222 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 service 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 Web sites, 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 Web sites are still unencrypted including many, many, many of the most popular ones. But even for encrypted Web sites, although the view of an ISP is partially obscured, there is plenty that they can see. They can basically compile a list of the domain name of every Web site 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 help 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.

OK, 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 deserves 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 on-line 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 Mr. Ohm follows:]

Statement of Paul Ohm
Professor, Georgetown University Law Center and
Faculty Director, Georgetown Center on Privacy and Technology

Before the
Subcommittee on Communications and Technology
Committee on Energy and Commerce
U.S. House of Representatives
June 14, 2016

Chairman Walden, Ranking Member Eshoo, and other Members of the Subcommittee, I appreciate the opportunity to discuss with you today the Federal Communications Commission's (FCC) proposal to protect the privacy of the customers of broadband Internet access service (BIAS).

I am a Professor of Law at the Georgetown University Law Center and a Faculty Director of the Center on Privacy and Technology at Georgetown. I have researched, written, and lectured extensively on information privacy, computer crime, and technology and the law. I make these comments to you today in my independent, academic capacity.

In 1996, Congress enacted section 222 of the Telecommunications Act of 1996, delegating to the FCC the power and obligation to promulgate rules to protect the information held by telephone companies and other telecommunications providers covered by Title II of the Act. Under this clear statutory authority, the FCC has proposed new rules requiring BIAS providers to respect and protect the privacy of their customers, in the wake of the agency's decision to reclassify these providers into Title II.

The FCC has acted appropriately and wisely. Rather than dissect the proposed rules, I will focus on how the application of section 222 to these providers represents not only a straightforward application of the law but also a laudable exercise of privacy theory and policy. I support these conclusions not only through my work¹ and the work of other scholars, but also by leveraging the experience I have gained as a former Senior Policy Advisor to the Federal Trade Commission (FTC) on privacy issues, Department of Justice computer crimes prosecutor, and professional network systems administrator.

In this testimony, I make four points:

- Section 1: The Telecommunications Act of 1996 obligates BIAS providers to serve as important gatekeepers of privacy, a sensible choice then and now,

¹ This testimony builds on several articles I have written on information privacy, most notably on Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417 (2009). A full list of my published works is available online at <http://paulohm.com/scholarship.shtml>.

one that continues to protect important values in today's online environment.

- Section 2: When Congress recognizes the need for sectoral privacy rules, as it has with this law, it is well-advised to create rules that draw bright and easily administrable lines rather than utilize murky balancing tests, in order to protect consumer expectations and engender consumer trust.
- Section 3: The proposed FCC rules create and preserve an important level playing field for information. Importantly, BIAS providers retain the ability to compete directly with search engines and other providers of edge services subject to precisely the same privacy law framework as any other company.
- Section 4: There is great need to strengthen privacy rules for online actors other than BIAS providers. To this end, the FTC does not have all of the authority or resources required to solve all online privacy problems.

1 THE STATUTE TREATS BIAS PROVIDERS AS GATEKEEPERS OF INDIVIDUAL PRIVACY

Our federal laws protect privacy on a sector-by-sector basis and in piecemeal. The FTC Act provides an essential backstop across many industries, but there are limits to its approach, as I will discuss later. In narrowly circumscribed contexts, Congress has seen fit to create heightened privacy obligations. HIPAA protects the privacy of some health information, FERPA does the same for some education records, and the Fair Credit Reporting Act protects some credit reports, to name only three examples. In the same way, Congress reaffirmed in the Telecommunications Act of 1996 (1996 Act) that certain telecommunications providers would be subject to heightened privacy obligations. This was a measured and appropriate choice at the time, and it remains even more so today, even in light of reclassification.

There are four reasons why it is essential to provide heightened protection for the privacy of information gathered by the companies that serve as our gatekeepers to the rest of the Internet: history, choice, visibility, and sensitivity. Each of these reasons contributes an answer to the question: why was Congress correct to require communications gatekeepers to respect the privacy of their customers? Let me elaborate each of these reasons in turn.

1.1 HISTORY

The first reason to subject BIAS providers to special privacy rules is history. Since the dawn of intermediated communications, we have almost always required our common carriers to respect the privacy of what they have carried. It was so for the postal service in the nineteenth century, the telephone service early in the twentieth century, and parcel delivery services in the modern age. Time, experience, and theory demonstrate why we must enact laws to create the conditions that allow people to have faith in the privacy, security, and confidentiality of the information and goods they entrust to intermediaries like these.

Congress enacted privacy protections in the original Communications Act of 1934 and restated and perhaps even broadened those protections in the 1996 Act. We are not working from a legal blank slate. Too much of the commentary around the FCC rules ignores the—perhaps inconvenient for some—fact that Congress has spoken quite clearly on this matter. The law protects what it protects, and the burden should be on those who would rewrite the statute, not on the agency that implements it.

1.2 CHOICE

It is also appropriate for Congress to protect the privacy of information sent through a BIAS provider because of the relative lack of choice consumers enjoy for BIAS services. Today, most people in the United States have only a single broadband Internet service provider to choose from.² Even when there is a nominal choice, high switching costs in the form of time, effort, hassle, and contractual lock-in make it difficult for a privacy-sensitive consumer to change providers in search of a more privacy-respecting alternative.

1.3 VISIBILITY

Every BIAS provider sits at a privileged place in the network, the bottleneck between the customer and the rest of the Internet. This favorable position gives it a unique vantage point, from which it enjoys the ability to see at least part of every single packet sent to and received from the rest of the Internet.

No other entity on the Internet possesses the same ability to see. If you are a habitual user of the Google search engine, Google can watch you while you search, and it can follow you on the first step you take away from the search engine. After that, it loses sight of you, unless you happen to visit other websites or use apps or services that share information with Google. If you are a habitual Amazon shopper, Amazon can watch you browse and purchase products, but it loses sight of you as soon as you shop with a competitor. Habitual Facebook users are watched by the company when they visit Facebook or use websites, apps or services that share information with Facebook, but they are invisible to Facebook at all other times.

When users interact with websites or use apps or devices that do not support encryption or do not enable it by default, a BIAS provider's ability to spy is complete and comprehensive. While it is true that BIAS providers can view less about its users' visits to websites that deploy encryption, it is a regrettable fact that millions of websites, including many of the most popular ones, still do not enable encryption by default.³

² FCC 2016 Broadband Progress Report (“Approximately 51 percent of Americans have one option for a provider of 25 Mbps/3 Mbps fixed broadband service.”).

³ Upturn, What ISPs Can See: Clarifying the Technical Landscape of the Broadband Privacy Debate, March 2016, <https://www.teamupturn.com/reports/2016/what-isps-can-see> (reporting that

Even for user visits to websites that deploy encryption, a BIAS provider retains a significant ability to observe. When you visit a website protected by the most widespread form of encryption in use, https or http over TLS, even though your BIAS provider cannot tell which individual page you are visiting on the website, it still can tell the domain name of the website you are communicating with, how often you return, roughly how much data you send and receive, and for how long each visit lasts.

Compare the richness of this information to the information a telephone company can see, which although subjected to the heightened protection of Title II, is relatively limited by comparison. In the 1996 Act, Congress decided to impose significant limits on what telephone companies could do with the list of numbers an individual customer dials. This made good sense because even though this list did not literally expose the contents of communications, it nevertheless testified to something very private, individual, and important about our habits and associations. The list of websites visited by an individual (including how often and how long she visits each site) is even more private, individual, and sensitive than those older lists of telephone contacts.

Some commenters who would prefer to place the burden of privacy protection on individual consumers, point to the availability of more complete forms of end-user encryption, such as Virtual Private Networks (VPNs). This is a specious argument. VPNs require additional technical overhead for the end user's computer, generally resulting in a slower, far less tolerable Internet experience. Although some VPNs offer their services for free, these free services typically offer poor performance, and are sometimes subsidized by even more surveillance to fuel even more advertising. To enjoy a tolerable and private VPN, most consumers need to pay for the privilege or have it provided by an employer. Treating a VPN as a bastion of privacy from BIAS providers, in other words, means that the only people in society who can access this level of privacy are those with means and knowledge. This argument relegates everybody else to second-class status, allocating privacy across society according to other pre-existing advantages.⁴

1.4 SENSITIVITY

Perhaps the most important reason to protect the information a BIAS provider can obtain is the intrinsic sensitivity of this information.⁵ A BIAS provider can gather at least three types of information we have long deemed sensitive: communications, reading habits, and location.

more than 85% of popular sites in health, news, and shopping categories do not encrypt browsing by default).

⁴ In addition, VPNs make it difficult for copyright owners to police their copyrights and for law enforcement to conduct lawfully authorized surveillance.

⁵ See Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125 (2015) (providing a detailed review of the use in privacy laws of the concept of sensitive information).

Our legal system has long recognized the sensitivity of our communications. Under the Fourth Amendment, almost nothing receives the heightened protection for privacy given to the content of our conversations. Federal and state statutes vigorously protect both the content of and the metadata associated with communications. We reveal intimate portraits of ourselves through what we say to our friends, family, and associates. A BIAS provider can readily access the content and metadata of communications, particularly sent across unencrypted services.

A BIAS provider can also build a fairly complete dossier of our reading habits across time. The list of websites an individual visits, available to a BIAS provider even when https encryption is used, reveals so much more than a member of a prior generation would have revealed in a composite list of every book she had checked out, every newspaper and magazine she had subscribed to, every theater she had visited, every television channel she had clicked to, and every bulletin, leaflet, and handout she had read. No power in the technological history of our nation has been able until now to watch us read individual articles, calculate how long we linger on a given page, and reconstruct the entire intellectual history of what we read and watch on a minute-by-minute, individual-by-individual basis.

Professor Neil Richards describes the right we should enjoy to “intellectual privacy.”⁶ He argues that the law ought to protect vigorously the record of what we read and write. His writing supplies a powerful and well-reasoned justification for treating BIAS providers precisely as the 1996 Act does.

Finally, with the rise of mobile broadband, BIAS providers now also track our location across time in a finely granular manner. Never before in human history has anybody compiled such a complete accounting of the precise comings-and-goings of so many of us.

So much of us can be revealed to a company that compiles a finely wrought accounting of where we have traveled, what we have read, with whom we have engaged, and what we have said. BIAS providers might respond that they want this information only to reduce us into marketing categories to sell and resell. I derive no comfort from that justification.

2 THE NEED FOR BRIGHT LINES

When Congress decides that a particular use of information or class of information—be it health information, student records, credit reports, or telecommunications records—justify a sectoral privacy law, the question next becomes, what form should that law take? Congress has often chosen to protect such contexts using relatively simple, easy-to-apply, bright lines rather than murky standards or balancing tests. Section 222 draws such a bright line, and the FCC is wise in its proposed rule to adhere to it with an opt-in rule for a broad class of information and uses, rather than turn to a more indeterminate alternative.

⁶ NEIL RICHARDS, *INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE* (2015).

The FCC should thus resist calls to alter its new rule to require opt-in consent only for uses of sensitive information, such as Social Security Numbers or medical diagnoses. This argument deeply misunderstands the way privacy laws have handled and should handle the trade-offs between sensitivity, trust, and administrability.

It is true that statutory bright lines sometimes protect nonsensitive information together with sensitive information. Statutes like HIPAA, FERPA, and the Wiretap Act sweep broadly and categorically, assuming that the default state of a particular category of information should be protected, then allowing for limited exceptions, for example, for individual consent, provider protection, or to respond to emergencies.

We protect information categorically in this way for at least two reasons. First, bright lines support a relationship of trust between provider and individual. We value the fact that everything we say to our doctor—the sensitive and the banal—is protected vigorously by default. This bright line helps foster a trusting relationship with our health care provider, liberating us from second guessing whether our doctor is trying to segregate out the nonsensitive information we tell her to sell to pharmaceutical manufacturers or advertisers. Likewise, section 222's bright line fosters trust in those who provide us access to essential communications networks.

Bright lines are valuable also because the alternative would be an administrative nightmare: an inefficient, and ineffective process of adjudicating every piece of information across an difficult-to-define spectrum of sensitivity. To follow the logic of these arguments, doctors would parse the sensitive from the nonsensitive in hospital records, creating a patchwork of privacy protection that no doubt would vary from doctor to doctor and patient to patient. Voice wiretaps would be legal without consent, so long as what was intercepted was deemed later to have been nonsensitive. The information in credit reports would be sliced and diced according to perceptions of sensitivity, with the nonsensitive portions falling outside legal protection. Allowing BIAS providers to treat sensitive and nonsensitive information differently would greatly increase compliance complexity and costs, costs that would likely be passed along as higher prices for consumers.

Rather than go down that uncertain road, we have decided that some categories of information or activity—health records, education records, credit records, or telephone conversations—are so intrinsically sensitive, we protect them categorically. This is what Congress did in the 1996 Act, and this is what justifies—as matters of both statutory and First Amendment law—applying the categorical rule, as the FCC has done in its proposal, to all customer proprietary information.

3 THE LEVEL PLAYING FIELD

The FCC's reclassification and proposed rules serve an important additional goal: they level the privacy playing field for entities that used to be subject to different rules. Until reclassification, providers of telephone service had been subject to section 222 rules while providers of Internet service had not. Often, the very same companies provided both types of services and were forced to live under very different rules.

Reclassification brings us a step closer to harmonization, and companies affected by the new rules will no doubt enjoy new efficiencies from being able to apply similar privacy rules for the different services they offer.

The new rules also do nothing to disrupt an important level playing field between BIAS providers and providers of other online services. Nothing in the law or proposed rules prevents a broadband Internet provider from entering into direct competition with search engines or other edge providers. A broadband Internet provider that launches a search engine will be able to use the information it takes from its search engine customers in the relatively unrestricted manner the law currently provides for that industry.

Likewise, if a search engine company decides to create a broadband Internet service (say a subsidiary that provides residential fiber optic service), it will fall within Title II of the Communications Act and thus be subject to the FCC's new rules. In either case, the two competing companies will be subjected to precisely the same rules under precisely the same terms.

By properly understanding the level playing field the rules preserve, we can unmask another commonly heard argument for what it really is. Some have complained that the FCC's proposed rules would unfairly distinguish or discriminate between the privacy law obligations imposed on different types of online providers. These complaints deserve little attention. What BIAS providers truly mean when they complain about unfair or discriminatory treatment is that a particular privacy law to which they are subject—section 222 of the Communications Act—protects privacy too much. This is a direct substantive critique of an act of Congress, one which should be lodged and addressed directly on its own terms, rather than dressed up in the obscuring language of fairness and discrimination. The idea that the FCC is acting discriminatorily or unfairly is a feint and a disingenuous distraction.

4 THE NEED TO ENHANCE PRIVACY IN OTHER CONTEXTS

Of course, the FCC's new privacy rule will not solve all of the privacy problems we face. Many of the arguments against the FCC's new rule lead us to understand that we need to raise our privacy standards across other parts of online ecosystem as well. On this point, we all can agree. We ought to increase the resources we provide to the FTC and enhance its power to police deceptive and unfair privacy practices. We also ought also to consider imposing new and more stringent rules for industries that are striving to develop the kind of pan-Internet view that BIAS providers structurally enjoy or that handle vast amounts of sensitive information, as BIAS providers do.

4.1 THE FTC CANNOT GO IT ALONE

In 2014, not long after completing my service to the FTC, I testified to the Subcommittee on Commerce, Manufacturing and Trade about the great successes of the FTC's mission to protect consumer privacy. I continue to feel today what I

expressed then, that the FTC has become a great bulwark of privacy in a tumultuous time of change. But the FTC simply cannot go it alone. There are significant limits to what the FTC can do to protect privacy. We should view the FTC as the irreducible floor of online privacy protection, and we should do what we can to give the FTC additional resources to raise that floor.

But the rise of the FTC as a capable and well-respected privacy regulator does not mean we should dismantle sectoral privacy regulation. The FTC's jurisdiction and enforcement activity cannot supplant the Department of Health and Human Service's role under HIPAA, the Department of Education's role under FERPA, or the Consumer Financial Protection Bureau's role under numerous financial privacy laws. Likewise, the fact that the FTC has been very active and successful policing privacy online does not mean we should discourage the FCC from protecting privacy under section 222 using its distinctive approaches and capabilities.

For all of the amazing strides the FTC has taken to become an expert in online data collection, the FCC has had a much longer time to develop expertise in the protection of network access subscribers. With this head start, the FCC has unparalleled experience ensuring that the nation's communications networks function in a way that is reliable and trustworthy and crafting regulations that promote the buildout of networks. Nobody has more experience and staff expertise on these matters than the FCC.

Moreover, the FCC's clear statutory mandate in Section 222 is specific and proactive, in contrast to the FTC's mandate in Section 5 of the FTC Act, which is far more general and reactive. I have already explained why the proactive approach is necessary and well-justified for BIAS providers. Fortunately, these two mandates work together, with the FCC's proposed rule giving BIAS providers an unambiguous roadmap for their future enforcement activities. It is also to the credit of the staff of these two agencies that they have entered into a Memorandum of Understanding committing to work together in their common privacy endeavors.

4.2 THE NEED TO STRENGTHEN OUR PRIVACY LAWS

As I have argued above, it is a combination of history, choice, visibility, and sensitivity that justify subjecting BIAS providers to the same kind of special privacy rules we have enacted for doctors, schools, credit agencies, and other industries. A sectoral approach to privacy law continues to be a desirable approach.

It is true that other online entities are beginning to rival BIAS providers on at least some of these critical dimensions.⁷ Other entities traffic in location information, a category Congress ought to consider protecting as especially sensitive. Social networking sites carry exceptionally sensitive information and they exhibit network effects and insufficient data portability that limit customer choice and exit. Finally, advertising networks strive to attain a BIAS-provider-like visibility across the Internet.

⁷ Peter Swire, et al., *Online Privacy and ISPs*, Alston & Bird LLP (May 2016) [*hereinafter* *Broadband for America Report*].

Congress should examine whether any other industry has implicated individual privacy along these dimensions so much that they have begun to rival doctors, schools, credit agencies, or BIAS providers. But once it identifies such an example, the answer will not be to decrease privacy law across industries, the answer will be to enact another new, measured and narrow sectoral privacy law, one which draws bright lines.

5 CONCLUSION

Given the deep concern many of your constituents feel about their lack of control of information about them; given the calls and emails you no doubt receive after every significant data breach or other privacy debacle; given the survey after survey which bear witness to the breadth and depth of concern American citizens have about this state of affairs; and given the critical importance of an Internet we can trust for commerce, communications, and innovation, this is an extremely ill-advised time to roll back one of the very few privacy protections we have for online activity. We should be strengthening not weakening the privacy of online activity. We owe our thanks to the Federal Communications Commission for taking a modest, sensible, and legally authorized step toward enhancing the protection we enjoy.

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 reason 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 Mr. Brake follows:]



**Testimony of
Doug Brake
Telecommunications Policy Analyst
Information Technology and Innovation Foundation**

**Before the
House Committee on Energy and Commerce
Subcommittee on Communications and Technology**

**Hearing on
“FCC Overreach: Examining the Proposed Privacy Rules”**

**June 14, 2016
2123 Rayburn House Office Building
Washington, DC**

Chairman Walden, Ranking Member Eshoo, and members of the Subcommittee, thank you for inviting me to share the views of the Information Technology and Innovation Foundation (ITIF) on the ongoing proceeding at the Federal Communications Commission (FCC) 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 reason, and others explored below, ITIF has opposed the entire FCC privacy undertaking.¹

There certainly is a role for government in protecting consumer privacy, but the oversight and enforcement provided by the Federal Trade Commission (FTC), along with existing industry practices and commitments, provide a superior framework for balancing privacy, consumer protection, and innovation. There is still time for Congress to direct the FCC to correct course.

BROADBAND PROVIDER ACCESS TO DATA DOES NOT JUSTIFY SECTOR-SPECIFIC REGULATORY SILOS

The FCC proposes strict data privacy regulations that will apply only to broadband Internet access providers.² In order to justify the FCC's sector-specific rules, one would expect an unusually high risk of consumer harm from consumer broadband data being shared inappropriately. After all, the only sector-specific privacy rules are for areas of the economy, such as healthcare or financial services, where there exists a heightened risk of harm from the disclosure of sensitive personal information. But, as a factual matter, that heightened risk does not exist with regard to broadband providers: their access to data is neither unique nor comprehensive.

In his report, *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others*, Professor Peter Swire lays out a number of ways in which broadband providers generally have less visibility into users' online activity compared to other actors in the Internet ecosystem.³ Broadband providers do not have anything near comprehensive access to consumer data for several reasons. One of the most prominent limitations on broadband providers' access to data is the growing use of encryption. When subscribers use encrypted protocols with their browsers, the broadband provider is unable to determine the content or information about the webpages that the user visits. And encryption adoption is on a sharp, recent rise: In 2014 a small percentage of traffic was encrypted, but by the end of 2016, it is estimated that 70

¹ See Doug Brake, Daniel Castro, & Alan McQuinn, ITIF, "Broadband Privacy: The Folly of Sector-Specific Regulation" (2016), <http://www2.itif.org/2016-broadband-privacy-folly.pdf>; Doug Brake, Daniel Castro, & Robert D. Atkinson, ITIF, "The FCC's Privacy Foray: Privacy Regulation Under Title II" (2015), <http://www2.itif.org/2015-fcc-privacy.pdf>; Doug Brake, "In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, Comments of ITIF," WC Docket No. 16-106, available at http://www2.itif.org/2016-broadband-privacy-comments.pdf?_ga=1.25209844.812486504.1449157248; Doug Brake, "The FCC's Privacy Ruse," *Forbes* (April, 2016), <http://www.forbes.com/sites/realspin/2016/04/27/the-fccs-privacy-ruse/#1c47825b10aa>.

² The FCC's proposed rules apply only to Broadband Internet Access Services, or "BIAS" as defined at 47 CFR § 8.2(a).

³ Peter Swire, et al, *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others*, The Institute for Information Security & Privacy, Georgia Tech, Feb 2016, <http://peterswire.net/wp-content/uploads/Online-Privacy-and-ISPs.pdf>.

percent of traffic will be encrypted.⁴ All of the top 10 websites now encrypt their traffic by default or on user log-in, and 42 of the top 50 do so as well.⁵

Broadband providers can still access high-level metadata even when consumer traffic is encrypted. For example, a broadband provider might be able to determine from metadata that a particular household is streaming video, but have no idea as to the actual content of the video. However, since encryption obscures most content, and virtually all sensitive content, the case for heightened rules applied only to broadband providers is extremely tenuous. The fact that consumers spread their Internet use over multiple broadband connections at home, work, and at various WiFi hotspots further reduces the risk of harm from any one provider's collection of information.

Privacy-sensitive consumers have additional options to protect their data if they choose. They can use virtual private networks (VPNs) to encrypt the Internet traffic a broadband provider would otherwise see. If a broadband subscriber is using a VPN, the broadband provider can see only that the subscriber accessed that VPN, not information about the user's end destination. If consumers want to use VPNs to obfuscate their online habits from their provider, they certainly can take that option.

Engineers have pointed out there is a significant gap between what information is technically available to Internet Service Providers (ISPs) and what is practically useful. Richard Bennett, a consultant with a thirty-year background in network engineering, points out that because of the numerous, diverse connections opened when a typical web page loads, "all the ISP can do with the all that information is guess what the important parts are.... As a practical matter, converting the raw information that ISPs can harvest from web requests made by users who aren't using VPNs is a very difficult task."⁶

Even given all that, provider access to data is simply not unique. As Jules Polonetsky, head of the Future of Privacy Forum, has put it, "[t]oday, data has been democratized"—large amounts of consumer data are already available to anyone with a credit card.⁷ The ability to obtain data like that which broadband providers have access to is widely available and in no way unique to broadband providers. The proposed rules would lead to the strange and market-distorting result where broadband providers would not be allowed to share or use the exact same information that is readily available to others.

Moreover, as ITIF has demonstrated, all major broadband providers already offer consumers the ability to opt-out of existing targeted advertising programs, an important and often-overlooked point.⁸ In line with the FTC's guidance, broadband providers all offer notice of the data that is collected and the option for

⁴ *Id* at 29, citing "2016 Global Internet Phenomena, Spotlight: Encrypted Internet Traffic," Sandvine, Feb. 2016.

⁵ *Id* at 28.

⁶ Richard Bennett, "FCC Confused About Privacy," *HighTech Forum*, <http://hightechforum.org/fcc-confused-about-privacy/>.

⁷ Jules Polonetsky, "Broadband Privacy and the FCC: Protect Consumers from Being Deceived and from Unfair Practices," *Future of Privacy Forum* (March 2016), <https://fpf.org/2016/03/11/13938/>.

⁸ See Doug Brake, Daniel Castro, & Alan McQuinn, Information Technology and Innovation Foundation, Broadband Privacy: The Folly of Sector-Specific Regulation, (2016), <http://www2.itif.org/2016-broadband-privacy-folly.pdf>.

consumers to opt out of practices they are uncomfortable with. The truth is users will have no more and no less “control” over how companies use their broadband data under the proposed rules, as the FCC has asserted. What will change, however, is the ability of ISPs to responsibly experiment with new ways of supporting the expensive deployment and maintenance of broadband networks.

In addition, persistent confusion stems from the popular, but mistaken, belief that because broadband providers operate the network connecting users to the rest of the Internet—the actual location of broadband providers as in the middle between users and the online services they access—these providers have a special relationship with consumers’ online activities. But this “gatekeeper” model is the wrong way to think about broadband providers’ relationship to consumer data. As the FTC explained in its 2012 Privacy Guidelines, although ISPs serve as intermediaries, giving consumers access to other services, “[a]t the same time, the Commission agrees that any privacy framework should be technology neutral. ISPs are just one type of large platform provider” that have access to consumer data.⁹

Instead, of recognizing this fact, and treating broadband providers with the same light-touch approach that has seen such success with respect to other large platform providers, the FCC proposes a three-tier consent scheme. This framework consists of (1) implied consent for data used in actually providing broadband service, (2) opt-out consent for marketing “communications-related” services, and (3) opt-in consent required for any other uses of data. The entire regulatory scheme is explicitly structured around what business practices broadband providers can and cannot participate in. As such, this proceeding is less about enabling consumers to make choices about how their information is used by broadband providers—again, those choices already exist. Instead, it is more an ongoing effort to continually narrow broadband providers’ businesses down to one of pure transport. It cuts off the possibility of targeted advertising-based models that would provide a revenue stream other than subscribers’ monthly bills to support deployment of next-generation networks or consumer broadband discounts. Discounts offered in exchanged for access to browsing data would be especially helpful to price sensitive consumers, who may well not value their privacy as highly as some of the privacy advocates pressuring the FCC.

In essence, the FCC is making the wrong up-front choice for consumers by mandating an opt-in process that will reduce consumer welfare, productivity, and innovation. Most people are happy to make trade-offs around privacy and other values, such as convenience or price, but requiring them to go out of their way and take the extra step of opting in would sharply reduce participation rates. For the small share of consumers who truly worry about broadband information practices, they have strong motivations to opt out, and are already able to do so under current practice. But the FCC proposal would effectively shut off innovative practices that would benefit the majority of broadband consumers who would otherwise likely be willing to participate. It is a widely agreed-upon point that privacy rules in particular, and rules governing technology-enabled practices and business models generally, should be technology-neutral and evenly applicable across different

⁹ Federal Trade Commission, “Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers,” at 56 (March 2012), <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.

entities.¹⁰ Instead, the FCC is looking to build new regulatory silos based on what business practices it thinks broadband providers should and should not be engaged in.

FTC ENFORCEMENT AND EXISTING CONSUMER CHOICE BETTER BALANCES PRIVACY AND INNOVATION

The tremendous value of innovation stemming from new sources of data has been well recognized by a number of respected institutions. The President's Council of Advisors on Science and Technology, for example, outlined a number of benefits in its recent report on privacy and big data, ultimately stating their strong belief that "the positive benefits of big-data technology are (or can be) greater than any new harms."¹¹ As noted by the White House, "properly implemented, big data will become a historic driver of progress."¹² And as the White House noted more recently, "big data provides opportunities for innovations that reduce discrimination and promote fairness and opportunity, including expanding access to credit in low-income communities, removing subconscious human bias from hiring decisions and classrooms, and providing extra resources to at-risk students."¹³

The FCC, however, focuses exclusively on hypothetical harms from information sharing and use by broadband providers, and fails to adequately recognize the significant upside to an additional source of data that can be put to innovative use. By helping individuals and organizations make better decisions, data has the potential to spur economic growth and improve quality of life in a broad array of fields—the FCC appears to under-appreciate this fact.

Any new regulations should recognize there is a balance between the benefits additional sharing and use of data and the risk of privacy harms.¹⁴ The research of Catherine Tucker at MIT has shown the light-touch privacy regime in the United States is a significant factor in why this country leads in the Internet economy compared regions under more restrictive privacy regimes, such as the European Union.¹⁵ There is a significant

¹⁰ Indeed, this was a motivating concern behind the Administration's proposed Consumer Privacy Bill of Rights. In supporting that proposed legislation, the White House explained that "[i]t is important that a baseline statute provide a level playing field for companies, a consistent set of expectations for consumers..." The White House, "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy," at 36 (February 2012), <https://www.whitehouse.gov/sites/default/files/privacy-final.pdf>.

¹¹ President's Council of Advisors on Science and Technology, "Big Data and Privacy: A Technological Perspective" (May 2014), at 14,

https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf

¹² Executive Office of the President, "Big Data: Seizing Opportunities, Preserving Values" (May 2014),

https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf

¹³ Executive Office of the President, "Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights" (May 2016), https://www.whitehouse.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf.

¹⁴ On this balance, see Avi Goldfarb & Catherine Tucker, "Privacy and Innovation," in *Innovation Policy and the Economy*, Volume 12 U. of Chicago Press (2012), 65-89.

¹⁵ Catherine Tucker, "Empirical Research on the Economic Effects of Privacy Regulation," 10 *J. on Telecomm. & High Tech. L.* 265 (2012) available at http://jthtl.org/content/articles/V10i2/JTHTLv10i2_Tucker.PDF

risk that privacy advocates will seek to use the FCC's more restrictive model to ratchet up rules across the rest of the Internet ecosystem in a way that would do significant harm to the online economy.

We should prefer the FTC model as simply superior in supporting data innovation compared to that proposed by the FCC. The FTC oversees fair competition and has broad authority under Section 5 of the Fair Trade Act to take enforcement actions against unfair or deceptive trade practices.¹⁶ The FTC also offers specific guidance when it comes to privacy, having put forth a single, comprehensive framework guided by three overarching principles: privacy by design, consumer choice, and transparency.¹⁷

By allowing flexibility for industry to develop best practices within these guidelines, and stepping in *ex post* where problems develop, the FTC does not have to predict the direction technological advancements or changes in business practices will take us. This allows firms to internalize or outsource different functions in fast-paced industries with a focus on efficiency rather than compliance. This type of privacy oversight, with rules that apply an even, light-touch approach to different actors, would be a better environment for dynamic competition to occur across platforms. A uniform oversight framework, with low regulatory barriers to entry, would not only allow carriers to explore further entry into areas like advertising, but would avoid discouraging new entrants from providing broadband services.

The FCC proposal deviates from the well-tested FTC enforcement model in several significant ways, most egregiously in structuring its opt-in choice architecture around the services broadband providers seek to engage in, instead of consumers' expectations of privacy or risk of harm. It also imposes significant burdens around ensuring data not be re-identifiable, and data security requirements.

Both current FTC staff and the former FTC Chairman, Jon Leibowitz filed comments outlining the ways in which the proposal deviated from the FTC approach. As Leibowitz put it, "in many important areas [the FCC's proposal] overshoots the mark, proposing regulations for broadband providers that go well beyond those imposed upon the rest of the Internet economy and which, if adopted, would undercut benefits to the very consumers it seeks to protect."¹⁸ Current FTC staff commented as well, writing that aspects of the proposed rules "[do] not reflect the different expectations and concerns that consumers have for sensitive and non-sensitive data. As a result, it could hamper beneficial uses of data that consumers may prefer...."¹⁹ Former

¹⁶ 15 USC § 45.

¹⁷ Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers," March 2012, <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.

¹⁸ Jon Leibowitz, "In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, Comments of Jon Leibowitz," at 2, WC Docket No. 16-106, *available at* <http://apps.fcc.gov/efds/document/view?id=60002014604>.

¹⁹ Staff of the Bureau of Consumer Protection of the Federal Trade Commission, "In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, Comments of FTC Staff," at 22, WC Docket No. 16-106, *available at* https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection-federal-trade-commission-federal-communications-commission/160527fcccomment.pdf.

FTC Commissioner Josh Wright specifically called out the negative impact on innovation, characterizing the proposal as one that “fails to consider the economic costs affecting consumers, ISPs, and innovation.”²⁰

A uniform set of light-touch privacy oversight tracking the FTC approach would preserve the flexibility needed for innovation and incentives for cross-platform competition.

PRIVACY POLICIES SHOULD BE ADDRESSED AT A CONGRESSIONAL LEVEL, IF AT ALL, NOT THROUGH NOVEL FCC STATUTORY INTERPRETATION

Privacy policies, especially those proposed by the FCC, impact a substantial portion of the Internet economy, and should be developed at a national level through Congress. Instead, the FCC is improvising, twisting a statute that was clearly developed for a different time. The FCC took this step backwards in time when forced to classify broadband providers as Title II common carriers in order to impose its ill-advised net neutrality rules. Many of the problems with this rulemaking, and common carrier classification generally, stem from the FCC attempting to fit a square broadband peg into a round Title II hole. The political and popular support for open Internet rules provided cover for the FCC to attempt to usurp jurisdiction over broadband privacy from the FTC, who had successfully overseen the privacy practices of broadband provider prior.

In its proposal, the FCC overwhelmingly relies on Section 222, within Title II of the Communications Act. Section 222 was written as a tool to prevent anti-competitive use of telephone records by rival phone companies as a part of the 1996 Telecommunications Act’s introduction of competition into the local telephone market. This was a time when only one type of company—telephone providers—had unique, and uniquely valuable, data about customers. The FCC now intends to repurpose this statute into a broad mandate to police virtually all aspects of broadband providers’ collection and use of customer data—even broader than it had interpreted the statute when regulating telephone records—in an economic system that is far more complex and dynamic.

This proceeding, and privacy generally, is an area of significant national concern, and policy here should be set through an open and democratic legislative process in Congress, not creative statutory re-interpretation by an independent agency. Congress is better suited to ascertain the implications of broadband privacy regulations on areas outside the FCC’s jurisdiction and balance the numerous policy goals implicated by this proceeding.

CONCLUSION

Some of the policy goals animating the FCC’s proposal are legitimate, but simply given undue weight. There is certainly an interest in ensuring customers have transparent notice and choice over how their information is used and collected when navigating the Internet ecosystem, but, consumers already have this choice and the FTC framework better balances competition, innovation, and consumer protection.

²⁰ Joshua D. Wright, “An Economic Analysis of the FCC’s Proposed Regulation of Broadband Privacy” (May 2016), available at <http://apps.fcc.gov/ecfs/document/view?id=60002077298>.

Given the advent of tools for users to protect their privacy and the fact ISPs provide consumers with meaningful control over the use of their data, there is no specific consumer harm occurring that the FCC needs to correct, and no justification for specific, heightened rules peculiar to the FCC's jurisdiction. Congress should direct the FCC to correct course, and adopt rules in line with the existing FTC framework.

Thank you again for this opportunity to appear before you today.

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 translates 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. 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, if 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 lead 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 invasive 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 data 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 Web sites 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 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 with 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 Web site, 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—your ISP is still privy—to the domain name, the domain name of the Web site 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 DC Circuit opinion, but they do know that you are at The New York Times Web site 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 OK. 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. LEIBOWITZ. 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 [continuing]. 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, OK. 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 of Things 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 ISPs. 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 Web site 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. OK. OK. 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. OK. 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 DC 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. OK. 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. SHIMKUS [presiding]. 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. 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 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 respected 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 enforce-

ment 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 Web sites 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 agree with Mr. Shimkus and in doing so disagree with Mr. Ohm. Nineteen Ninety-Six 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—in my district of Louisville, Kentucky, 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 up. 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 Web site, 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 2½ 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 rule-making, 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. OK, 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. OK, 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. OK, 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 be 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. OK, 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 treat-

ing ISPs' use of data differently than other businesses who use on-line 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 OK.

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 are negotiated consent decrees that last for 20 years, another tool is its ability to find practices unfair even without a finding of economic 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 Web sites.

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, OK, 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 take 2½ years to go through a workshop and put out a draft rule and take 2½ 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 perspective.

Mr. LONG. OK. 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 inconsis-

encies. 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.

OK, 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 markup on a bill to change the FTC's enforcement authorities. Given your experi-

ence 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 leads 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 overreaching 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 8½ years 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 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 12:21 p.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

PREPARED STATEMENT OF HON. FRED UPTON

Today we focus on the latest regulatory overreach by the FCC to create a new privacy regime for broadband providers. As a result of last year's reclassification of

Internet service providers, the industry was removed from the Federal Trade Commission's jurisdiction and placed in unclear territory. Attempting to fill the void it created, the FCC proposed a set of complex and burdensome new restrictions that will create uncertainty for consumers and cause harm to the marketplace.

These rules simply miss the mark. By singling out broadband providers, the FCC is feeding unbalance into the Internet economy. Until recently, the entire Internet ecosystem successfully operated under the enforcement-based privacy protections of the FTC model and I fear this new approach will reduce competition in the flourishing Internet marketplace. The FCC should hear the widely shared concerns and collaborate with industry to balance consumer privacy and innovation policy.

The focus of the Energy and Commerce Committee has always been consumers. We all share the goal of keeping personal data safe and secure, and while doing so encouraging innovation, growth, and better services. I joined with my colleagues earlier this month to encourage the FCC to reconsider their proposal. I hope our panel of experts today can help provide further insight into the proposed rules and an optimal path forward that will provide the greatest benefits for consumers.

FRED UPTON, MICHIGAN
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FOURTEENTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115

Majority (202) 225-2827
Minority (202) 225-3941

June 1, 2016

The Honorable Tom Wheeler
Chairman
Federal Communications Commission
445 12th Street, S.W.
Washington, DC 20553

Dear Chairman Wheeler:

On April 1, 2016, the Federal Communications Commission (FCC) released a Notice of Proposed Rulemaking (NPRM) proposing novel privacy and data breach notification requirements on broadband Internet access service providers (ISPs).¹ Creating a disparate set of rules for *some* members of the Internet ecosystem is the wrong approach and ignores the last four decades of development in the U.S. The inconsistencies in the proposed rules undermine the public's expectation of a seamless and contextually relevant online experience.

To date, the Federal Trade Commission (FTC) has been the primary arbiter of consumers' rights and expectations with regard to Internet privacy. Under the FTC's enforcement-oriented approach, all participants – from back-end database service providers to consumer-facing content creators – have existed under the same set of privacy rules. As a result, Internet deployment and adoption has thrived, consumers have quickly adopted services, and providers of both access and services continue to develop new products and services to meet consumer demand.

Notwithstanding the evolving definition of broadband, since 2000, broadband penetration has gone from three percent of the population to 67 percent;² Internet-connected mobile devices have penetrated 68 percent of the American population;³ and, broadband providers have covered 95 percent of the United States population.⁴ In 2014 alone, broadband providers invested \$78

¹ *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Notice of Proposed Rulemaking, WC Docket No. 16-106, 31 FCC Rcd 2500 (2016).

² Pew Research Center for Internet and American Life at <http://www.pewinternet.org/three-technology-revolutions/>.

³ *Id.*

⁴ See Broadband for America at <http://www.broadbandforamerica.com/issues>.

Letter to Chairman Tom Wheeler
Page 2

billion in infrastructure to serve American consumers. All this investment activity has benefited the nation through increased communication, increased access to services, and increased economic activity. A recent study indicated that in 2014, the broadband and information communications technology sector was directly responsible for nearly 6 percent of the 2014 U.S. GDP – over \$1 trillion.⁵

Despite the success and economic benefit that a sensibly regulated Internet brought to the U.S. economy, in February of 2015, the FCC reclassified broadband Internet service providers as common carriers under Title II of the Communications Act of 1934.⁶ The activities of common carriers, as services highly-regulated by specialized agencies, have long been exempt from FTC authority. By reclassifying broadband, the FCC removed broadband Internet access service providers from the FTC's jurisdiction, creating a two-tiered Internet. This is exactly the kind of system the FCC's 2015 Open Internet Order purported to prevent. Now, to solve a problem of its own making, the FCC seeks to establish an entirely new regime of prescriptive privacy regulations unique to broadband Internet service providers. The FCC's approach summarily rejects the proven model of the FTC, which preserved the value of the "end-to-end" Internet, in favor of a rulemaking that somehow manages to be both unclear and overly prescriptive.

The FCC attempts to justify special treatment for ISPs based on its conclusion that "ISPs are the most important and extensive conduits of consumer information and thus have access to very sensitive and very personal information that could threaten a person's financial security, reveal embarrassing or even harmful details of medical history, or disclose to prying eyes the intimate details of interests, physical presence, or fears."⁷ The FCC offers no evidence for this conclusion which stands in contradiction to a recent report by Peter Swire, privacy czar under President Clinton.⁸ According to the Swire report, ISPs do not have a comprehensive ability to collect data on consumers, nor are they unique in their data collection capabilities.⁹ The FCC, however, seems to gloss over the facts, skips the data collection process that would have surfaced these facts, and proceeds to single out ISPs for privacy requirements that do not match up to the privacy challenges consumers face.

The FCC claims that it is not reinventing the wheel, but this assurance is belied by its recent actions and the plain text of the FCC's proposed rules. For example, there is no state law that sets a ten-day deadline for notification to consumers after discovery of a breach. Yet, this is exactly what the NPRM proposes. Ample testimony has been given to Congress and state legislatures about the time it takes after a breach to ensure that the compromised system is

⁵ Kevin A. Hassett and Robert J. Shapiro, "The Impact of Broadband and Related Information and Communications Technologies on the American Economy" (rel. Mar. 23, 2016) at http://internetinnovation.org/images/misc_content/Report_on_the_Economic_Impact_of_Broadband_-_Hassett-Shapiro_-_Rev_-_March_23_2016.pdf.

⁶ *Protecting and Promoting the Open Internet, Report and Order on Remand, Declaratory Ruling, and Order*, 30 FCC Rod 5601 (2015) (2015 Open Internet Order).

⁷ *FCC Privacy NPRM* at para. 2.

⁸ Peter Swire, Justin Hemmings, Alana Kirkland, "Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others," Georgia Tech Institute for Information Security and Privacy Working Paper (rel. Feb. 29, 2016) at <http://www.iisp.gatech.edu/working-paper-online-privacy-and-isps>.

⁹ *Id.*

Letter to Chairman Tom Wheeler
Page 3

secured without putting more information at risk.¹⁰ Requiring a company to start preparing notification letters before it contained the breach is unprecedented and irresponsible. This is only one example of many that raise concerns.

Ultimately, the FCC's proposal for new ISP-specific privacy rules seems to miss the point: rather than serve the public interest, these new rules will create public confusion. By subjecting data to multiple and varying privacy regimes within a consumer's single Internet experience, consumers will be left to question which privacy rules apply. For example, in today's Internet ecosystem, a single company theoretically could collect data from an operating system, a browser, a content website, an app, as well as a retail broadband service. In this situation, the FTC would continue to regulate all but the retail ISP offering, which would be subject to new and different rules under the FCC's proposed rules. It is unlikely that consumers will quickly grasp the regulatory arcana that changes the way their data are protected.

Rather, it is more likely the disparate privacy regimes will distort the marketplace. Disparate sets of rules for similarly situated entities create opportunities for regulatory arbitrage. Although we may not know in what ways this arbitrage will manifest, it is almost always the consumer who suffers in the end. Consumers will bear the impact of delayed innovation, consumers will suffer from deferred deployment, and consumers will suffer from inefficient design as companies seek to avoid a more burdensome and costly privacy regime. This unjustified bifurcation of the U.S. Internet privacy regime is particularly troubling at a time when there is so much focus on setting international standards on data flows.

The free flow of information over the Internet has allowed for one of the greatest technological transformations of the last century. This was no accident. Around the world, countries are attempting to create their own version of Silicon Valley because they see the economic value generated when a government gets out of the way and lets its citizens innovate. The FCC's proposed rule endangers the regulatory framework that has made the U.S. the world leader on the Internet and created hundreds of thousands, if not millions, of U.S. jobs.

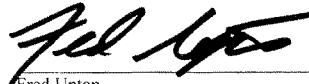
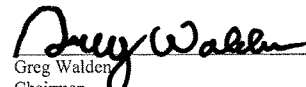
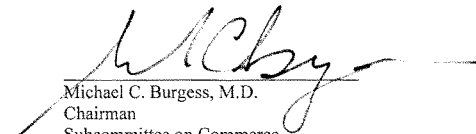
We recognize that even in a world where the FCC erroneously considers the Internet to be common carriage, consumers deserve to be protected. However, rather than a prescriptive rulemaking, we believe that the FCC should create a more consistent privacy experience for consumers by mirroring the FTC's successful enforcement-based regime. We know that the FCC can successfully implement such an approach. As recently as March 7, 2016, the FCC relied on an enforcement action to address concerns over the use of "supercookies" by ISPs.¹¹ Knowing that an enforcement-based approach at the FCC, modeled on the FTC's success, can work to protect consumers without injecting new complexity and uncertainty into the Internet economy, we urge you to reconsider your approach.

¹⁰ See e.g. Written testimony of Michael R. Kingston, "Protecting Consumer Information: Can Data Breaches Be Prevented?" Subcommittee on Commerce, Manufacturing, and Trade, February 5, 2014, <http://docs.house.gov/meetings/IF/IF17/20140205/101714/HMTG-113-IF17-Wstate-KingstonM-20140205.pdf>; Response of Ms. Madigan, "Protecting Consumer Information: Can Data Breaches Be Prevented?" Subcommittee on Commerce, Manufacturing, and Trade, February, 5, 2014, p. 40, and response of Mr. Noonan, p. 85, <http://docs.house.gov/meetings/IF/IF17/20140205/101714/HMTG-113-IF17-Transcript-20140205.pdf>.

¹¹ *In the Matter of Cellco Partnership, d/b/a Verizon Wireless*, Order, File No. EB-TCD-14-00017601, 31 FCC Rcd 184 (2016).

Letter to Chairman Tom Wheeler
Page 4

Sincerely,


Fred Upton
Chairman
Greg Walden
Chairman
Subcommittee on Communications and Technology
Michael C. Burgess, M.D.
Chairman
Subcommittee on Commerce,
Manufacturing, and Trade

cc: The Honorable Frank J. Pallone, Jr., Ranking Member

The Honorable Anna G. Eshoo, Ranking Member
Subcommittee on Communications and Technology

The Honorable Janice Schakowsky, Ranking Member
Subcommittee on Commerce, Manufacturing, and Trade



June 13, 2016

The Honorable Greg Walden
Chairman, Subcommittee on Communications and Technology
House Committee on Energy and Commerce
2185 Rayburn House Office Building
Washington, DC 20515

The Honorable Anna Eshoo
Ranking Member, Subcommittee on Communications and Technology
House Committee on Energy and Commerce
241 Cannon House Office Building
Washington, DC 20515

Dear Chairman Walden and Ranking Member Eshoo:

We write to commend the Subcommittee for holding its hearing to examine the FCC's proposed broadband privacy rules. Given the substantial interest in the proceeding and the significant concerns that have been raised about the proposed rules' impact on consumers, competition, and innovation, the hearing is timely and important.

A unified privacy framework applicable to all entities collecting and using consumer data, based on the FTC's longstanding and successful approach, has been essential to the growth of the Internet economy and the multitude of affordable and cutting edge online services available to consumers today. Accordingly, we believe the FCC's primary objective in adopting privacy rules for Internet Service Providers (ISPs) should be to ensure consistency with the FTC's existing framework. The need for a consistent regulatory approach was stressed in numerous comments filed in response to the FCC's broadband privacy Notice of Proposed Rulemaking (NPRM). Many commenters also discussed the negative consequences for consumers, competition, innovation, and broadband

investment that will result if such burdensome and prescriptive regulations are imposed on only one segment of the Internet.

In no way does the FCC's decision to reclassify broadband as a Title II service require a departure from the FTC's successful approach to privacy based on effective notice to consumers and a meaningful choice as to how their data is used. Comments from the staff of the FTC's Bureau of Consumer Protection pointed out that the FCC's proposed rules that are only applicable to ISPs "is not optimal." More specifically, the FTC's staff called into question the FCC's proposed rules that are based on the type of entity with access to data, rather than the sensitivity of particular information which "could hamper beneficial uses of data that consumers may prefer, while failing to protect against practices that are more likely to be unwanted and potentially harmful." These sentiments were reflected in numerous comments from current and former FTC Commissioners, civil rights organizations, the advertising industry, health and home efficiency companies, economists, academics, constitutional scholars, and technology organizations who called on the FCC to develop a common, harmonized approach to online privacy that limits the imposition of an opt-in consent requirement to the use and disclosure of sensitive data such as social security numbers, health and financial data, children's information, and precise geolocation information. Recent survey research provided to the FCC shows that consumers agree, with 83% of respondents indicating that privacy protections should be based on the sensitivity of data, *not* on who collects it.

We agree as well. In March, a broad industry coalition composed of ISPs, tech companies, equipment providers, and many others urged the FCC to adopt a flexible, principles-based privacy regime based on the FTC's notice-and-choice framework that remains applicable to the rest of the Internet ecosystem. The privacy proposal, attached to this letter, includes central elements of the FTC framework – transparency, respect for context, and choice –to protect consumers. The principles give consumers the ability to choose how their data is used and protects their personal information by prohibiting unfair or deceptive acts or practices. Unlike the FCC's proposal, however, the flexibility the principles permit would allow consumers to experience the substantial benefits that result from companies having the ability to responsibly use data in ways that foster competition, innovation, and the continued emergence of new services and applications.

Adoption of the principles-based approach would be consistent with the White House's longstanding call for a uniform privacy framework. It would also be consistent with the suggestions of the many parties who have already weighed in with the FCC and made clear that the FCC should abandon its flawed approach and harmonize privacy regulation with the well-established and effective approach implemented by the FTC and consistently endorsed by the Obama Administration. Finally, it would ensure consistency internationally as discussions continue around the "Privacy Shield" to facilitate cross-border data sharing and avoid what one Member of the European Parliament recently called a "glaring double standard" that "would certainly raise eyebrows from a European perspective."

We appreciate the Subcommittee's important recognition of this issue and the need for Congressional oversight. We are hopeful that your examination of these issues will highlight the need for an FCC approach that is consistent with the Administration's call for a uniform privacy framework and that closely harmonizes FCC privacy rules with the existing FTC framework. Doing so would protect consumer privacy, minimize consumer confusion resulting from inconsistent regulations, and provide the flexibility the online marketplace needs in order to continue to innovate and evolve as it has done for many years under such a regime.

Sincerely,



Matthew M. Polka
President & CEO
American Cable Association



Meredith Attwell Baker
President & CEO
CTIA®



Jim Halpert
President & CEO
Internet Commerce Coalition



Genevieve Morelli
President
ITTA



Jonathan Spalter
Chair
Mobile Future



Michael Powell
President & CEO
National Cable & Telecommunications Association



Scott Belcher
CEO
Telecommunications Industry Association



Walter B. McCormick, Jr.
President & CEO
USTelecom

June 13, 2016

The Honorable Greg Walden
Chairman, Subcommittee on Communications and Technology
House Committee on Energy and Commerce
2185 Rayburn House Office Building
Washington, DC 20515

The Honorable Anna Eshoo
Ranking Member, Subcommittee on Communications and Technology
House Committee on Energy and Commerce
241 Cannon House Office Building
Washington, DC 20515

Dear Chairman Walden and Ranking Member Eshoo:

We, the undersigned trade associations, collectively represent hundreds of companies from small businesses to household brands engaging in responsible data collection and use that benefit consumers and the economy. We appreciate the Subcommittee on Communications and Technology (“Subcommittee”) convening the upcoming June 14th hearing on “FCC Overreach: Examining the Proposed Privacy Rules,” which will examine the Federal Communications Commission’s (“FCC”) recent “Notice of Proposed Rulemaking on Protecting the Privacy of Customers of Broadband and Other Telecommunications Services” (“NPRM”). We believe that the NPRM would create restrictions that are unnecessary, overly burdensome, and outside the FCC’s statutory authority.

The Internet—powered by data, innovation, and private investment—has been an engine of economic growth and a source of exciting consumer benefits, even during challenging economic times. In recent decades, consumers’ daily lives have been transformed by a wealth of data-driven online resources, including an unprecedented array of high-quality information and entertainment, all available to consumers because these resources are subsidized by advertising. The economic benefits of the Internet revolution are just as substantial. One recent study estimated that the use of data-driven marketing added output of at least \$202 billion to the U.S. economy in 2014, representing a 35% increase since 2012.¹ All 50 states experienced job growth in the data-driven marketing economy during the same time period.²

We and our member companies are concerned that the FCC is using the NPRM in an attempt to create restrictive new requirements for the data collection and use that are central to economic success and consumer benefits. We believe that the proposed restrictions are unnecessary and would exceed statutory authority.

¹ Deighton and Johnson, “The Value of Data 2015: Consequences for Insight, Innovation and Efficiency in the U.S. Economy” 16 (December 2015), <http://thedma.org/advocacy/data-driven-marketing-institute/value-of-data/>.

² *Id.* at 5 (Preface by the Direct Marketing Association).

- **Existing voluntary self-regulatory standards supported by Federal Trade Commission (“FTC”) enforcement are the appropriate tool to govern the dynamic and interrelated online content and advertising ecosystem.** Currently, online data collection and use are governed by robust industry self-regulatory regimes that subject the industry to the jurisdiction of the FTC and state attorneys general. These regimes are regularly updated to reflect new business models. Responsible data practices are essential for the continued success of the Internet economy. Enforceable, voluntary self-regulatory codes remain best suited to promote consumer privacy protections while allowing these legitimate data practices to flourish. The Congress has considered these issues many times based on ample hearings and debate, and each time has declined to enact new legislation, recognizing that new regulation in this rapidly evolving area would hinder innovation, not provide new benefits to consumers, and threaten the economic value of a thriving market sector.
- **The NPRM is unnecessary because effective legal safeguards already exist for online data practices.** In addition to industry self-regulation, the FTC vigorously enforces consumer privacy and data security standards using its authority to address “unfair or deceptive” business practices under Section 5 of the FTC Act. The FTC has used this authority to enforce prior company commitments to comply with industry self-regulatory requirements and to protect consumers from harm. State attorneys general typically follow FTC positions to actively enforce similar laws at the state level. These legal frameworks already provide consistent, meaningful consumer protections which can apply across industries, including to the practices the FCC now seeks to regulate. A new framework is not needed because the FTC has already established principles in this area.
- **The FCC is overreaching and lacks congressional authority to issue the proposed regulation.** Congress directed the FCC to foster competition among telephone providers, and in that context to enforce rules to safeguard the proprietary data that such providers maintained through their services. The FCC does not have authority from Congress to establish new privacy restrictions in the very different area of online data collection.
- **Consumers and industry benefit when one agency takes the lead on privacy regulation and enforcement.** The FTC has a long history of addressing and enforcing privacy-related issues across industries. The FCC’s NPRM is not consistent with the established approach of the FTC, and would result in a different and problematic regime. The FCC has not sufficiently analyzed the implications of its NPRM, but is now rushing to finalize its flawed proposal; in fact, it denied industry’s request for a reasonable extension of time to properly evaluate and advise the FCC on the NPRM’s impact. The limited time for the creation of a robust record is all the more concerning when the FCC does not have the FTC’s long history of expertise on this issue. The FCC would benefit from allowing more time for public comments.
- **The NPRM is out of step with existing privacy frameworks and would undermine the ad-supported Internet.** For example, the FCC would expand the definition of personally identifiable information (“PII”) to data elements that generally are not, and have not been considered, individually identifiable, such as application usage data,

persistent online identifiers (cookies), device identifiers, and Internet browsing history. Many companies have developed service models that focus on collecting such data instead of PII.

- **The proposed consent standard is too restrictive.** Further, the FCC has proposed to restrict most uses and disclosures of such data with an “opt in” consent standard. Experience shows that where consumer choice is warranted, an opt-out or implied consent standard is the best way to recognize consumer privacy preferences with respect to these types of online data while allowing legitimate practices, including advertising, to continue.
- **There is no record of harm to justify new regulation in this area or the specific proposals put forward by the FCC.** Consumers have embraced today’s thriving Internet, which is fueled by responsible data practices governed by the existing regulatory framework. The current online ecosystem subsidizes online offerings that consumers value, promotes innovation, and grows the economy. There is no record of consumer harm that supports the FCC’s proposal for such restrictive regulations.
- **Congress should set a uniform national breach notification and data security standard.** The FCC has proposed to regulate breach notification in a way that is contrary to the existing state notification regimes as well as the proposals under consideration by Congress. This would cause compliance burdens for businesses and confusion for consumers. Congress should establish a uniform standard for breach notification and data security.

* * *

The undersigned organizations thank you for your oversight of this important issue. The NPRM, as drafted, would create unnecessary and inconsistent privacy regulations that would undercut the vibrant online ecosystem. Congress can and should exercise its oversight authority to protect consumers and the economy from this outcome.

American Advertising Federation
 American Association of Advertising Agencies
 Association of National Advertisers
 Direct Marketing Association
 Electronic Retailing Association
 Electronic Transactions Association
 Interactive Advertising Bureau
 National Business Coalition on E-Commerce & Privacy
 National Retail Federation
 Network Advertising Initiative
 U.S. Chamber of Commerce



June 14, 2016

The Honorable Greg Walden
Chairman
Subcommittee on Communications and
Technology
Committee on Energy and Commerce
U.S. House of Representatives
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Anna Eshoo
Ranking Member
Subcommittee on Communications and
Technology
Committee on Energy and Commerce
U.S. House of Representatives
2322A Rayburn House Office Building
Washington, DC 20515

Dear Chairman Walden and Ranking Member Eshoo:

Competitive Carriers Association (CCA) thanks the Subcommittee on Communications and Technology for its timely attention to the Federal Communications Commission's (FCC) proposed rules governing the privacy practices of Broadband Internet Access Service providers ("BIAS"). CCA members take their customers' privacy seriously and value the trust they've engendered. In crafting new privacy rules for BIAS providers, the FCC should build upon successful models that establish clear privacy rules to protect consumers and foster continued innovation from BIAS providers and others in the Internet ecosystem while appropriately considering impacts on smaller, rural and regional companies.

CCA is the nation's leading association for competitive wireless providers and stakeholders across the United States. CCA's membership includes nearly 100 competitive wireless providers ranging from small, rural carriers serving fewer than 5,000 customers to regional and national providers serving millions of customers. CCA also represents approximately 200 associate members including vendors and suppliers that provide products and services throughout the mobile communications supply chain. CCA is uniquely positioned to provide guidance on both large and smaller wireless providers' privacy practices.

CCA, along with a coalition of ISPs and other industry stakeholders, submitted a privacy proposal to the FCC recommending a flexible privacy framework consistent with the Federal Trade Commission's (FTC) longstanding approach to broadband privacy. This proposal's four core tenets – transparency, respect for context and consumer choice, data security, and data breach notification – protect consumers by prohibiting unfair and deceptive practices, without unnecessarily compromising the everyday business needs of BIAS providers of all sizes. Additionally, and consistent with Administration policy, the Industry Proposal is harmonized with existing FTC rules that protect consumers as they engage with Internet companies other than BIAS providers, including edge providers, to reach new content, products, technologies and services to provide businesses and consumers alike with a common set of rules.

The FCC rules as currently proposed, however, take a different approach that could lead to bifurcated consumer protections and experiences across different entities in the Internet ecosystem creating uncertainty and consumer confusion.

The record clearly reflects broad concern that the FCC's proposed rules could be overly-burdensome, particularly for smaller rural and regional BIAS providers, when other approaches have been proposed that the FCC could take to more appropriately protect consumers. For example, new contractual and oversight liabilities for consumer information lawfully shared with third parties could confuse consumers and disrupt the now-unified privacy regime controlling the rest of the Internet ecosystem.

Further, smaller carriers may struggle to implement the FCC's proposed rules. The scope of information covered, "customer proprietary information" (customer PI), a category of information seemingly without limit that captures all information "linkable" to a subscriber, may be so broad as to render proposed rules untenable for smaller carriers seeking to comply. For example, the "consumer-facing dashboard" envisioned by the FCC would require a carrier to create a persistently-available interface allowing a subscriber to review a list of all customer PI that an ISP may possess (in effect, *all* information remotely related to that subscriber), and the choice that consumer has made regarding how that information might be used. This burden alone could needlessly stress limited programming resources and impose costs where small carriers already transparently disclose their privacy practices through direct relationships with their customers as a part of the communities they serve. The FCC's proposal contains other proposals involving similarly taxing notice, retention, and disposal requirements that do not offer meaningful consumer benefits. Instead, the Commission should limit protections to the most sensitive data collected by an ISP.

Also burdensome is the Commission's proposed data security regime, which would require all carriers to "ensure the security...of all [customer PI]." Even the largest companies, employing cutting-edge protections and using every tool reasonably available to protect consumers, experience hacks and data security breaches. It is, therefore, especially unreasonable for the Commission to place such a burden on a small BIAS provider, who likely retains as little subscriber data as possible. A principles-based regime centered on "reasonable" data security protections that considers the size and resources available to an ISP, as well as how an ISP utilizes personal information, would protect consumers without making compliance impossible, and would remain applicable as data security technology evolves.

CCA commends and appreciates your leadership in convening this important hearing, and urges policymakers to explore alternative privacy protections like the Industry Proposal. Any adopted rules should blend seamlessly with privacy regimes controlling the rest of the Internet ecosystem, which would promote consumer welfare by making it easier for consumer to predict how their choices would impact the way their information is shared, used, or stored by a BIAS provider, while appropriately considering treatment of smaller carriers.

Please do not hesitate to contact me with any questions.

Sincerely,



Steven K. Berry
President & CEO
Competitive Carriers Association

Cc:

The Honorable Fred Upton, Chairman House Energy and Commerce Committee
The Honorable Frank Pallone, Jr. Ranking Member, House Energy and Commerce Committee
The Honorable Bob Latta, Vice Chairman, Communications and Technology Subcommittee
The Honorable Joe Barton
The Honorable John Shimkus
The Honorable Marsha Blackburn
The Honorable Steve Scalise
The Honorable Leonard Lance
The Honorable Brett Guthrie
The Honorable Pete Olson
The Honorable Mike Pompeo
The Honorable Adam Kinzinger
The Honorable Gus Bilirakis
The Honorable Bill Johnson
The Honorable Billy Long
The Honorable Renee Ellmers
The Honorable Chris Collins
The Honorable Kevin Cramer
The Honorable Michael Doyle
The Honorable Peter Welch
The Honorable John Yarmuth
The Honorable Yvette Clarke
The Honorable David Loebsack
The Honorable Bobby Rush
The Honorable Diana DeGette
The Honorable G. K. Butterfield
The Honorable Doris Matsui
The Honorable Jerry McNerney
The Honorable Ben Ray Lujan

Congress of the United States
Washington, DC 20515

May 25, 2016

The Honorable Tom Wheeler
 Chairman
 Federal Communications Commission
 445 12th Street SW
 Washington, DC 20554-0004

The Honorable Jessica Rosenworcel
 Commissioner
 Federal Communications Commission
 445 12th Street SW
 Washington, DC 20554-0004

The Honorable Michael O'Rielly
 Commissioner
 Federal Communications Commission
 445 12th Street SW
 Washington, DC 20554-0004

The Honorable Mignon Clyburn
 Commissioner
 Federal Communications Commission
 445 12th Street SW
 Washington, DC 20554-0004

The Honorable Ajit Pai
 Commissioner
 Federal Communications Commission
 445 12th Street SW
 Washington, DC 20554-0004

Dear Chairman Wheeler and Commissioners Clyburn, Rosenworcel, Pai, and O'Rielly:

The Internet is revolutionizing the way consumers communicate, shop, learn, and entertain themselves. It is changing how they control their homes, their cars, and many parts of their lives. Consumers derive substantial benefits from using and relying on these connected products and services, which are powered and enabled by data. With these uses, consumers have certain Internet-related privacy and security expectations. Consumers rightly expect all companies that collect and use their data to be transparent about their practices and to provide them with appropriate choices with respect to how their information is used and shared.

Until last year, the Federal Trade Commission (FTC) provided a robust consistent privacy framework for all companies in the Internet services market. That holistic and consistent approach struck the right balance: consumers' use of Internet services and applications has continued to increase and consumers' privacy has been protected.

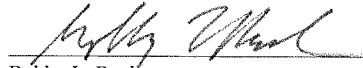
As you are aware, a consequence of the FCC's reclassification of broadband services has been to upset this consistent treatment giving rise to the rulemaking now under consideration aimed at Internet Service Providers (ISPs), which comprise only a portion of the Internet services market.

We had hoped that the FCC would focus on those protections that have traditionally guarded consumers from unfair or deceptive data practices by ISPs and the other companies in the Internet services market. But, based on the Commission's Notice of Proposed Rulemaking, we remain increasingly concerned that the Commission intends to go well beyond such a framework and ill-serve consumers who seek and expect consistency in how their personal data is protected.

If different rules apply to the online practices of only selected entities, consumers may wrongly assume that the new rules apply to all of their activities on the Internet. But when they discover otherwise, the inconsistent treatment of consumer data could actually undermine consumers' confidence in their use of the Internet due to uncertainty regarding the protections that apply to their online activities.

With the above considerations in mind, we strongly urge the FCC to consider a consistent FTC-type approach to protect consumer privacy that balances consumers' privacy expectations and avoids negative impacts on consumers.

Sincerely,



Bobby L. Rush
Member of Congress



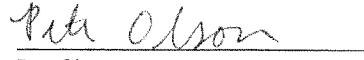
Gene Green
Member of Congress



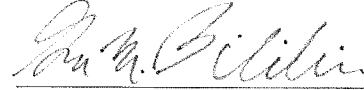
Leonard Lance
Member of Congress



Renee L. Ellmers
Member of Congress



Pete Olson
Member of Congress



Gus M. Bilirakis
Member of Congress



Kurt Schrader
Member of Congress

FRED UPTON, MICHIGAN
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FOURTEENTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115
Majority (2021) 225-2927
Minority (2021) 225-3041

July 5, 2016

The Honorable Jon Leibowitz
Co-chair
21st Century Privacy Coalition
901 15th Street, N.W.
Washington, DC 20005

Dear Mr. Leibowitz:

Thank you for appearing before the Subcommittee on Communications and Technology on Tuesday, June 14, 2016, to testify at the hearing entitled "FCC Overreach: Examining the Proposed Privacy Rules."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions with a transmittal letter by the close of business on Tuesday, July 19, 2016. Your responses should be mailed to Greg Watson, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to Greg.Watson@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Greg Walden
Chairman
Subcommittee on Communications and Technology

cc: Anna G. Eshoo, Ranking Member, Subcommittee on Communications and Technology

Attachment

Attachment – Additional Questions for the RecordThe Honorable Greg Walden

1. How and why does the FCC's approach fall short to protect consumers in current form? Do you have any suggestions for the FCC on how it could improve the proposal?

The Federal Communications Commission ("FCC") approach does not adequately protect consumers because it would create a bi-furcated regime for protecting privacy between the FCC's rules for Internet Service Providers ("ISPs") and the Federal Trade Commission's ("FTC") enforcement framework for the rest of the internet ecosystem. A holistic approach to internet privacy would provide the type of certainty and consistency that consumers expect, and would ensure that all entities that collect, use, and share information about consumers' online activities would respect consumer privacy in the same manner.

The FCC could improve its proposal by learning from the FTC's privacy experience and listening to the concerns raised in the FTC's Comment to the FCC. The FTC's comments support a privacy framework focused on consistency across industries and on the sensitivity of consumer information.

Instead of protecting consumers, the FCC proposal could harm them by making it more difficult for ISPs to provide services and capabilities their customers want. Most broadband consumers have shown -- by their behavior under the FTC framework -- that they are comfortable with having non-sensitive data utilized to provide them with customized advertising and offerings. Those that prefer not to have their data used in such a manner have ample opportunity to opt-out.

By requiring opt-in approval, the FCC's approach could harm consumer welfare by needlessly restricting data uses preferred by most consumers. While the FCC proposal makes it harder for ISPs to offer services and capabilities their customers favor, it fails to materially improve the privacy of consumers, because every non-ISP internet company would continue to be subject to different restrictions on their use of broadband data. Consumers would be made worse off by a framework that makes it more difficult for them to receive information about offerings and capabilities they enjoy today, while failing to provide any meaningful improvement in privacy protection.

2. During your tenure at the FTC, first as a commissioner, then as chairman, did the agency ever come to the conclusion that ISPs alone posed a unique problem in terms of privacy that warranted a more stringent and restrictive set of privacy obligations for them? Has anything changed since then?
 - a. During your tenure as FTC Chairman, the White House and Commerce Department also issued a privacy report and Consumer Privacy Bill of Rights regarding commercial uses of data. Did the Administration single out ISPs for special treatment or identify any unique problems associated with ISPs in setting forth its privacy policies and standards? Has anything changed since then?

The FTC's 2012 Privacy Report did not single out ISPs as posing unique privacy challenges; rather, the Report concluded that "to the extent that large platforms, such as Internet Service Providers, operating systems, browsers, and social media, seek to comprehensively track consumers' online activities, it raises heightened privacy concerns."¹ The FTC also concluded that "any privacy framework should be technology neutral."² Thus, the FTC report did raise potential concerns about "large platform providers," but not just ISPs. In the wake of that Report, the FTC gathered further information in a workshop and carefully examined the question of whether large platform providers, including major search engines and browser providers, as well as ISPs, should be subject to heightened restrictions and ultimately refrained from doing so.

Similarly, the Administration concluded that "[i]t is important that a baseline [privacy] statute provide a level playing field for companies, a consistent set of expectations for consumers, and greater clarity and transparency in the basis for FTC enforcement actions."³

The Honorable Adam Kinzinger

1. Mr. Leibowitz, in your testimony you went into detail on the differences between the FTC's current approach to data breach notification and the FCC's proposed regulation. You say that a balanced approach will avoid over-notification which would confuse customers and cause them to ignore notices they receive. Can you elaborate on this point? How does an optimal approach determine when a customer needs to be notified?

A balanced approach would limit the type of information for which an ISP would be required to notify consumers in the event of a breach of sensitive information the disclosure of which could result in identity theft or other financial harm. Unfortunately, the FCC's extremely broad proposed definition of "customer proprietary information" would require breach notification even for information the disclosure of which does not present a risk of harm to consumers. Consumers want to (and need to) be notified about breaches that present the reasonable risk of harm. But when consumers receive notices about breaches related to mundane, non-sensitive information, they will stop paying attention to breach notifications. Thus, when the notices are truly important, consumers may miss the opportunity to protect themselves.

2. Mr. Leibowitz, the FTC staff noted that the FCC's proposed data breach notification timeline would not allow companies adequate time to conduct an investigation. Do you agree with that conclusion?

¹ Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers at 14 (2012), <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.

²*Id.* at 56.

³ Executive Office of the President, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, at 36, January 2012, <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>.

10 days is not enough time to conduct an investigation. In 10 days, a company may not be able to determine whether a breach was inadvertent or whether it could result in identity theft or other financial harm. It is critical that companies have enough time to take remedial steps to address a breach and to conduct a comprehensive investigation before notifying consumers. The FTC expressed concerns about the FCC's proposed breach notification timeline, which is considerably shorter than each of the 47 state data breach notification laws.

The Honorable Gus Bilirakis

1. Mr. Leibowitz, Professor Lawrence Tribe from Harvard had an interesting Constitutional argument in his comments to the FCC about restrictions to commercial speech. Do you think we are looking at another issue in which we will all become court watchers and have to wait for months for a First Amendment challenge to work its way through the courts?

The FCC's proposed requirements would impose a substantial burden on speech because they would preclude ISPs from engaging in important and relatively routine communications with their customers. Such requirements would prevent the type of targeted speech from which consumers benefit, and would prevent speech which will continue to be permitted for non-ISPs. In order to pass constitutional muster, such a burden on commercial speech must satisfy each element of the three-part test set out in *Central Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n*, 447 U.S. 557 (1980), which asks whether (1) "the government interest is substantial"; (2) "the regulation directly advances the governmental interest asserted"; and (3) "it is not more extensive than necessary to serve that interest."

Professor Tribe concludes that the NPRM fails on each prong of the *Central Hudson* test.⁴ First, in Professor Tribe's view, the government has not articulated a substantial interest in restricting ISPs' ability to use customer information already in its possession, particularly where that information is not disclosed to third parties. Second, as discussed above, the NPRM completely ignores the fact that, even if the proposed highly burdensome rules are imposed on ISPs, edge providers will continue to collect and share precisely the same type of consumer information. For this reason, Professor Tribe has concluded that this asymmetry demonstrates that the NPRM cannot be considered to directly advance an important governmental interest. And third, Professor Tribe believes that the NPRM's proposed opt-in rule is not narrowly tailored because a less obtrusive opt-out rule would serve any legitimate government interest in protecting consumers from first-party marketing.

The FCC is already familiar with the *Central Hudson* constraints on the restrictions the agency may impose pursuant to Section 222 of the Communications Act (47 U.S.C. § 222). In *U.S. West Communications, Inc. v. FCC*, 182 F.3d 1224 (10th Cir. 1999), the

⁴ Laurence Tribe and Jonathan Massey, The Federal Communication Commission's Proposed Broadband Privacy Rules Would Violate the First Amendment, at 4 (May 27, 2016), <http://www.ctia.org/docs/defaultsource/defaultdocument-library/ctia-ncta-ust-file-tribe-paper.pdf>.

U.S. Court of Appeals for the 10th Circuit struck down the FCC's attempt at regulations governing Customer Proprietary Network Information ("CPNI") with respect to voice communications. In that case, the court determined that the collection and sharing of CPNI among affiliates constituted speech and that the FCC's opt-in regime did not satisfy intermediate First Amendment scrutiny. As Professor Tribe notes, the proposals in the NPRM "represent a *much larger* burden on speech and are far *less* tailored to any substantial governmental interest" (emphasis in original).⁵ Because the NPRM's proposed opt-in requirement poses a substantial burden on speech and is not tailored to any substantial governmental interest, it is susceptible to a constitutional challenge.

2. Mr. Leibowitz, can you expand on your concern that this new framework creates a serious risk of unforeseen consequences? Do you think the FCC appropriately took these into account? In your time at the FTC, how did you evaluate similar potential disruptions to consumer expectations and unequal application of consumer protections?

The FCC's proposal would substantially limit an ISP's ability to market its own products and services that are not "communications-related" to its own customers, including home security, energy management, and music streaming. That means consumers may not know about innovative or lower-priced offerings from which they would benefit. The FCC's NPRM does not provide an economic analysis, and its proposal does not appear to take these adverse consequences into account.

During my tenure at the FTC, we attempted to ensure that consumers had the opportunity to make informed choices about services and products, and that they knew about a breadth of alternatives. If a company failed to adequately inform consumers about the consequences of a product or service – or worse, deceived consumers – we would take action against that company. But ultimately, we believed in the ability of consumers to make choices themselves, and we believed that allowing such choices drives innovation, competition, and lower prices. That thinking seems absent in the "command and control" approach of the NPRM; as a result, it is more likely to harm than benefit the very consumers the FCC is supposed to serve.

The massive and unprecedented breadth of data covered by the FCC proposal threatens to harm consumers – and, potentially, basic Internet functionality and practices employed today – in ways known and unknown. It is not just ISPs that are saying this. The Internet Commerce Coalition, which includes edge providers, notes that the FCC proposal "covers a broad swath of information that is not in the least sensitive" and sweeps in "information that travels widely across the Internet whenever a user communicates." Parties with IT, network engineering, and security expertise express particular concern with regard to the FCC's proposal to restrict the use of IP addresses, device identifiers, domain information, and other data elements which cannot, on their own, identify specific persons, but which are basic elements of network engineering and operations. The FCC needs to take more time to fully examine a raft of complex technical issues that could have serious consequences for consumers' Internet experience.

⁵ *Id.*

FRED UPTON, MICHIGAN
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FOURTEENTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115
Majority (201-225-2927)
Minority (202-225-3641)

July 5, 2016

Mr. Paul Ohm
Professor of Law
Georgetown University Law Center
600 New Jersey Avenue, N.W.
Washington, DC 20001


Dear Mr. Ohm:

Thank you for appearing before the Subcommittee on Communications and Technology on Tuesday, June 14, 2016, to testify at the hearing entitled "FCC Overreach: Examining the Proposed Privacy Rules."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions with a transmittal letter by the close of business on Tuesday, July 19, 2016. Your responses should be mailed to Greg Watson, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to Greg.Watson@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Greg Watson
Chairman
Subcommittee on Communications and Technology

cc: Anna G. Eshoo, Ranking Member, Subcommittee on Communications and Technology

Attachment



GEORGETOWN LAW

Paul Ohm
Professor of Law

July 29, 2016

Chairman Greg Walden
Subcommittee on Communications and Technology
U.S. House of Representatives Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Walden,

Thank you for the opportunity to testify to the subcommittee on June 14, 2016. I truly appreciated the opportunity to share my thoughts with Members about the FCC's important proposal to protect the privacy of consumers of broadband Internet.

I also appreciate the additional questions for the record you have asked me. My answers follow. Please do not hesitate to let me know if you have any other questions for me.

Answers to Additional Questions for the Record

1. In your 2009 working paper titled, "The Rise and Fall of Invasive ISP Surveillance", you write that ISPs have "an amazingly pristine track record" when it comes to respecting consumer privacy. It appears from your testimony that you believe that they are, nonetheless, deserving of regulation to protect consumers. Could you give specific examples, other than the FTC's enforcement actions levied against ISPs, in which ISPs appear to have violated consumers' privacy, justifying your stance?

Answer: It is my great regret that this statement from seven years ago is no longer true. Although I hesitate to claim that there is an epidemic of reported violations of consumer privacy by ISPs, there is a worryingly long and growing list of examples I can point to. Simply put, ISPs seem to be abandoning their historical reticence to intrude into consumer privacy in ways that I find highly problematic. Let me give you three examples.

Example 1: Verizon Wireless and UIDH. In October 2014, researchers discovered that for two years Verizon Wireless had been injecting a unique tracking number, known as

a Unique Identifier Header or UIDH, into the private communications of its customers.¹ A unique identifier is like a fingerprint, which allows a user to be tracked as he or she moves around the web, and can actively subvert user efforts to preserve a modicum of privacy surrounding their online behavior.

For example, if a user follows standard consumer protection advice and clears his cookies from his browser, the UIDH will give any observer on the web the ability to completely undo this action, restoring whatever profile the user had attempted to clear. Because of the way a UIDH works, this power to subvert user wishes extends not only to Verizon Wireless and its business partners, but it is instantly available to *any* entity online that communicates with the user. Because of this user-expectation-defeating characteristic, researchers have referred to the UIDH as a “supercookie” or a “permacookie,” both terms that carry a significant negative connotation.²

There is even documented evidence (to be clear, not about this specific example) that non-commercial actors such as intelligence agencies exploit commercial unique identifiers to further their own surveillance activities.³ It is thus no exaggeration to say that the Verizon Wireless UIDH subverted the lawful efforts by citizens to protect their communications from tracking by domestic and international governments.

In my expert opinion, Verizon Wireless’s silent deployment of this technology without asking for consent represented a breach of online norms, a violation of technical edicts such as the end-to-end principle, and a potential violation of consumer protection laws.

This example also underscores the importance of Section 222, the very authority under which the FCC purports to promulgate the rule that was the subject of my testimony. After Verizon Wireless’s actions came to light, the FCC opened an investigation under the authority of Section 222. In March of this year, the FCC and Verizon Wireless reached a settlement in which the company agreed to obtain opt-in consent—the very form of consent proposed by the FCC its new rule—and to pay a fine of \$1.25 million.⁴

Example 2: CableOne’s use of FICO Scores. In May of this year, Thomas Might, the CEO of Cable One, revealed that his company takes a customer’s FICO score into account

¹ Robert McMillan, *Verizon’s ‘Perma-Cookie’ is a Privacy-Killing Machine*, WIRED, Oct. 27, 2014, <http://www.wired.com/2014/10/verizons-perma-cookie/>.

² See Craig Timberg, *Verizon, AT&T Track Their Users with ‘Supercookies’*, WASH POST, Nov. 3, 2014, available at http://www.washingtonpost.com/business/technology/verizon-atandt-tracking-their-users-with-supercookies/2014/11/03/7bbbf382-6395-11e4-bb14-4cfea1e742d5_story.html; Jacob Hoffman-Andrews, *Verizon Injecting Perma-Cookies to Track Mobile Customers, By-Passing Privacy Controls*, Electronic Frontier Foundation, November 3, 2014, available at <https://www.eff.org/deeplinks/2014/11/verizon-x-uidh>.

³ Ashkan Soltani, Andrea Peterson & Barton Gellman, *NSA Uses Google Cookies to Pinpoint Targets for Hacking*, WASH POST, Dec. 10, 2013, <https://www.washingtonpost.com/news/the-switch/wp/2013/12/10/nsa-uses-google-cookies-to-pinpoint-targets-for-hacking/>.

⁴ FCC, *Verizon Wireless to Pay \$1.25 million to Settle Investigation*, https://apps.fcc.gov/edocs_public/attachmatch/DOC-315501A1.pdf (July 31, 2012).

when deciding whether to provide adequate customer service.⁵ Speaking at an industry conference, Mr. Might explained that “We don’t turn people away,” but that they would not allow their support staff to “spend 15 minutes setting up an iPhone app” for a customer with a poor credit history. He defended this as a way to “pinpoint where churn and bad debt was coming from.”⁶

After receiving criticism from consumer advocates and policymakers, the company backtracked, contradicting its CEO in a letter to the FCC.⁷ In this letter, the company is reported to have explained that FICO scores are used to “determine the size of the deposit and the installation charge” but does not use it to later dole out customer service. Although the company characterized this letter as a clarification, it appears to flatly contradict the earlier revelation by the CEO, at the very least raising serious questions about whether this company has systematized the violation of customer privacy.

Example 3: DNS Hijacking. In the Swire Report, which has generated much commentary in this FCC proceeding, the authors describe the growing trend of users configuring their computers to send DNS directory lookup requests to an entity other than their ISP.⁸ The suggestion is that this is one other way market developments and user self-help has blinded ISPs to the traffic of their users. The report fails to mention many well-documented examples of ISPs embracing a questionable tactic known as “DNS Hijacking” to subvert this user choice and to restore visibility into a user’s browsing activity.⁹ Once again, this conduct violates well-established norms of appropriate online behavior as well as intrudes into user privacy.

The bottom line is that ISPs have demonstrated on multiple occasions that the restraint and respect for user privacy I complimented in 2009 has unfortunately dissipated in the intervening years. These developments justify the fear I expressed in that article, Congress’s prescient decision to treat telecommunications services as deserving of a sectoral privacy law in enacting Section 222, and the FCC’s proposal to enact this law in its proposed rule.

2. **You state that it is true that other online entities are beginning to rival BIAS providers with regard to the information they collect. You highlight social networking sites. Is it your contention that other parts of the online ecosystem like these should be more heavily regulated—sector specific—with regard to online privacy—yes or no?**

Yes.

⁵ Daniel Frankel, *Cable One using FICO Scores to Qualify Video Customers, Might Says*, FIERCECABLE, May 23, 2016, <http://www.fiercecable.com/story/cable-one-using-fico-scores-qualify-video-customers-might-says/2016-05-23>.

⁶ *Id.*

⁷ Daniel Frankel, *Cable One Clarifies FICO Score Usage with FCC, Says it has its own System for Determining Customer Value*, FIERCE CABLE, June 28, 2016, <http://www.fiercecable.com/story/cable-one-clarifies-fico-score-usage-fcc-says-it-has-its-own-system-determi/2016-06-28>.

⁸ Peter Swire, et al., *Online Privacy and ISPs* (May 2016).

⁹ Cade Metz, *Comcast Trials Domain Helper Service/DNS Hijacker*, THE REGISTER, July 28, 2009, http://www.theregister.co.uk/2009/07/28/comcast_dns_hijacker/.

To be clear, I am far from unusual in decrying the state of online privacy and elaborating the useful role that Congress can serve in addressing this problem. Survey after survey reveals that consumers are dissatisfied with the level of privacy they enjoy online as well as hopeful that their elected officials will enact smart, measured new laws to address these concerns.¹⁰

In addition, policymakers have agreed, calling for new privacy laws for online activity. The White House issued a widely hailed 2012 call for a “consumer privacy bill of rights,” specifically urging Congress to codify these rights in new legislation.¹¹ Successive Chairs of the FTC, together with FTC Commissioners from both parties have urged Congress to enact new comprehensive privacy and data security legislation.¹² To date, Congress has not enacted any laws in response to these calls.

To be more specific, Congress should enact a sectoral privacy law for entities that possess precise geolocation information. It should enact a sectoral privacy law limiting the use of facial recognition systems. It should enact a law to regulate the activities of data brokers. Wise and measured proposals on each of these topics have been proposed but unfortunately have languished in recent Congresses. I am happy to elaborate on my support for specific bills, if you would find it useful.

Thank you once again for giving me the opportunity to express my opinions about these vital issues. I truly admire the hard work and thoughtfulness with which your subcommittee has been engaging with this vital topic.

Sincerely,



Paul Ohm

¹⁰ Berkeley Law, Berkeley Consumer Privacy Survey, <https://www.law.berkeley.edu/research/bclt/research/privacy-at-bclt/berkeley-consumer-privacy-survey/> (series of studies); Pew Research, Online Privacy and Safety, <http://www.pewresearch.org/topics/privacy-and-safety/> (collecting studies).

¹¹ <https://www.whitehouse.gov/sites/default/files/privacy-final.pdf>.

¹² E.g., https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-balancing-privacy-and-innovation-does-presidents/120329privacytestimony.pdf; http://www.americanbar.org/news/abanews/aba-news-archives/2015/02/ftc_chair_edith_rami.html.

FRED UPTON, MICHIGAN
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FOURTEENTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115
Majority (202) 225-2927
Minority (202) 225-3641

July 5, 2016

Mr. Doug Brake
Telecom Policy Analyst
Information Technology and Innovation Foundation
1101 K Street, N.W.
Washington, DC 20005


Dear Mr. Brake:

Thank you for appearing before the Subcommittee on Communications and Technology on Tuesday, June 14, 2016, to testify at the hearing entitled "FCC Overreach: Examining the Proposed Privacy Rules."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions with a transmittal letter by the close of business on Tuesday, July 19, 2016. Your responses should be mailed to Greg Watson, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to Greg.Watson@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Greg Walden
Chairman
Subcommittee on Communications and Technology

cc: Anna G. Eshoo, Ranking Member, Subcommittee on Communications and Technology

Attachment



July 21, 2016

Communications and Technology Subcommittee Chairman Greg Walden
c/o Greg Watson, Legislative Clerk
Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515

Thank you again for the opportunity to share my views on the Federal Communications Commission's (FCC) proposed privacy rules with the subcommittee at the June 14, 2016, hearing entitled "FCC Overreach: Examining the Proposed Privacy Rules." Please accept my answers below to the additional questions for the record.

The Honorable Adam Kinzinger

1. Mr. Brake, you acknowledge the only other examples of sector-specific privacy regulations exist when there is a heightened risk of disclosure of sensitive personal information, which are financial and healthcare services. What evidence or reason did the FCC have when proposing these rules to a specific sector of the internet ecosystem?

While I am certainly not familiar with all of the factors that lead the FCC to propose the rules that it did, a charitable interpretation of its actions would recognize three main points.

First, the FCC privacy proposal mirrors the legacy section 222 regulations as they were applied to telephone networks. In that context, the FCC used the same three-tier consent framework. This would conceivably make the rules easier to defend in court. In the privacy notice of proposed rulemaking (NPRM), the FCC put it simply: "we propose to apply the traditional privacy requirements of the Communications Act to the most significant communications technology of today."¹ But I see this assertion from the FCC as self-indicting: when it comes to broadband Internet—the "most significant communications technology of today"—we should take care to regulate in a way that does not limit its growth or potential for innovation, not simply import rules written in the mid-1990s, for a different and altogether simpler type of network. Moreover, the legacy section 222 rules were explicitly a tool to facilitate competition in the provision of telephone services—

¹ FCC, *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Notice of Proposed Rulemaking, WC Docket No. 16-106 (Apr. 2016), at 2, available at https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-39A1.pdf.

not for privacy. When crafting competition regulations in a market a regulator is trying to open to competition, it makes sense to make narrow, specific rules. The Internet, on the other hand, is incredibly dynamic and complex, with competition expanding across traditional industry sectors. In regulating here, an ethos of “do no harm” should guide the Commission: better to hew close to the established Federal Trade Commission framework that successfully oversaw privacy practices of the broadband industry up until Title II common carrier classification.

Second is the “choice” argument. The FCC points to the fact that once a user is connected to a broadband service, he or she cannot avoid the network in the same way one can choose from the variety of websites or edge services. I think this argument is misleading for a number of reasons. First of all, the FCC has understated the number of choices most consumers have for broadband providers. By considering only connections of 25 Mbps or higher as broadband (by this measure South Korea is the only country in the world that makes “broadband” available to the majority of its citizens), the FCC paints a distorted picture of broadband choice. But more importantly, this “choice” argument does not justify the heightened privacy rules proposed. Every major broadband provider already offers customers an opportunity to opt out of targeted advertising programs—when privacy-sensitive customers can simply opt out, there is no need to switch ISPs to find the privacy policy one likes. An opt-out should offer consumers sufficient choice to protect their privacy, and better balances that legitimate interest with the benefits that flow from increased sources of data to fuel our information-based economy.

The third reason the FCC has given for heightened rules is the position of ISPs as a conduit for all information a consumer accesses online. I think this does not do the work the FCC requires of it, for the reasons outlined in my answer to your second question below.

2. Mr. Brake, at the recent Senate hearing on privacy, Chairman Wheeler attempted to contrast what an ISP can collect from its customers with what a website can collect. The FCC Chairman asserted that “Only one entity connects *all* of that information...and can turn around and monetize it.” He also claimed that when an individual goes to a website to enter information, that it is the consumer’s choice and only that website receives and is able to use that information. That seems to be an incorrect assessment of how consumer data is collected on the Internet, and who is engaged in such collection. Do you agree with Chairman Wheeler’s description and analysis?

I believe Chairman Wheeler has significantly overstated how much information an ISP can collect, and

detailed just this point in an op-ed titled “The FCC’s Privacy Ruse.”² Professor Peter Swire’s much-discussed report outlines many of the reasons ISPs have limited access to information—most notably the remarkable uptake in encryption that limits ISP access to content of electronic communications, the small but growing use of virtual private networks and other proxy services, as well as consumers’ use of multiple networks throughout the day.³

The Honorable Gus Bilirakis

1. Mr. Brake, you make an interesting point about how this overreaching shift against ISPs will narrow the businesses down to one of pure transport. Can you expound a little about the effect on future innovation and the handcuffing of job creation that might result from this?

I very much view the proposed rules as designed more to constrain business models of ISPs than to protect consumer privacy. And the proposed privacy rules are only one step in the broader imposition of Title II common carrier regulations imposed by the FCC. Populist activists would like to see the FCC go even further and impose price regulations or even unbundling elements of the network in the name of superficial, service-based competition. This line of reasoning wrongly views the applications and services riding on top of the Internet as the only source of dynamic innovation—they prefer broadband providers as a simple dumb pipe to access the Internet, and turn a blind eye to the innovation and investment required to make abundant bandwidth available throughout America. The key to taking us off this path is an alternative legal authority for baseline net neutrality rules other than Title II of the Communications Act. I commend this subcommittee’s work in considering an update to the Communications Act, and hope the next session presents an opportunity to continue that effort.

Sincerely,

Doug Brake
Telecommunications Policy Analyst
Information Technology and Innovation Foundation

² Doug Brake, “The FCC’s Privacy Ruse,” *Forbes Opinion* (Apr. 2016)
<http://www.forbes.com/sites/realspin/2016/04/27/the-fccs-privacy-ruse/#2d1f224710aa>.

³ Peter Swire, et al., *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others* (Feb. 29, 2016), available at <http://b.gatech.edu/IRIWXUa>.