S. HRG. 114–564

HOW WILL THE FCC'S PROPOSED PRIVACY REGULATIONS AFFECT CONSUMERS AND COMPETITION?

HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

JULY 12, 2016

Printed for the use of the Committee on Commerce, Science, and Transportation

U.S. GOVERNMENT PUBLISHING OFFICE

24–204 PDF WASHINGTON : 2017

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

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

JOHN THUNE, South Dakota, *Chairman*

ROGER F. WICKER, Mississippi
ROY BLUNT, Missouri
MARCO RUBIO, Florida
KELLY AYOTTE, New Hampshire
TED CRUZ, Texas
DEB FISCHER, Nebraska
JERRY MORAN, Kansas
DAN SULLIVAN, Alaska
RON JOHNSON, Wisconsin
DEAN HELLER, Nevada
CORY GARDNER, Colorado
STEVE DAINES, Montana

BILL NELSON, Florida, *Ranking*
MARIA CANTWELL, Washington
CLAIRE MCCASKILL, Missouri
AMY KLOBUCHAR, Minnesota
RICHARD BLUMENTHAL, Connecticut
BRIAN SCHATZ, Hawaii
EDWARD MARKEY, Massachusetts
CORY BOOKER, New Jersey
TOM UDALL, New Mexico
JOE MANCHIN III, West Virginia
GARY PETERS, Michigan

NICK ROSSI, *Staff Director*
ADRIAN ARNAKIS, *Deputy Staff Director*
REBECCA SEIDEL, *General Counsel*
JASON VAN BEEK, *Deputy General Counsel*
KIM LIPSKY, *Democratic Staff Director*
CHRIS DAY, *Democratic Deputy Staff Director*
CLINT ODOM, *Democratic General Counsel and Policy Director*

CONTENTS

WITNESSES

APPENDIX

HOW WILL THE FCC'S PROPOSED PRIVACY REGULATIONS AFFECT CONSUMERS AND COMPETITION?

TUESDAY, JULY 12, 2016

U.S. SENATE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Committee met, pursuant to notice, at 10:04 a.m. in room SR–253, Russell Senate Office Building, Hon. John Thune, Chairman of the Committee, presiding.

Present: Senators Thune [presiding], Nelson, Cantwell, Blunt, Rubio, Klobuchar, Ayotte, Blumenthal, Heller, Schatz, Markey, Fischer, Sullivan, Moran, Manchin, Johnson, Peters, Gardner, and Daines.

OPENING STATEMENT OF HON. JOHN THUNE, U.S. SENATOR FROM SOUTH DAKOTA

The CHAIRMAN. Good morning. This hearing will come to order.

The protection of privacy on the Internet is vital. Protection from identity theft, protection from deeply private information: this is important to us as citizens and as consumers, and it's fundamental for allowing the Internet and the information economy to thrive, and thrive they have.

Internet usage has increased 900,000 percent since the Telecom Act of 1996, and to meet that demand, the broadband industry has invested $1.4 trillion. This growth occurred under the Federal Communications Commission's light regulatory treatment of the Internet as an information service, and under the careful eye of the Federal Trade Commission, which, with limited exceptions, was responsible for protecting consumer privacy on the Internet. The FTC has brought over 500 cases protecting the privacy and security of consumer information, including cases where companies were alleged to have deceptively tracked consumers online or to have shared privacy consumer data with unauthorized third parties.

The FTC has been the leader in protecting consumer privacy, but with the FCC's 2015 Open Internet Order, all of that changed. Broadband Internet Access Service, or BIAS, was reclassified as a telecommunications service, which, in turn, meant the FTC lost its jurisdiction over the privacy policies of BIAS providers.

So now, after having forced the FTC off the field for broadband providers, the FCC has proposed a novel regulatory scheme for the newly reclassified providers. But the FCC's rules would apply only to certain parts of the Internet, and that is a source of significant

concern. Both the Obama administration and the FTC have endorsed a consistent privacy regime across the digital landscape. Indeed, the FTC staff filed comments with the Commission stating, "The FCC's proposed rules, if implemented, would impose a number of specific requirements on the provision of BIAS services that would not generally apply to other services that collect and use significant amounts of consumer data. This outcome is not optimal."

For those of you not familiar with bureaucrat-speak, let me tell you this, when they say, "this outcome is not optimal," it's pretty strong stuff for one agency to say about another.

I share the FTC's concern, and by overwhelming majority, so do the American people. Progressive Policy Institute polling shows that 94 percent of Internet users believe that all 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.

I am concerned that at any particular time consumers will not have reasonable certainty of what the rules are and how their privacy decisions apply. At home on Wi-Fi? At home on a smartphone? Using your smartphone on a friend's Wi-Fi? Using the Internet at a library? Each of these could have very different privacy implications for a consumer because of the FCC's proposed piecemeal approach to privacy.

There are other problems for consumers as well. Will the Commission's proposed rules make it more or less likely that BIAS providers will be able to provide better and more innovative services that could benefit consumers? And of particular importance to our rural communities, how are small BIAS providers going to be able to comply with the Commission's proposed regulations? Most of the rural carriers in South Dakota have between 2,000 and 5,000 broadband subscribers. How are they supposed to pay for the additional staff, software licenses, training, and other expenses that would be required to comply with the Commission's proposed rules?

The FCC's push for a separate regulatory scheme for BIAS providers is based in significant part on their claim that ISPs are the most important and extensive conduits of consumer information, and thus have access to very sensitive and very personal information. I am not so sure about that. It appears that many companies that are not broadband providers have access to information about consumers that is more personal and more sensitive than much of what ISPs can access, yet those entities are not covered by the Commission's proposal.

Is the FCC, which is a novice when it comes to regulating Internet privacy, the right agency to protect us from identity theft and to protect our private information? Do we want to have inconsistent privacy protection for consumers, with distinctions based upon how the Commission chooses to classify services under the Communications Act, an act that never envisioned the FCC dealing with online privacy or cybersecurity? Would consumers and companies be better off with the FCC's proposal?

The witnesses we have before us today represent a broad variety of backgrounds and are true experts on these issues. And I look forward to your answers to these and other questions that you are asked here today.

With that, I would yield to our distinguished Ranking Member, the Senator from Florida, Senator Nelson, for an opening statement.

STATEMENT OF HON. BILL NELSON,
U.S. SENATOR FROM FLORIDA

Senator NELSON. Thank you, Mr. Chairman.

If we all share the same goal of how to best protect consumer online privacy, then it seems that we are bifurcated in our approach to this because in looking at the FCC's proposed privacy rules, both sides of the debate come at these questions with preconceived notions about how best to achieve this goal. On the one side, we are told that the FCC should not be adopting any rules for broadband providers because we are not also applying those same rules to every online player. On the other side, we're told that the FCC should adopt the most stringent rules possible in order to prohibit broadband providers from using any consumer data.

Well, it seems to me that the question is ultimately how to preserve the benefits of online commerce, but in a way that takes into account consumers' right to know about and, when appropriate, control the collection and use of their personal information. So putting aside the claims of regulatory overreach or power grabs, isn't it clear the FCC is the expert agency for regulating communications networks, including broadband networks? It is an expert oversight agency with flexible forward-looking authority to protect consumers.

If the content is governed by the FTC under the fair and deceptive practices standard, isn't it right for the FCC, as it has over the past several years and as I have pushed, to also use its authority to protect privacy? We need regulators who are not afraid to use their authority when necessary, to protect consumer privacy, but also we need the regulators to know when to exercise that authority in a restrained manner.

Now, this is a difficult balance, but that doesn't mean that an agency should defer or otherwise be reluctant to do what it believes is in the best interest of protecting consumers. The FCC is still in the middle of a rulemaking to sort all of this out.

Thank you, Mr. Chairman, for calling this hearing so that we can hear all the attitudes about the FCC's proposals and alternative approaches, but at the end of the day, I can tell you this Senator is going to side with the consumers in whichever approach that I can conclude best protects the privacy of broadband subscribers.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Nelson.

We've got a great panel today to hopefully shed some light on this subject. And on my left and your right is Mr. Jon Leibowitz, a Partner at Davis, Polk & Wardwell, and a Co-Chair of the 21st Century Privacy Coalition. He is also a former Chairman of the Federal Trade Commission.

Next to him is Mr. Dean Garfield, who is the President and CEO of the Information Technology Industry Council.

Professor Paul Ohm of Georgetown University Law Center.

And Mr. Matthew Polka. He is the President and CEO of the American Cable Association.

And Professor Peter Swine [sic], the Huang Professor of Law and Ethics for the Scheller College of Business at the Georgia Institute of Technology.

We're delighted to have all of you with us today. Thank you for being here. We look forward to hearing from you and asking you some questions. And we'll start, as I said, on my left, and your right, with Mr. Leibowitz. So please proceed with your remarks. And if you could all confine it as close to possible with 5 minutes, we would very much appreciate it.

Thank you.

STATEMENT OF HON. JON LEIBOWITZ, PARTNER, DAVIS, POLK & WARDWELL AND CO-CHAIRMAN, 21ST CENTURY PRIVACY COALITION

Mr. LEIBOWITZ. Thank you, Chairman Thune, Senator Nelson, other distinguished members of the Committee. I appreciate you inviting me to testify today on behalf of the 21st Century Privacy Coalition, which I chair with former Representative Mary Bono.

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 Obama administration has endorsed and the FTC has taken in decades, as you know, of robust privacy enforcement.

The FTC has held hundreds of companies, large and small, accountable for breaking their privacy commitments to consumers, and by taking a largely enforcement-based approach rather than setting out prescriptive rules, the FTC has powerfully protected privacy while permitting the type of high-tech innovation that has yielded huge benefits to all Americans. And when the FTC has done a rulemaking—so think about Do Not Call or the Children's Online Privacy Protection Act, as Senator Klobuchar and Senator Markey know, they have been successful. Indeed, the FTC approach has been so successful that in 2012 the White House called on the FTC to be solely responsible for protecting the privacy of every American across every industry, and that, of course, includes ISPs.

As we know, last year the FTC's sister agency, the FCC, reclassified Internet service providers as common carriers, as part of the Open Internet Order. That decision removed ISPs from the FTC's jurisdiction. Having assumed sole jurisdiction to protect privacy among broadband users, the FCC is reasonably engaged in rulemaking. After all, we want to have a cop on the beat. And 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 private report in mind.

But the FCC's proposed rules, as currently drafted, are very different from FTC practice and policy. Instead, the proposed rules impose a restrictive set of requirements on broadband providers that don't apply to other entities that collect much or more con-

sumer online data. The ISP's specific rules don't provide clear benefits to consumers, they don't protect privacy in the way that they should, they may themselves be unconstitutional, and more troubling, or at least as troubling, these restrictive requirements represent a fundamental change in the U.S. approach to privacy, a change that should not be made lightly or without the input of all stakeholders. Indeed, the FCC has not identified any consumer harms that warrant a vast departure from the FTC's successful approach.

So the goals may be laudable, I have no doubt they are, but the draft rules betray a fundamental lack of understanding regarding how the Internet ecosystem works. Indeed, the FCC's proposed rules may well discourage the very broadband innovation that the FCC is statutorily obligated to promote, thereby harming the very consumers it's 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 by doing so, diminish broadband providers as a potential competitive force to benefit consumers.

Second, the FCC's proposal would impose opt-in consent requirements for non-sensitive data and basic everyday business practices, like first-party marketing. For example, an ISP, absent an opt-in consent, would be prohibited from marketing its own home security, music streaming, or energy management services to its own customers using its own customer lists, that makes no sense at all, nor would prohibiting a typical working-class family of four from accepting a discount in exchange for an ISP using customer information, even if that information isn't shared with anybody else. Consumers should be able to make their own choices as long as they are informed choices. Choice is really supposed to be what the Internet is about.

Third, the NPRM, as drafted, would miss the opportunity to create consumer benefits from de-identified data.

And, fourth, the proposal would impose an unrealistic timeline for breach notification and mandate massive overnotification that could cause consumers to ignore truly important messages from their ISP or from others.

And don't take my word for it, as you pointed out, Senator Thune, my former agency, the FTC, has referred to aspects of the NPRM as, "not optimal." In the FTC's comments on the FCC proposal, comment to the FCC, there are 28 separate instances where the FTC raises concerns about the FCC's approach.

If I could make one suggestion to the FCC, it would be this: listen to the FTC and consider whether the FCC proposal is in tension with the U.S. successful NIST cybersecurity framework or could undermine the EU-U.S. Privacy Shield as it works its way through the European Parliament.

Mr. Chairman, I ask for an additional 30 seconds and then I will end. Thank you.

But with that said, let me make one last point: Final rules are often more balanced than proposed ones. I think you made this point, Senator Nelson. We may see a lot of improvement when the NPRM moves to completion. But even if you don't believe the

FCC's current proposal is a solution in search of a problem, it would nevertheless create inconsistent standards across the Internet, confuse consumers, and undermine innovation that benefits consumers as well. And there are serious questions about whether it would withstand constitutional scrutiny.

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, a privacy framework that has largely been embraced by the Obama administration.

Thank you. I'm happy to answer questions.

[The prepared statement of Mr. Leibowitz follows:]

PREPARED STATEMENT OF HON. JON LEIBOWITZ, PARTNER, DAVIS, POLK & WARDWELL AND CO-CHAIRMAN, 21ST CENTURY PRIVACY COALITION

Chairman Thune, Ranking Member Nelson, other distinguished Members of the Committee, 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 that consumers have a clear notion of how their data is being used and shared, and what is being done to protect their data from hackers and other bad actors. 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 over the privacy practices of ISPs, 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, "Protecting Consumer Privacy in an Era of Rapid Change:" 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. This would protect consumers while continuing to facilitate and encourage innovation and competition on the Internet.

Such an approach also would better reflect the privacy and data security principles promoted by the Obama Administration after extensive research and outreach to stakeholders. In its 2012 Report "Consumer Data Privacy In a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy," the Administration advocated for "a level playing field for companies, a consistent set of expectations for consumers, and greater clarity and transparency." Moreover, the Report also recognizes that most first-party marketing is consistent with the context of the provider-consumer relationship, and that "[c]ompanies should be able to infer consumer consent to collect personal data for these limited purposes." And the Report encourages companies to develop privacy protections based upon the "sensitivity of the personal data that they collect, use, or disclose." In addition, the National Institute of Standards and Technology ("NIST") Cybersecurity Framework has been highly lauded as an effective means of fostering increased security across a multiplicity of industries by placing a priority on risk management and flexible standards, rather than prescriptive and inflexible *a priori* rules.

Unfortunately, while some parts of the FCC's proposed rules are consistent with the Obama Administration and FTC approach, in many important areas the rules deviate sharply from that approach, demonstrating both the FCC's lack of experience in the privacy area, and its failure to fully consider and test the likely impact

of its proposed rule on consumers and ISPs alike during the course of its drafting process. Thus, we agree that, as the FTC noted, the FCC's approach is "not optimal."

The FCC has proposed regulations for ISPs 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, which bears little to no resemblance to the traditional voice services market that the FCC has regulated under its Title II authority. In addition, it is inapposite to attempt to analogize the ISP industry to banks or health-care companies to which sector-specific laws apply. Online data is collected and exchanged by many entities other than ISPs.

In the Internet ecosystem, myriad entities have access to and use consumers' online information to provide customers free, 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. Unfortunately, the FCC's proposed rules will make it much harder for ISPs to deliver these benefits, particularly compared to other online entities. For example, the NPRM would restrict consumer choice by prohibiting efforts by ISPs to promote broadband access by offering discounted service in exchange for targeted marketing. Thus, if enacted in its current form, the NPRM would harm, rather than benefit, consumers.

In fact, ISPs are new entrants in the online advertising market, where ten companies, none of which are ISPs, hold over seventy percent of the market. The proposed rules would curtail ISPs' ability to enter that market and provide sorely needed competition. Under a reasonable reading of proposed rules set forth in the NPRM, ISPs would not be able to market their own non-communication-related products—like cloud services, music streaming, or a home security system—to their own customers without such customers' prior opt-in consent. The FCC must avoid an outcome in which ISP marketing practices that are clearly consistent with consumer expectations are restricted in a way that undermines consumer choice and eliminates opportunities for consumers to save money on products offered by an existing service provider. These marketing restrictions are also inconsistent with marketing laws already on the books—including CAN–SPAM and Do-Not-Call—in which Congress struck a balance between privacy and the dissemination of information to consumers by setting up opt-out regimes.

Moreover, the proposed rules threaten to create not only consumer confusion, but also frustration and disruption of their online experiences. In a recent survey published by the Progressive Policy Institute, 94 percent of consumers agreed 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 U.S. international privacy negotiations. As the Obama Administration and FTC have long recognized, 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 online innovation and competition to continue to flourish. The FCC's approach, as currently drafted, fails to achieve these important goals. This is an outcome that the FCC should abandon before adopting final rules.

Further, the FCC's approach suffers from multiple constitutional infirmities and is unlikely to withstand court scrutiny. Rather than embark on such an approach just to be rebuked by the courts, the FCC should redraft its proposal to take into consideration the FTC's successful approach to privacy and to respect the constitutional boundaries of the FCC's authority.

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 to ensure that consumers continue to benefit from the high-tech innovation and competition that has revolutionized modern life. As consumers 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 500 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, 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 FTC's 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: Even after thoroughly studying the data collection and use practices of ISPs and other large platform providers, the FTC concluded that "[a]ny 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 ISPs, but also social networks, operating systems, browsers, and advertising platforms—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 in the FCC's privacy proceeding, based largely on its 2012 Privacy Report, were unanimously supported by all three sitting commissioners. There is more enduring impact, and often more legitimacy, 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. And certain specific proposals in the NPRM are also consistent with the FTC approach. For example, 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 on the FCC's proposal, "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 technology neutral treatment of ISPs under the same set of standards applicable throughout the Internet ecosystem. 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 FCC should recognize the FTC's experience and heed the latter's concerns with the NPRM.

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 as well as 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 a sweeping range of information that is not sensitive, such as IP and MAC addresses, as well as any other information that is "linked or linkable to" a user or device. 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. For example, as discussed below the proposed breach notification rules would require ISPs to notify consumers if there is an incident in which IP addresses are compromised. Because IP addresses on their own cannot be used to identify, let alone contact, an individual, the proposed rule would force ISPs to associate IP addresses with appropriate customer contact information to comply, increasing the likelihood that any incident results in the release of information that could be used to harm consumers. But both the Administration and FTC policies encourage providers to dissociate such data to minimize the potentially harmful effects of any security incident.

Finally, by including broad categories of non-sensitive data within the scope of the NPRM's definition of customer proprietary information, the FCC invites irrational outcomes by placing burdensome requirements on ISPs that serve no discernible consumer privacy interest. For example, under a reasonable reading of the rule, ISPs must provide notice of data breaches to law enforcement and customers even *under circumstances where there is no risk of harm to consumers.* ISPs would also

be prohibited from using their own customer lists to e-mail consumers about their own non-communications-related products and services.

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 ISPs, 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 percent will be encrypted by the end of this year. This sea change in only four years 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. Unfortunately, the NPRM seems to be unaware of marketplace developments in the last several years as well as the harms caused by a bi-furcated privacy framework.

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." In particular, the FTC has never considered all web address information to be sensitive. Such a conclusion would have major implications for the entire Internet ecosystem.

The FCC's proposed restrictive choice mandates that selectively target ISPs prevent consumers from accessing new products and services and potentially confuse them, but provide no benefits to consumers. They also constrain ISPs' ability to compete with edge providers, and likely will 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. As the FTC commented "[o]pt-in consent should be required for use and sharing of contents of consumer communications and sensitive data for purposes other than those for which consent is implied." The Administration's 2012 report, also recognizes that "companies may infer consent to use personal data to conduct marketing in the context of most first-party relationships." 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. According to the FTC, "[o]pt-out is sufficient for use and sharing of non-sensitive data." 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 ISPs 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. The notion that a bright-line opt-in requirement should apply to the collection of online information would represent a wholesale revision of U.S. privacy laws and would risk harm to the overall health of the Internet by constraining the beneficial use of data.

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. It 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 the proposed rules, an ISP would likely 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, and, indeed, with the significant benefits consumers have received from lower bundled prices and innovative new offerings for many years.

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. But consumers presented with an opt-in notice are likely to choose the path of least resistance. That is, many consumers will click "no" to avoid devoting time and energy to understanding an opt-in request. However, when opt-in requirements are the rule rather than the exception, and consumers take this approach in aggregate, everyone loses out on the benefits of reduced-cost or free products and services subsidized by the effective monetization of online data. While ISPs rely primarily on subscription fees, limiting their ability to effectively use customer data in turn limits a potential avenue for reducing the cost of broadband Internet access to consumers. Consistent with the FTC's technology-neutral approach, ISPs 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 consent mechanisms would unduly restrict ISPs 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 ISPs from offering discounted services in exchange for being able to offer targeted marketing. Many of us may decide that the price to pay to avoid personalized marketing is worthwhile, and so long as ISPs provide sufficient information to enable an informed choice, consumers themselves should be able to choose how to value their own privacy. The FCC should not interfere with consumer choice.

The application of a broad opt-in requirement 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 any clear benefits to consumers or identifying harms it is trying to address. Rather than pay lip service to the FTC's well-tested approach to privacy, the FCC should actually heed the FTC's advice and harmonize the former's privacy regime with the latter's.

Data Security and Breach Notification

The FCC's proposed data security provisions, requiring ISPs 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 NIST 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. Specifically, the FCC should replace its strict liability data security standard with a reasonableness standard. 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 ISPs 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 any 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 rules, 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.'" The NPRM states that the FCC intends to avoid this outcome, but major changes are required to the breach notification provision to achieve this goal. Otherwise, the FCC will jeopardize, rather than enhance, data security.

The proposed rules also contain an unrealistic timeline for customer notification, requiring ISPs to notify customers of a breach no later than ten days after the discovery of a breach. 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.

Constitutional Flaws In the FCC's Proposal

Fundamentally, the NPRM's requirements would impose a substantial burden on speech because they would preclude ISPs from engaging in important and relatively routine communications with their customers. As discussed above, the NPRM would impose an opt-in consent requirement for the use or sharing of information, including non-sensitive information, by ISPs and their affiliates to market a broad category of non-communications related services. While this requirement is also the wrong policy outcome, it 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." Harvard Professor Laurence H. Tribe has concluded that the NPRM fails on each prong of the *Central Hudson* test.[1]

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, myriad edge providers will continue to collect and share the same type of consumer information. As Professor Swire notes in his testimony, edge providers often collect more consumer information than ISPs and the former represent the dominant players in the online advertising market. 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 has concluded that the NPRM's proposed opt-in rule is not narrowly tailored because a less obtrusive opt-out rule

[1] 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/default-source/defaultdocument-library/ctia-ncta-ust-file-tribe-paper.pdf.*

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 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)[2] 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.

Conclusion

Mr. Chairman, thank you for holding this hearing today. Our Coalition commends you and Senator Nelson for devoting the Committee'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, practical policy goals.

In reviewing the record in the FCC's privacy proceeding, the breadth and depth of the objections to the proposed rules are striking. A diverse set of parties, ranging from civil rights groups, academics, researchers, security specialists, start-ups, advertisers, ISPs, equipment companies, software providers, IT providers, edge entities, and other Federal agencies all raise important and substantive concerns about key features of the FCC's proposal. Indeed, separate and apart from ISP objections to the FCC's proposal, there is very little support in the record for these rules from any entity that is in any way involved in network operations, management or security, or otherwise involved—either as an ISP or an edge provider—in providing services to broadband consumers. The FCC's proposal is so troubling that a number of parties that are clearly outside the scope of the proposed rules (as well as competitors in the marketplace) nonetheless felt compelled to submit comments due to the proposal's potentially disruptive effects on the Internet ecosystem as a whole. I think this is something that should give policy-makers—both here and at the FCC—pause. And it certainly counsels against rushing ahead to adopt an entirely new set of rules that depart so dramatically from the proven and effective FTC framework that governed ISPs online activities prior to reclassification.

As the FCC formalizes its privacy and data security rules, the agency should hold ISPs 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 has been 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. The NPRM is of questionable constitutionality and does not reflect a reasoned approach to consumer privacy. For all these reasons, the 21st Century Privacy Coalition's view is that the FCC should ensure that any rules it adopts hew closely to the FTC's time-tested and proven approach, which is consistent with the Obama Administration's approach to privacy and data security, and abandon its overly prescriptive, asymmetric rules.

The CHAIRMAN. Thank you, Mr. Leibowitz.
Mr. Garfield.

---

[2] *Id.*

STATEMENT OF DEAN C. GARFIELD, PRESIDENT AND CEO, INFORMATION TECHNOLOGY INDUSTRY COUNCIL (ITI)

Mr. GARFIELD. Good morning. Chairman Thune, Ranking Member Nelson, members of the Committee, on behalf of 60 of the most dynamic and innovative companies in the world, we thank you for inviting us to present at this hearing.

This hearing is both timely and important. The companies that we represent that are members of ITI reflect the full cross-section of the tech sector, from servers to software and service, from social media to search. Those companies do not fall within the ambit of the FCC's Open Internet Order and so are not covered by the proposed rules.

We are not here to choose sides between distinct regulatory agencies. Instead, what we present is our perspective on how to ensure that this vibrant ecosystem remains innovative and vibrant. I've submitted my testimony for the record, so rather than repeat it, I would like to hone in on three things: one, our perspective on privacy and cybersecurity; two, our views on the flaws of the FCC's approach; and, third, a path forward.

I've chosen to focus on privacy and cybersecurity first because for our companies, they are first principles that are foundational. No two issues are more important to building and retaining trust with our customers, and we treat them accordingly. Privacy and security, by design, are not catchphrases in the tech sector, they're truly reflective of the commitment we place on privacy and security from the design phase to the delivery.

The commitment of our companies to privacy and security is complemented by a rich, robust, well-developed privacy ecosystem that works. Jon alluded to much of it. In addition to the work of our companies, we have self-regulatory standards. We have the enforcement from the FTC and State attorney generals and, importantly, constant and consistent feedback from our companies that help to inform the approach that we take. The problem with the FCC's approach is that it parachutes into this rich, robust, well-developed ecosystem and assumes that it needs to rework all of the rules whole cloth. That presumption is faulty. For example, as Jon noted, the definition of PII is uniquely broad and bolts onto it a binary and rigid framework that's likely to prove unworkable. As well, around consent and choice, the FCC proposes an opt-in approach and to put its fingers on the thumb of the scale with no evidence that it's likely to work more effectively for consumers.

The FCC takes the same approach on cybersecurity, where rather than following the leadership of the experts at NIST, that have focused on a risk-based approach that's grounded in standard global standards, it instead adopts an approach that's mechanical and focused on mandates. The rules, or the proposed rules, around data breach are reflective of that. There is little evidence that the approach proposed by the FCC will be more workable, and it's completely inconsistent with the approach that's being taken at the state level today.

Our suggestion, or my testimony, should not be read to suggest that the FCC does not have a role here. Senator Nelson, the point you made resonates. We do not intend to suggest that the FCC's evaluation of these issues and attempt to find resolution of them

is mistaken. What we intend to suggest is that the approach that they've taken is one that's inconsistent with best practices and what we know works.

And so what we suggest as a path forward is that the FCC should take on board the comments that it's receiving, revise the existing NPRM to one that's more consistent with the well-established privacy and security framework that exists today, largely guided by the FTC and NIST, and then come back with further comments so that we end up with something and rules in place that will help to advance the innovation ecosystem rather than to stymie them.

I see that I have a few minutes remaining. I would just like to really thank the folks who are sitting behind me who are responsible for this testimony. My comments are really an embodiment of the thoughts that they've helped us to develop.

Thank you.

[The prepared statement of Mr. Garfield follows:]

PREPARED STATEMENT OF DEAN C. GARFIELD, PRESIDENT AND CEO, INFORMATION TECHNOLOGY INDUSTRY COUNCIL (ITI)

Chairman Thune, Ranking Member Nelson, and members of the Committee, thank you for the opportunity to testify today. I am Dean Garfield, President and CEO of the Information Technology Industry Council (ITI), and I am pleased to testify before your committee today on the important topic of how the Federal Communications Commission's (FCC or the "Commission") proposed broadband privacy regulations could impact consumers and competition.[1]

ITI shares the Commission's interest in, and respects its efforts to, protect the privacy of consumers of broadband Internet access services. Privacy is of paramount concern to our member companies, many of whom are providers of information technology and Internet services, because it is at the core of the trust relationship with our customers. Though the FCC lacks the authority to regulate our member companies who are the "edge providers" of "over the top" internet-based services referred to in its Notice of Proposed Rulemaking ("NPRM"), we are nonetheless concerned with the approach taken by the Commission in a number of respects. We therefore welcome your interest and engagement on this subject.

ITI is the global voice of the tech sector. We are the premier advocate and thought leader in the United States and around the world for the information and communications technology (ICT) industry, and this year we are pleased to be commemorating our centennial. ITI represents 61 of the world's leading ICT companies,[2] and we advocate globally for policies that advance U.S. leadership in technology, promote innovation, open access to new and emerging markets, protect and enhance consumer choice, and foster increased global competition. ITI's members comprise leading technology and innovation companies from all corners of the ICT sector, as well as companies using technology to fundamentally evolve their businesses, including wireless and wireline network equipment providers, computer hardware and software companies, mobile computing and communications device manufactures, Internet and digital service providers, and network security providers. ITI's member companies are also at the forefront of developing next-generation wireless communications equipment, infrastructure, networks, and services, along with the content, applications, and new uses that will be enhanced as mobile service evolves and advances. In other words, many of our members are the "edge providers" referred to in the FCC's proposal.

Privacy is of paramount concern to our member companies. Protecting our customers' personally identifiable information (PII) and their privacy, along with providing robust security, are essential to earning citizens' trust in the global technology marketplace. Innovating to protect privacy and security and to strengthen consumers' trust in the global digital infrastructure and Internet services are core

[1] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services,* WC Docket No. 16–106, Notice of Proposed Rulemaking, FCC 15–138 (April 1, 2016) ("Broadband Privacy NPRM").

[2] For more information on ITI, including a list of its member companies, please visit: *http://www.itic.org/about/member-companies.dot.*

to our companies' business practices and philosophies. Privacy is thus critical to our members' success, an essential component of our businesses, and impacts our ability to grow and innovate in a future heralding continued advances in the Internet of Things, Big Data, and beyond. Consequently, ITI has been a leading voice in advocating effective approaches to privacy, both domestically and globally.

The Internet has thrived—and privacy has been protected—under the Federal Trade Commission's (FTC) approach to privacy, which is grounded in the Fair Information Practices Principles ("FIPPs"). This framework applies to all entities under the FTC's jurisdiction who collect and use consumer data. We believe the FCC's primary objective should be to closely harmonize with the existing FTC framework any Internet Services Provider (ISP) or broadband privacy rules it ultimately adopts. While the FCC has concluded that the regulation of Broadband Internet Access Services (BIAS) providers is uniquely within its purview following the FCC's decision to reclassify broadband as a Title II service, irrespective of whether that order is ultimately upheld in the courts, there is nothing in that decision that necessarily warrants 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. Unfortunately, the FCC intends to proceed in another direction, proposing a series of onerous privacy and data security rules that are out of step with established policy, law, and practice in this area.

I will focus my testimony on four areas: (1) The FCC's lack of legal authority to regulate ITI's companies, including "OTT" or "Edge" providers; (2) the inconsistency of the FCC's proposed privacy regulations with consumer expectations; (3) the broader inconsistency of the FCC's proposed privacy regulations with existing privacy authorities, frameworks and enforcement regimes, as embodied in the FTC's well-established approach to privacy; and (4) ITI's concern that the proposed rules will establish negative precedents that will ultimately adversely impact consumers, businesses, and the global policy ecosystem.

On this latter point, I will highlight our concerns regarding how several of the specific rules proposed by the FCC are out of step with current law and practice, including: (1) the unreasonably short and inflexible breach notification periods; (2) the overbroad and unnecessary definition of personally identifiable information; (3) the overly burdensome consumer choice and consent framework; and (4) the prescriptive, inflexible data security requirements that are misaligned with current industry practice and Federal and state policymaking.

The FCC Lacks the Authority to Regulate ITI's Companies

By and large, ITI's companies do not offer broadband Internet access service as a core part of their businesses, and could not be categorized as such given the definitions for BIAS and BIAS providers in the Open Internet Order and these proposed broadband privacy rules.

Given this, ITI's companies are not subject to the FCC's jurisdiction under Title II, even after the FCC reclassified broadband Internet access service as a telecommunications service under Title II, nor is there a valid legal argument which could subject our companies to Title II regulation under the Open Internet Order adopted last year.

The FCC specifically defines BIAS to mean "[a] mass-market retail service by wire or radio that provides the capability to transmit data to and receive data from all or substantially all Internet endpoints, including any capabilities that are incidental to and enable the operation of the communications service, but excluding dial-up Internet access service. This term also encompasses any service that the Commission finds to be providing a functional equivalent of the service described in the previous sentence, or that is used to evade the protections set forth[.]" The FCC defines a "broadband Internet access service provider" as a person or entity engaged in the provision of broadband Internet access service. Furthermore, the Commission specifically notes over-the-top services and service providers—a category into which many ITI member companies fit—are not broadband Internet access service providers and were not captured under the Open Internet Order nor the Broadband Privacy Notice of Proposed Rulemaking. In fact, in the Open Internet Order the Commission went out of its way to emphasize that while broadband Internet access service providers may offer over-the-top services, over-the-top providers of voice over Internet protocol, Internet protocol messaging services, and Internet video providers are separate and distinct from broadband Internet access providers.

There are well-founded consumer, business, and economic reasons to rationalize why Internet and IT services providers and network operators including broadband services providers are treated differently from a regulatory perspective. From a consumer choice standpoint, there are significant differences between OTT services providers or Internet companies and BIAS providers. Consumers have traditionally had

limited choices when it comes to choosing a BIAS provider for purposes of acquiring broadband or Internet service. Indeed, broadband access itself is increasingly considered a fundamental right by many—it is necessary for basic services at all levels of government, educational opportunities, workforce opportunities, and numerous other basic needs. Once a consumer has a broadband connection, however, consumers can easily choose amongst many different OTT applications and Internet service options, including choosing to discontinue one service, switch to another service, or subscribe to several comparable services simultaneously. And certainly, these types of services are not considered a right; rather, inherent in their multiplicity is the very concept of choice.

Additionally, there are significant differences between the business and economic models of ISPs and edge service providers. Internet companies providing content or services to consumers have different economic interests than ISPs. For instance, consumers typically pay for broadband services whereas much of the content and many of the services provided to consumers over the Internet are ad-supported and thus provided to consumers free of charge. This relationship has not changed under the reclassification of broadband Internet access service, nor has the legal and regulatory authority governing that relationship. Internet companies' relationship with their customers and the use of their customers' data has been and remains subject to FTC enforcement.

ITI's perspective on this matter is solely driven by years of experience in engaging with, and helping to develop, the domestic and global privacy policy frameworks we operate under today.

The FCC's Proposed Data Privacy Rules are Inconsistent with Consumer Expectations

As I described above, ISPs and edge providers are very differently situated from the perspectives of consumers both in terms of how their business models are implemented and in terms of the regulatory reach of the FCC. The fact that there are fundamental differences between ISPs and Internet companies and those differences have historically given rise to different regulatory and enforcement regimes, however, does not give license to creating data privacy rules that are inconsistent with consumer expectations. Rather, how the FCC regulates data should be determined by what is best for consumers, whether consumers are suffering identifiable and quantifiable harms, and whether gaps exist in the current regulatory and enforcement regime.

Additionally, sound privacy policy for one entity in the Internet ecosystem should be sound policy for all others. The FCC has not made the case to justify the type of expansive and prescriptive regulatory regime contemplated by the NPRM—a significant departure from the current FIPPs-based approach undertaken by the FTC.

Fundamentally, if the FCC seeks to ensure the goals articulated in the NPRM of protecting consumer privacy, it must carefully weigh consumer interests and expectations. Unfortunately, the proposed regulations contain no indication that consumer interests—in particular whether they are suffering any harm under the current regulatory approach—demand expansive new regulations in this area. Consumers have embraced today's thriving internet, fueled by responsible data practices governed by the existing regulatory framework, and they have come to expect a seamless online experience across multiple devices that delivers convenience while also protecting their privacy. The current online ecosystem subsidizes online offerings that consumers value, promotes innovation, and grows the economy. There is simply no record of consumer harm supportive of the FCC's proposal for such restrictive regulations. In other words, the FCC's proposal should embrace a more measured approach. Consumer expectations have also not been factored into the FCC's analysis. Indeed, as Commissioner O'Reilly points out in his dissent, "there is no need for the Notice to describe consumer expectations because it is irrelevant to the FCC's analysis."

The FCC's Proposed Data Privacy Rules are Inconsistent with Existing Privacy Frameworks and Enforcement Regimes

We believe what would most benefit consumers is an approach that is consistent with existing privacy frameworks grounded in the FIPPs and consistent with existing privacy enforcement regimes. Consumers and industry benefit when one agency takes the lead on privacy regulation and enforcement because regulatory consistency permits continued innovation without bias among sectors. The FTC has a long history of addressing and enforcing privacy-related issues across industries. Indeed, the FTC has shown much leadership over the years as the enforcer on digital ecosystem issues, for both technical and legal reasons, and it remains well-situated to provide such leadership into the future.

Specifically, existing voluntary self-regulatory standards supported by 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, which reflect the responsible data practices so 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.

Further, the FTC's enforcement authority provides effective legal safeguards for online data practices. In addition to industry self-regulation, the FTC robustly enforces consumer privacy and data security standards using its authority to address "unfair or deceptive acts or practices" under Section 5 of the FTC Act. The FTC has used this authority to enforce company commitments to customers, to comply with industry self-regulatory requirements, and to protect consumers from harmful practices. 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. There is no need to create a new framework such as that proposed by the FCC because the FTC has well-established principles in this area.

Nonetheless, if the FCC is ultimately found to possess the requisite authority to regulate broadband privacy and follows through on its intent to do so, it should make certain that any such efforts are consistent with existing robust privacy frameworks and enforcement authorities, particularly those of the FTC. One way to ensure this sort of consistency is for the FCC to work closely with the FTC to harmonize its privacy rules for broadband ISP consumers with the framework that protects consumers of those online businesses or services falling under the jurisdiction of the FTC. In addition, the FCC and FTC should work closely together to help the communities within their purview—broadband ISPs and businesses providing service over the internet, respectively—to clearly understand the applicable rules to enable good faith compliance.

The FCC's Privacy Proposal is Out of Step with Current Law and Practice, and would Establish Precedents that Will Negatively Impact Consumers, Companies, and the Internet Ecosystem

Rather than adopt a regime aligned with the FTC's well-established approach to privacy, the privacy regime proposed by the FCC in the NPRM departs from the FTC framework in significant and material respects. We are particularly concerned that the prescriptiveness of the proposed regulatory approach could have precedential effects that would negatively impact the rest of the Internet ecosystem, including the tech sector. While it is hard to say for certain what the implications on other sectors will be if the FCC moves forward with the NPRM and adopts standards that diverge from those the FTC has already established for customer information, we believe the existence of multiple sets of privacy rules will, at a minimum, send a troubling message to governments and businesses internationally. Additionally, I'd like to point out four specific components of the FCC's proposal that are out of step with currently established policy and practice and raise significant concerns for both consumers and businesses.

The Breach Notification Periods are Unreasonably Short and Inflexible. The FCC proposes extremely short data breach notification periods in the NPRM—entities suffering a breach would be required to provide notice within seven days to the Commission, FBI, and Secret Service, and within 10 days to customers (NPRM ¶ 75), without regard to whether the breach creates a significant risk of customer harm. Such notices would need to be provided regardless of whether a breach is malicious or inadvertent, which is an element in determining whether a risk of harm exists (NPRM ¶ 75).

First, the FCC's data breach proposal fails to include a risk analysis, and therefore will contribute to notice fatigue at best or incite unnecessary panic at worst. Additionally, the proposal fails to account for breaches of data that are rendered not actionable through technology, such as encryption, or for inadvertent but innocent breaches, such as an employee accidentally opening the wrong file. Notifying individuals that their information has been compromised is an important step that enables them to take protective measures. Notification to consumers, however, is not productive if all data breaches result in notifications. If over-notification becomes commonplace, consumers will have difficulty distinguishing between notices and determining which ones warrant them to take action. Notification should be made to consumers if an organization has determined there is a significant risk of identity

theft or financial harm. Upon receipt of such a notice, consumers can then implement measures to help avoid being financially damaged.

Second, the proposal does not afford organizations adequate time to remediate any discovered vulnerabilities or to conduct thorough investigations to ascertain the nature and scope of any breach before notifying customers or government agencies of a breach of data. Unless vulnerabilities are addressed prior to making the breach incidents public, organizations and their customers are susceptible to further harm by wrongdoers. Because the NPRM does not afford organizations adequate time to investigate the scope and nature of breach incidents, the NPRM not only encourages over-notification by organizations, but it creates a standard of notification that would be counterproductive should the alleged breach prove a false alarm or if the breach does not create a significant risk of identity theft. A tremendous amount of forensics, decision-making, and clerical and legal work is required before ascertaining the nature and scope of a breach, assessing the risk of harm, or in determining the appropriate form of notification based on the organization's relationship with the effected customer.

More fundamentally, the FCC proposes to regulate breach notification in a way that is contrary to the existing state notification regimes and the proposals under consideration by Congress. Recognizing the sophistication of today's hackers and the challenging nature of a post-data breach forensic investigation, a breach notification regime must provide realistic, flexible, and workable time requirements. ITI has long advocated for Congress to establish a uniform but flexible approach to data breach notification that notifies customers where there is a significant risk of identity theft or other financial harm. Such a uniform approach not only eases compliance burdens for businesses, but it reduces or eliminates confusion for consumers.

The Proposed PII Definition is Overbroad and Unnecessary. The FCC proposes to define PII as "any information that is "linked or linkable to an individual." (NPRM ¶ 60). This is an overly broad definition that subsumes the entirety of the Customer Proprietary Network Information ("CPNI") category that the FCC proposes to expand elsewhere in the NPRM. As a result, both the proposed PII and CPNI definitions expansively include data elements that have never before been considered PII under U.S. law, such as Internet protocol addresses or other unique identifiers necessary for the functioning of connected Internet devices, application usage data, persistent online identifiers (cookies), and Internet browsing history—data that is highly unlikely to contribute to a risk of concrete harm such as identity theft. (NPRM ¶¶ 62–63).

First, it is unclear why the Commission endeavors to define PII at all, rather than just focusing on the CPNI data clearly within its statutory ambit. Further, the Commission acknowledges that BIAS providers may not actually collect all of the categories of information included within the proposed expansive definitions, yet the FCC proposes to regulate the collection of such data anyway. The potential unintended consequences of these overly and unnecessarily broad definitions are quite concerning, particularly since many of the types of data captured by the proposed definitions are integral to providing Internet services to consumers, including securing Internet transactions.

Exhibiting some awareness of the potential unintended consequences that could flow from such a broad PII definition, the FCC proposes a number of exceptions to the definition of PII. For example, the NPRM exempts from the definition of PII data collected by entities "to protect themselves or others from cybersecurity threats or vulnerabilities." (NPRM ¶ 117). We are concerned this exception may not be nearly broad enough to adequately help protect the Internet ecosystem. To illustrate, the definition suggests that companies would only be allowed *to collect* such information to counteract specific threats. This belies the reality that some of this information, such as unique IDs, must be collected *and shared* by companies as part of their cybersecurity risk management programs in order to prevent cybersecurity intrusions from happening. Indeed, the trajectory of Federal policymaking in this area over the past several years has been to encourage both continuous monitoring by organizations and the sharing of cybersecurity threat information to counteract cyber threats. The approach here is illustrative of the overall flawed approach to, and treatment of, PII in the FCC's proposal.

The Proposed Consumer Choice and Consent Framework is Overly Burdensome and Restrictive. The consent standard proposed by the FCC is both overly burdensome and restrictive. Generally, the FCC has proposed to restrict most collection, use, and disclosures of data with an "opt-in" consent standard, which it acknowledges may cause "notice fatigue" for consumers (NPRM ¶ 141). The Commission further acknowledges the "burden of [their] proposed customer choice framework" on businesses, particularly on smaller entities (NPRM ¶ 151). The proposed choice framework is also out of step with current policy and practice.

Experience shows that an opt-out or implied consent standard is an effective mechanism to effectuate consumer privacy preferences with respect to non-sensitive online data while allowing legitimate practices, including advertising, to continue. We urge the FCC to follow the FTC approach of permitting an opt-out approach for use of consumer data in most instances, with an opt-in approach reserved for uses of the most sensitive consumer data.

The Proposed Data Security Requirements are Prescriptive, Inflexible, and Misaligned with Both Industry Approaches and Federal Cybersecurity Policies. In the NPRM, the FCC proposes both general data security requirements for BIAS providers and "specific types of practices they must engage in to comply with the overarching requirement." (NPRM ¶ 167).

While the Commission acknowledges any proposed security requirements must "allow for flexibility for practices to evolve as technology advances," and claims it does not propose "to specify technical measures for implementing the data security requirements," (NPRM ¶ 176), it nonetheless proposes a series of increasingly prescriptive security requirements. For example, the Commission proposes to not only require regular Graham-Leach-Bliley-like risk assessments (NPRM ¶ 180) at a frequency to-be-determined (NPRM ¶ 183), but it also asks whether the FCC should prescribe specific risk-management requirements on BIAS providers, and how the risk assessments themselves should be conducted. (NPRM ¶ 182) These proposed requirements contradict existing cybersecurity public policy—such as that embedded in the Framework for Improving Critical Infrastructure Cybersecurity ("Cybersecurity Framework")—that risk management is a continuous process demanding flexibility in order to provide reasonable protections in light of the nature and scope of the activities of a given company, including the sensitivity of the data it handles, its threat profile, and the size and complexity of the relevant data operations of the company. Another example can be found in the series of proposed specific authentication measures the Commission proposes to prescribe (NPRM ¶¶ 191–200).

Indeed, the structure of the entire security section appears contrary to many of the core concepts of risk management (*e.g.,* voluntariness, flexibility, etc.) as throughout the NPRM the Commission asks a series of "should we require this" and "should we require that" questions. This is a fundamentally flawed approach, out of step with the approach embodied in the Cybersecurity Framework and the consensus standards and best practices included within. We agree with Commissioner O'Reilly's dissenting statement that the proposed prescriptive security rules are inconsistent with the voluntary approach embodied in the Framework and are indeed "alarming."

Conclusion

Members of the Committee, ITI and our member companies are pleased you are examining the important issue of how the FCC's proposed broadband privacy regulations may impact consumers and competition. We share both the FCC's and your interest in protecting the privacy of consumers of broadband Internet access services. As noted above, however, we are concerned with the approach taken by the Commission in a number of respects. We have raised our concerns directly with the Commission by submitting comments on the NPRM, urging the agency to reconsider promulgating data privacy rules that are inconsistent with consumer expectations or existing privacy authorities, frameworks and enforcement regimes, such as embodied by the FTC's longstanding approach to privacy. We appreciate the opportunity to reiterate these concerns today, including our belief that the privacy regime proposed by the FCC is out of step with current law and practice and would establish precedents that will negatively impact not only consumers but companies and the Internet ecosystem as a whole. Please consider ITI a resource on these important issues moving forward, and do not hesitate to contact us with any questions regarding this submission.

Thank you for the opportunity to appear before you today.

The CHAIRMAN. Thank you, Mr. Garfield.

Professor Ohm.

STATEMENT OF PAUL OHM, PROFESSOR, GEORGETOWN UNIVERSITY LAW CENTER AND FACULTY DIRECTOR, GEORGETOWN CENTER ON PRIVACY AND TECHNOLOGY

Mr. OHM. Chairman Thune, Ranking Member Nelson, and distinguished members of the Committee, it's really my privilege to be

here today to discuss a very important topic with you. The basic principle at stake is a very old one. The Postal Service cannot track the letters you send or open your letters in order to sell that information to marketers. Without your consent, your telephone company cannot track the phone numbers you dial or listen in on your conversations in order to sell that information to advertisers. We should have the same rule for ISPs, and without your consent, they should not be able to sell your reading habits and your physical location to advertisers.

So to help protect this very old basic principle, the FCC has proposed the rule we are discussing today. I want to say three things about the rule. I believe it is unambiguously authorized by law, it is a wise rule, and it is a measured rule. Let me take those in turn.

Now that the D.C. Circuit has ruled that reclassification of broadband service into Title II was within the power of the FCC, it's incumbent on the FCC to elaborate what this means for broadband providers, including rules for customer privacy. And nobody in the debate disputes that Congress enacted Section 222 of the Telecommunications Act to obligate telecommunications providers, such as telephone companies, to respect the privacy of their customers. It makes a straightforward reading of the statute to extend this obligation to ISPs as well. Because this is a straightforward reading, the burden should be on those who would rewrite the statute, or even worse, ask the FCC to disregard it, rather than the agency that's merely trying to apply it.

Number two, and I want to spend the most of the time on this, Why is the law wise? Congress's act reflects the well-reasoned conclusion that telecommunications providers owe a heightened level of privacy to their customers. I've already explained the historical antecedent for this with our Postal Service and our telephone companies. Three other factors support this conclusion: visibility, choice, and sensitivity.

Visibility. Your ISP sits at a privileged place in the network. They are the bottleneck between you and the Internet. You cannot access the Internet but by sending information through this bottleneck, and with this privileged location, they can be a part of every website or online destination that you visit. For unencrypted websites, this visibility is unparalleled, comprehensive, and complete, but even for websites that use encryption, the ISP's view is only partially obscured, they can see the domain names of the websites you visit, how often you return to these websites, how much information you exchange with these websites. It is a very, very complete and privileged location.

Number two, choice. Most Americans today, as you well know, do not have a meaningful choice when it comes to fixed broadband service. The situation is specifically and especially difficult in rural America, and I'm glad, Chairman Thune, you raised rural America, where only 13 percent of residents have more than one choice for high-speed fixed broadband. And even for those Americans who do happen to have more than one choice, switching costs make it quite difficult to switch their ISP.

Finally, sensitivity. With the visibility providers have and given the lack of your choice for exit, your provider can compile a detailed list of what you read, with whom you communicate, what

you say, and, increasingly, where you go. And because storage is cheap, ISPs can record all of this vital sensitive information about you across years and eventually across decades. Privacy scholars have long tried to properly come up with a metaphor to characterize what we should think about a data base like this about every person in this room. Some have referred to them as digital dossiers. Others have talked about the right to intellectual privacy we ought to enjoy. My contribution to the metaphor debate has been to describe the database of ruin, the idea that there is now a corporate database in the celestial cloud that contains at least one fact about every member of our society that you would not want your worst enemy to know.

These four factors together—history, choice, visibility, and sensitivity—led Congress in 1996 to do what it had done several times before. Simply put, in the American privacy law system, when we identify a sector or a context that has unique privacy risks like we have in telecommunications, we create a sectoral privacy law. We did this for health information in HIPAA, we did this for education information in FERPA, and, indeed, we did this in Section 222 of the Telecommunications Act.

Finally, why do I believe that the FCC proposal is measured? Number one, the FCC proposal does not propose a ban. You might be excused from misunderstanding that based on some of the heated rhetoric that has come from critics of the proposal. You are not prohibited from any conduct under this rule. This is simply a disagreement about the type of user consent we ought to require before your ISP can look over your shoulder and record everything you do in order to sell it to advertisers. The FCC decided to require prior, informed, expressed consent before they could undertake this type of activity. I think this is the only sensible choice. And I'm happy to talk with you more about why during Q&A.

Last, the proposal preserves the necessary conditions for competition by treating all providers alike. When Google operates as a broadband provider, as it now does in Kansas City through Google Fiber, they are required to follow the strictures of Section 222. When Verizon acquires American Online in order to bolster its advertising business, as it did last year, they are no longer regulated for that activity under Section 222. The playing fields are level.

In closing, we do not have many privacy laws in this country. Section 222 is one of the few. And given the powerlessness your constituents feel and all Americans feel about this state of affairs, we ought to be bolstering and supplementing our privacy law, not cutting back on one of the very few that we have on the books.

Thank you again for your invitation.

[The prepared statement of Mr. Ohm follows:]

PREPARED STATEMENT OF PAUL OHM, PROFESSOR, GEORGETOWN UNIVERSITY LAW CENTER AND FACULTY DIRECTOR, GEORGETOWN CENTER ON PRIVACY AND TECHNOLOGY

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

I am a Professor at the Georgetown University Law Center and a Faculty Director of the Center on Privacy and Technology at Georgetown. I specialize in information

privacy, computer crime law, and technology and the law. I make these comments to you in my independent, academic capacity.

In 1996, Congress enacted section 222 of the Telecommunications Act of 1996, delegating to the FCC the power 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, a reclassification recently found to be a proper exercise of the FCC's power by a panel of the Court of Appeals for the D.C. Circuit.

The FCC has acted appropriately and wisely. The application of section 222 to BIAS providers represents not only a straightforward implementation of the law but also a laudable exercise of privacy theory and policy. I support these conclusions not only through my academic work [1] 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 telecommunications providers to serve as important gatekeepers of privacy, a sensible choice then and now, one that continues to protect important values in today's online environment.
- Section 2: The proposed FCC rules will decrease overall consumer confusion by creating a clear, bright line of privacy protection.
- Section 3: Rather than ban any behavior, the proposed rules will create and preserve opportunities for innovation and competition. Importantly, BIAS providers will retain the ability to compete directly with edge providers subject to the same privacy rules as any other company.
- Section 4: There remains a significant need to strengthen privacy rules for online actors other than BIAS providers. The Federal Trade Commission (FTC) does not have all of the authority or resources required to solve all online privacy problems.

1 The Statute Treats BIAS Providers as the 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

---

[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.*

I have recently filed two public documents commenting on the FCC's NPRM. *See* Statement of Paul Ohm Before the Subcommittee on Communications and Technology, Committee on Energy and Commerce, U.S. House of Representatives (June 14, 2016), available at *http://paulohm.com/projects/testimony/PaulOhm20140614FCCPrivacyRules.pdf* and Reply Comments of Paul Ohm Before the Federal Communications Commission in the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16–106 (June 22, 2016), available at *https://www.fcc.gov/ecfs/filing/10622254783425.*

century, and parcel delivery services in more recent years. 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 not visible to Facebook at any 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]

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 section 222, 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.

---

[2] FCC 2016 Broadband Progress Report, 31 FCC Rcd 699 ("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 more than 85 percent of popular sites in health, news, and shopping categories do not encrypt browsing by default).

1.4 Sensitivity

Perhaps the most important reason to protect the information a BIAS provider can obtain is the intrinsic sensitivity of this information.[4] A BIAS provider can gather at least three types of information we have long deemed sensitive: communications, reading habits, and location.

Our laws have 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. Nobody 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."[5] 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 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.

1.5 Privacy for All

The four reasons for holding BIAS providers to high privacy standards—history, choice, visibility, and sensitivity—each implicate the same, difficult question: will privacy be enjoyed by every American, regardless of wealth or station in life, or only by America's privileged few? For each of these factors, the need for meaningful privacy protections for broadband customers is even stronger from the perspective of mainstream and marginalized Americans.

For example, when it comes to visibility, some have argued that we need not worry about the privacy threat to a given consumer from any single ISP because the average American owns 6.1 devices and accesses the Internet using at least three different networks: one each for home, mobile, and work.[6] These arguments ignore the lived reality for the many Americans who rely on only a single smartphone with a single connection as their lifeline to the Internet, and as a group tend to be less wealthy, younger, and disproportionately members of minority groups than the general population.[7] Also, the average American worker does not have access to a Virtual Private Network (VPN) provided by an employer, the way some white collar workers do, and so is left looking for clunkier, costlier alternative technologies if she wants to shield her online activities from her provider.

The problem of insufficient choice, the next factor, is particularly stark for rural Americans, many of whom have only a single available provider to access the network. While 44 percent of Americans in urban areas have more than one available

---

[4] *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).

[5] NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE (2015).

[6] *E.g.,* Comments of the United States Telecom Association, WC Docket No. 16–106 at 4; Comments of Mobile Future, WC Docket No. 16–106 at 6. These commenters uniformly rely on statistics cited in a report by a team of attorneys from Georgia Tech and Alston & Bird, Peter Swire, *et al.,* Online Privacy and ISPs at 3 (May 2016) [*hereinafter* Broadband for America Report].

[7] Pew Research, *Chapter One: A Portrait of Smartphone Ownership,* U.S. SMARTPHONE USE IN 2015, April 1, 2015, *http://www.pewinternet.org/2015/04/01/chapter-one-a-portrait-of-smartphone-ownership/*.

provider offering 25 Mbps/3Mbps fixed broadband, only 13 percent of Americans in rural areas can say the same.[8] Protecting only information deemed "sensitive" tends to underprotect Internet users with idiosyncratic or non-majoritarian sensitivities, such as members of minority religions, racial or ethic groups, or marginalized political viewpoints. Finally, history suggests that we protect the privacy of the telephone system (and the mail system before it) as a reflection of how important these networks are for average Americans seeking basic access to employment, social interaction, and benefits, which is even more true today for the Internet. This argument weighs much more heavily for those without stable employment or social support than for those who enjoy greater stability, wealth, and political power.

We should reject arguments that would set information policy based only on the conditions of urban and wealthier Internet users who have relatively more (but still very little) service choice, more devices, more connections, better access to privacy tools, and whose sensitivities conform to society's default standards. Privacy should be available to all.

2 The FCC's Proposed Rule Will Decrease Consumer Confusion

The FCC has proposed a simple, bright-line rule for the privacy of information transiting a BIAS provider's network: a BIAS provider may not use its customer's private information for purposes unrelated to the provision of service unless and until the informed consumer consents to those uses. The burden of communicating the purported benefits of uses of information rests on the party best positioned to make that case, the BIAS provider itself. This approach mirrors the approach the law takes in other sectors where the information at stake is especially sensitive or private, including healthcare, banking, and education.

Contrast the straightforward nature of this proposal with the "notice-and-choice" background rules that apply to otherwise unregulated online actors. Notice-and-choice regimes rest on the fiction that Internet users read and understand the hundreds of Terms of Service and Privacy Policy documents with which they are presented online each year.[9] Each one of these lawyer-drafted and densely-worded documents sets idiosyncratic ground rules for acceptable provider behavior for a single site or service alone. Even when companies break their own ground rules, they cannot be held to account unless the FTC or a state Attorney General notices, pursues, and proves the deception or unfairness.

This crazy cacophony is somehow the ideal framework that BIAS providers urge the FCC to embrace, in the dubious name of reducing consumer confusion. The FCC's proposed default rule is much simpler and comprehensible: no unexpected uses of your information. A BIAS provider can diverge from the default, but only if it explains to you in clear, non-deceptive terms what it intends to do and receives your informed, express consent. To argue that this will increase rather than decrease consumer confusion not only defies good sense but also fails to give the consumer his or her due respect.

3 By Allowing Data Uses with Consent, the FCC's Proposed Rule Benefits Consumers Without Unduly Burdening Providers or Competition

In section 222, Congress made clear that covered providers could continue to use any information they could access "with the approval of the customer." Faithfully applying this provision, the FCC proposes to allow any uses of information after prior customer consent. Neither Congress nor the FCC has enacted or even proposed a ban on uses of information, although you might think otherwise based on the characterizations of many of the covered providers.

Put plainly, this debate is not about prohibiting conduct. Stripped of this confusion, this is simply a disagreement about the type of user consent we ought to require for conduct that at least some consumers find objectionable. In my reply comment to the FCC, I pointed out that the difference between the proposed opt-in rule and an alternative opt-out rule is not nearly as stark a difference as some have stated.[10] Recent research suggests that companies in other industries subjected to opt-

---

[8] FCC 2016 Broadband Progress Report, 31 FCC Rcd 699, ¶ 86 (2016).

[9] Two noted privacy experts, Aleecia McDonald and Lorrie Faith Cranor (currently Chief Technologist of the Federal Trade Commission), estimate that it would take the average person 244 hours per year to read the privacy policies of all sites and apps they used. Aleecia M. McDonald and Lorrie Faith Cranor, *The Cost of Reading Privacy Policies,* 4 I/S: J L & Pol Info Soc'y 540, 560 & table 7 (2008), available at *https://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf.*

[10] Reply Comments of Paul Ohm Before the Federal Communications Commission in the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16–106 (June 22, 2016), available at *https://www.fcc.gov/ecfs/filing/10622254783425.*

in requirements have managed to convince large numbers of users to choose to opt in.[11] I do not doubt that BIAS providers will try to replicate these results.

The new rules also preserve other level playing fields to facilitate unburdened competition. BIAS providers like Verizon or Comcast can acquire (and have acquired) edge provider services such as content publishers, search engines, and social networking sites. A BIAS provider that launches or acquires 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 traditional edge provider like Google creates or acquires a broadband Internet service, such as the Google Fiber service, it will fall for those purposes within Title II of the Communications Act and thus be subject to the FCC's privacy rules. In either case, any two companies competing in the same market will be subjected to precisely the same rules under precisely the same terms.

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. We need to raise our privacy standards across other parts of the online ecosystem as well. 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 industry segments 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

It was my privilege to serve the FTC as a Senior Policy Advisor on privacy issues from 2012 to 2013. I was convinced during my service and continue to feel today that the FTC has become an important bulwark of privacy in a tumultuous time of change. 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 FTC simply cannot go it alone. 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. Fortunately, these two mandates work together, as nothing in the proposed FCC rule will subject any company to conflicting FTC rules and vice versa. It is 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 Other Privacy Laws

As I have argued above, it is a combination of history, choice, visibility, and sensitivity that justifies 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.[12] Other entities traffic in location information, a category Congress ought to consider protecting as especially sensitive. Social networking sites carry exceptionally sensitive information and exhibit network effects and insufficient data portability that limit customer choice and exit. Finally,

[11] *Id. citing* Lauren E. Willis, *When Nudges Fail: Slippery Defaults,* 80 U. CHI. L. REV. 1155 (2013).

[12] Peter Swire, *et al.,* Online Privacy and ISPs (May 2016).

advertising networks strive to attain a BIAS-provider-like visibility across the Internet.

Congress should examine whether any other industry segment 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, perhaps one modeled on the FCC's rules.

5 Conclusion

Given the deep concern many of your constituents feel about their lack of control of information about them; given the calls and e-mails 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 not the 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. All American Internet users owe owe our thanks to Congress and the Federal Communications Commission for taking modest, sensible, and legally authorized steps toward enhancing the protection we enjoy.

The CHAIRMAN. Thank you, Professor Ohm.

Mr. Polka.

STATEMENT OF MATTHEW M. POLKA, PRESIDENT AND CEO, AMERICAN CABLE ASSOCIATION

Mr. POLKA. Thank you, Chairman Thune, Ranking Member Nelson, and members of the Committee, for inviting me to testify about the Federal Communications Commission's proposed privacy regulations and their effect on consumers and competition. Today I would like to focus on four essential points.

First, American Cable Association members are already subject to a host of privacy and data security obligations, take those obligations seriously, and have an excellent track record of compliance. We, too, are consumers and so understand the need for privacy protections.

Second, to best serve the interests of broadband consumers, the FCC should adopt a privacy and data security regime that is consistent with the FTC's framework. It has proven valuable and workable for all interests.

Third, we fear that the FCC's proposed privacy and data security rules would impose needless, unduly burdensome obligations on smaller broadband providers, chilling investment and innovation, all with little consumer benefit.

And fourth, should the FCC nonetheless proceed and adopt rules in line with its proposals, it should ease the burden on small broadband providers by providing tailored exemptions, extending compliance deadlines, and streamlining its rules.

The American Cable Association represents 750 smaller cable operators, incumbent telephone companies, municipal utilities, competitors, and other local providers which offer service in all 50 States. Eighty percent of our members serve fewer than 5,000 customers. Fifty percent serve fewer than 1,000. Most have 10 or fewer employees and cannot afford to dedicate employees solely to regulatory compliance.

As I said at the outset, ACA members must comply, and have complied, with numerous privacy and data security obligations, several of which were the work of this committee. These two long-

standing provisions include the Communications Act, Section 631, for cable services enacted in 1984, and Section 222, the Consumer Proprietary Network Information rules, also known as CPNI, for voice and now broadband services, enacted in 1996. These also include Section 5 of the Federal Trade Commission Act for non-common carrier services and the laws of the states where providers operate. Complying with all of these requirements imposes a significant burden on smaller providers, but ACA members understand their duty and their legal obligations to protect the confidentiality of their customers' information.

Because ACA members are subject to so many time-tested privacy and security obligations, they had hoped that the FCC, in crafting CPNI regulations to cover broadband, would have proposed a regime consistent with requirements already on the books. In fact, ACA joined with other industry organizations last year to present to the FCC a privacy framework that would promote the goals of transparency, choice, data security, while retaining consistency with the FTC's framework.

Our privacy proposal would protect consumers and equally regulate all participants in the Internet ecosystem. It would also enable smaller providers to comply without undue burdens. Unfortunately, the FCC insisted on blazing an entirely new path by proposing novel, complex, and overly burdensome requirements. In comments filed recently with the FCC, the Small Business Administration's Office of Advocacy said that smaller providers will be subject to onerous obligations.

In our view, these obligations would chill investment and innovation while providing uncertain consumer benefits. Even more importantly, these rules would apply only to broadband providers, a mere subset of players in the Internet ecosystem. This would lead to customer confusion as well as distort the market through asymmetric regulation. The FCC should revise its approach, reassess the costs and benefits of its proposal, and seek to blend it with the FTC's approach.

In closing, ACA members have spent decades protecting their customers' privacy and data security. As the FCC moves to craft new rules for broadband, we seek to bring to bear our experience and the previous efforts of this committee and other government bodies to build a sound and lasting regulatory regime. And we promise to continue our efforts to develop a solution that works for all.

Thank you.

[The prepared statement of Mr. Polka follows:]

PREPARED STATEMENT OF MATTHEW M. POLKA, PRESIDENT AND CEO, AMERICAN CABLE ASSOCIATION

Thank you, Chairman Thune, Ranking Member Nelson, and Members of the Committee, for inviting me to testify on behalf of the American Cable Association (ACA) and its members about the steps we are taking to protect the privacy and security of our customers' personal information and our thoughts on the Federal Communications Commission's (FCC's or Commission's) proposed privacy and data security rules for broadband Internet access service (broadband service).

In my testimony, I will focus on four points. First, ACA members are already subject to a host of privacy and data security obligations, take those obligations seriously, and have an excellent track record of compliance. Because they too are consumers, ACA members understand consumers' expectations and the need for privacy

protections. Second, to best serve the interests of broadband consumers, the FCC should adopt a privacy and data security framework that is consistent with the Federal Trade Commission's (FTC's) approach, which has proven valuable and workable for all interests. Third and most unfortunately, we fear that the FCC's proposed privacy and data security rules would impose needless, unduly burdensome obligations on smaller broadband providers, chilling investment and innovation, all with little consumer benefit. And finally, if the FCC nonetheless proceeds and adopts rules in line with its proposals, it should ease the burdens on small providers by providing tailored exemptions, extending compliance deadlines, and streamlining its rules.

I. Background on ACA's Members

ACA represents approximately 750 small and medium-sized cable operators, incumbent telephone companies, municipal utilities, and other local providers, which provide service in all fifty states. ACA members provide a variety of services to their residential and business customers, including voice, cable service, broadband, and various non-common-carrier services, such as home security, PC support, e-mail, and data center services. Eighty percent of ACA members serve fewer than 5,000 subscribers, and roughly fifty percent serve fewer than 1,000 subscribers. Half of ACA's members have ten or fewer employees, with typically just one or two engineers or individuals with technical expertise, and these employees perform many duties within their companies. Few have in-house personnel dedicated to privacy and data security compliance. Yet, they take all necessary steps to comply with today's regulatory mandates, even though it is a challenge and cuts into their ability to upgrade systems and to offer new products and services.

Consequently, ACA urges Congress and the Commission to continue to seek to balance actions that would impose new obligations with the resource capabilities of smaller providers. Skewing that balance against broadband providers—as the Commission proposes to do—imperils investments in high performance networks and information services so critical for consumers and our economy.

II. ACA Members Are Already Subject to A Host of Privacy and Data Security Rules, Take Those Obligations Seriously, and Have an Excellent Track Record of Compliance

ACA members must comply and have complied with numerous privacy and data security obligations, several of which were the work of this Committee. ACA members that provide cable service must comply with Section 631 of the Cable Communications Policy Act of 1984 (the Cable Act).[1] ACA members that provide voice services—whether traditional circuit-switched voice or interconnected voice over Internet Protocol (VoIP)—must comply with Section 222 of the Communications Act of 1934, and its implementing rules related to customer proprietary network information (CPNI).[2] ACA members that provide broadband service must comply with the FCC's transparency rule (which requires disclosure of privacy policies), and since the *2015 Open Internet Order,* the FCC has asserted that they must comply with Section 222 (notwithstanding ongoing challenges to the agency's authority to do so). ACA members that provide non-common-carrier information services, a term which until recently applied to broadband service, must also comply with Section 5 of the Federal Trade Commission Act, which prohibits "unfair or deceptive acts or practices," including those related to privacy and data security. Further, our members are subject to the laws and rules of the states in which they operate, including but not limited to data breach notification laws.[3] In addition, to the extent that they interact with

[1] Cable operators have been subject to Section 631 for over 30 years. Section 631 includes a robust set of requirements, including annual subscriber notices, a customer consent framework, access rights, and a private right of action.

[2] Section 222 and its implementing rules are designed to protect the confidentiality of individually identifiable CPNI, a narrow category of information that includes information about a customer's use of the network (*e.g.,* call detail records) and information contained within customer bills. The CPNI rules include a three-tiered notice and consent regime, data security safeguards, a breach notification rule, and annual certifications. Beginning in 2014, the FCC began to read Section 222 more broadly to protect "customer proprietary information," a category of information that according to the FCC includes both CPNI as well as all personally identifiable information. ACA and others have challenged the Commission's broad interpretation of the statute as unlawful.

[3] Every state has a law prohibiting deceptive practices, and most have laws prohibiting unfair practices, similar to the FTC's Section 5 prohibition. *See, e.g.,* Conn. Gen. Stat. § 42–110b(a); Fla. Stat. Ann. § 501.204; Mass. Gen. Laws Ch. 93A, § 2(a); S.D. Codified Laws § 37–24–6(1). Further, 47 states have enacted data breach notification laws. *See, e.g.,* Conn. Gen Stat. § 36a-701b; Fla. Stat. §§ 501.171, 282.0041, 282.318(4)(j)(1); Mass. Gen. Laws § 93H–1 *et seq.* Moreover, several states have enacted additional privacy and data security requirements. *See, e.g.,* Fla. Stat. § 501.171; 201 CMR 17.00. For example, Massachusetts requires companies to "develop, imple-

institutions handling sensitive information such as banks, hospitals, and schools, they often must assume obligations—by statute, rule, or contract—to protect such information.

Complying with all of these privacy and data security laws is a significant burden for smaller providers, but they understand their responsibilities and have taken the necessary steps to ensure they comply. ACA members notify their subscribers of their privacy practices through welcome packages, annual notifications, and website privacy policies. Our members also provide opportunities for customers to make choices about how service providers use or share their information and give all the necessary information to make an informed choice. They also understand the importance of effective personnel training, as well as the need to ensure that agents and independent contractors—*e.g.,* billing and customer service companies—protect the confidentiality of customer information.

ACA members employ reasonable physical, technical, and administrative data security practices to protect against breaches of customer information. For example, ACA members have established robust authentication requirements, such as password protection for access to customer information or, for small-town providers, requiring customers to authenticate themselves in person with proper identification. In addition, our members are responsible in their duties to comply with the record-keeping and reporting obligations of the FCC's existing privacy and data security rules, including obligations to keep records of customer approval status and marketing campaigns, as well as annual certification obligations. We have been active in the FCC's Communications Security, Reliability and Interoperability Council Working Group IV proceeding, which is intended to assist companies with implementing voluntary cybersecurity measures for the communications sector that respect the unique challenges that small and medium-sized providers face.

The privacy and data security actions described above and others that smaller providers undertake do not exist in a vacuum—they are just one part of an increasingly complex web of legal and regulatory obligations with which providers must comply, including law enforcement, disabilities access, copyright, emergency alert service, universal service, and open Internet obligations, as well as a variety of state and local regulations.

ACA members have an excellent track record in protecting the confidentiality of their customers' information and complying with privacy and data security laws and rules. Indeed, in the decade during which the FTC exercised its authority over broadband providers—conducting innumerable investigations and actions against companies related to privacy and data security—we are not aware of a single action against a smaller broadband provider for the sorts of privacy and data security practices that the FCC seeks to regulate pursuant to its proposals. Such a long run free of major incidents reinforces the view that a new and more intrusive privacy and data security regime is not needed to protect consumers.

III. To Best Serve the Interests of Broadband Consumers, the FCC Should Adopt a Privacy and Data Security Framework That Is Consistent With the FTC's Approach, Which Has Proven Valuable and Workable for All Interests

Until the FCC classified broadband service as a Title II telecommunications service in the *2015 Open Internet Order,* all industry participants in the Internet ecosystem were subject to the jurisdiction of the FTC. The FTC's approach combines a flexible statutory provision—Section 5 of the FTC Act—with heightened obligations for limited categories of sensitive information (*e.g.,* children's information, health information, or financial information). As such, the FTC's approach has at its core the concepts of flexibility, context specificity, and technological neutrality. This framework has enabled the Internet ecosystem to flourish to the benefit of consumers, edge providers, and broadband providers alike. Further, by avoiding hyper-prescriptive rules and focusing instead on the reasonableness of providers' practices and the truthfulness and completeness of their representations to their customers, the FTC's framework lessens the compliance burdens on smaller providers.

In contrast, the FCC proposes to cleave the Internet ecosystem in two by subjecting one set of participants—broadband providers—to a different and more burdensome privacy and data security regime, while another set—including edge providers—remain subject to the FTC's approach. The FCC is proposing these rules despite the fact that the large edge providers can know more about a user's activity

---

ment, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards," with granular requirements that every such information security program must include. *See* 201 CMR 17.00.

and, unlike broadband providers, often employ business models that depend on the collection, use, and sharing of their customers' personal information. For smaller broadband providers, which lack scale, such business models are rarely in our members' strategic plans.

In advance of the FCC issuing its proposals, ACA and several trade associations proposed a framework that would protect consumers and promote the FCC's goals of transparency, choice, and data security while retaining consistency with the FTC's framework. Such an approach would protect consumers and avoid entity-based regulation that would create consumer confusion and stifle innovation. Consumers expect their data will be subject to consistent privacy standards based upon the sensitivity of the information and how it is used, regardless of which entity in the Internet ecosystem uses that data. Indeed, FTC staff has stated that "any privacy framework [for broadband providers, operating systems, browsers, and social media] should be technology neutral," and has argued that the FCC's failure to propose a consistent privacy regime is "not optimal."

We recommended that to maintain consistency with the FTC's framework, the FCC should adopt rules based on the following principles:

- *Transparency.* A broadband (telecommunications service) provider should provide notice, which is neither deceptive nor unfair, describing the CPNI that it collects, how it will use the CPNI, and whether and for what purposes it may share CPNI with third parties.
- *Respect for Context and Consumer Choice.* A broadband provider may use or disclose CPNI as is consistent with the context in which the customer provides, or the provider obtains, the information, provided that the provider's actions are not unfair or deceptive. For example, the use or disclosure of CPNI for the following commonly accepted data practices would not warrant a choice mechanism, either because customer consent can be inferred or because public policy considerations make choice unnecessary: product and service fulfillment, fraud prevention, compliance with law, responses to government requests, network management, first-party marketing, and affiliate sharing where the affiliate relationship is reasonably clear to consumers. Consistent with the flexible choice mechanisms available to all other entities in the Internet ecosystem, broadband providers should give consumers easy-to-understand choices for non-contextual uses and disclosures of their CPNI, where the failure to provide choice would be deceptive or unfair. The provider should consider the sensitivity of the data and the context in which it was collected when determining the appropriate choice mechanism.
- *Data Security.* A broadband provider should establish, implement, and maintain a CPNI data security program that is neither unfair nor deceptive and includes reasonable physical, technical, and administrative security safeguards to protect CPNI from unauthorized access, use, and disclosure. Providers' CPNI data security programs should provide reasonable protections in light of the nature and scope of the activities of the company, the sensitivity of the data, and the size and complexity of the relevant data operations of the company.
- *Data Breach Notifications.* A broadband provider should notify customers whose CPNI has been breached when failure to notify would be unfair or deceptive. Given that breach investigations frequently are ongoing at the time providers offer notice to customers, a notice that turns out to be incomplete or inaccurate is not deceptive, as long as the provider corrects any material inaccuracies within a reasonable period of time of discovering them. Broadband providers have flexibility to determine how and when to provide such notice.

Our proposal would meet consumers' privacy needs while allowing them to take advantage of products and services they expect from their service provider and would avoid inconsistent and burdensome oversight. Moreover, it would ensure a level playing field between edge providers and broadband providers, promoting an innovative and competitive broadband ecosystem.

Our proposal also would improve the ability of smaller providers to comply without incurring undue costs or other burdens. As I explained earlier, smaller providers work to ensure that they use customer information consistent with their customers' expectations. Since these providers are already familiar with the FTC framework, they would not have to incur material additional costs to bring their policies, processes, and systems into compliance if the FCC adopts rules consistent with this framework.

Our proposal also is superior because the consumer choice provisions align with consumer expectations by respecting the context of customer-carrier interactions.

This will enable small providers to offer new and innovative services to their customers, increasing consumer choice and competition.

The data security rule in our proposal also contains a robust general security standard that requires "physical, technical, and administrative" security safeguards while including the size of the company as a factor in determining whether particular safeguards are reasonable. As such, in the event that smaller providers grow, the rules will require more sophisticated processes commensurate with their larger operations. Additionally, our framework enables the FCC to establish best practices through multi-stakeholder processes.

Finally, our proposed data breach notification rule is superior to the FCC's proposed rule because it provides flexible deadlines that will not overburden small providers and a safety valve for good faith disclosures so that small providers can avoid counterproductive strict liability enforcement actions associated with inflexible and overly prescriptive regimes.

IV. The FCC's Proposals Would Needlessly Impose Unduly Burdensome and Costly Restrictions on Small Providers, Chilling Investment and Innovation With Minimal Additional Consumer Benefit

The FCC proposes a set of privacy and data security rules that, if adopted, would be one of the most complex in the United States. Let me highlight just some of the new notice, customer approval, data security, and data breach notification obligations the FCC proposes to impose on smaller broadband providers.

- *Proposed Notification Rules.* The proposed notification rules would prescribe, in minute detail, when, where, how, and how often providers must notify their subscribers about their privacy and data security practices, which would require smaller providers incur legal costs to draft and update privacy notices, administrative costs to deliver the notices, and technical costs to post the notices "persistently" on the provider's website, mobile app, and any functional equivalent.
- *Proposed Customer Approval Rules.* The proposed customer approval rules would replace the long-standing, context-specific, and consumer-friendly opt-out regime of the FTC with an incredibly complex and restrictive three-tiered framework that would erect unnecessary barriers to collecting, using, or sharing customer information by requiring opt-in consent in many situations that are well within consumer expectations.
- *Proposed Data Security Rules.* The proposed data security rules would replace the FTC's reasonable security standard with a general strict liability rule requiring providers to "ensure" the confidentiality, security, and integrity of customer information, irrespective of the sensitivity of that information and ignoring the fact that most agencies recognize that there is no such thing as perfect security. The proposed data security rules also would impose exacting operational requirements on broadband providers, such as: requiring regular risk management assessments; appointing "senior officials" to oversee providers' privacy and data security practices; implementing third party oversight mechanisms; and conducting training for personnel, agents, and affiliates.
- *Proposed Data Breach Notification Rules.* The proposed data breach notification rules would impose a strict, seven-day turnaround time from discovery of the breach to notify the FCC and law enforcement about any data breach, and a ten-day turnaround for notifying affected customers, regardless of whether the breach was intentional or whether consumer harm is reasonably likely. The result of this proposed breach notification rule will be over-notification, often including incomplete or evolving facts, which will confuse consumers, breed unnecessary distrust in the Internet ecosystem, and work to undermine the "virtuous circle" of demand for Internet services, deployment of broadband infrastructure, and innovation.

Unlike the existing CPNI rules, the proposed rules would not be limited to "customer proprietary network information"—the narrow set of information that Section 222 was drafted to address—but rather would apply to all "customer proprietary information," a broad, amorphous term that appears nowhere in the Communications Act and covers everything from the make and model of a user's modem to an individual's public demographic information. Further, unlike the existing CPNI rules, the proposed rules would apply to all past, present, and prospective customers of a broadband provider. The FCC even seeks comment on whether to expand the definition of customer to include minors, members of a group plan, or other individual users who can access a shared account. By extending the universe of covered information and individuals, smaller providers will need to manage significantly more information, dramatically increasing the costs and burdens of compliance.

To meet all of these new, extensive obligations, smaller broadband providers would need at least to:

- Develop and implement new data security controls, website policies, and customer approval tracking systems;
- Hire and train dedicated privacy and data security staff;
- Provide additional customer notices, including data breach notifications that would increase customer confusion and "notice fatigue";
- Retain attorneys and consultants for such activities as regulatory analysis, contract negotiation, risk management assessments, and preparing required policies, forms, training, and audits;
- Ensure compliance for call centers, billing software, and others that interface with customer proprietary information; and
- Divert scarce resources from innovation and infrastructure deployment to regulatory compliance.

These new costs would be most burdensome for smaller providers, decreasing their ability to innovate, upgrade systems, and compete while increasing costs, confusion, and inconvenience for their customers. Indeed, the Office of Advocacy for the Small Business Administration (SBA) told the FCC that its "proposed rules will be disproportionately and significantly burdensome for small Broadband Internet Access Service (BIAS) providers," arguing that "the FCC failed to comply with the [Regulatory Flexibility Act's] requirement to quantify or describe the economic impact that its proposed regulations might have on small entities," and "[t]he FCC has provided no estimate of the paperwork hours required to comply with the regulations."

V. If the FCC Adopts Its Proposed Rules, It Should Take Steps to Ease the Burden on Smaller Providers Through Exemptions to the More Onerous Elements of the Rules, Extensions of the Applicable Compliance Deadlines, and Streamlined Regulations

If the FCC rejects our proposal in favor of its prescriptive, *ex ante* privacy and data security framework, it should, consistent with similar privacy regimes:

- Exempt smaller providers from prescriptive specific data security requirements (while maintaining a flexible general data security standard) and add "the size of the BIAS provider" to the factors that the FCC must consider when assessing the reasonableness of a BIAS provider's security program;
- Exempt smaller providers from the more onerous elements of its customer approval framework by grandfathering existing customer consents and exempting smaller providers from the requirement to obtain additional approval where they do not share sensitive personal information with third parties for marketing purposes;
- Exempt smaller providers from several elements of the FCC's proposed data breach notification rule (as applied to voice and broadband services) by exempting smaller providers from the specific notification deadlines in favor of an "as soon as reasonably practicable" standard; and
- Exempt smaller providers from any customer dashboard requirements that it adopts pursuant to its notice and choice regulations.

These exemptions address and reduce the burdens that the proposed privacy rules would have on smaller providers, and align with the SBA Advocacy Office's request that the FCC adopt "exemptions for small BIAS providers wherever practicable."

The FCC also should extend the deadlines for smaller providers to comply with any new privacy and data security rules by at least one year beyond any general compliance deadline (*i.e.,* the date at which larger providers must comply with the rules). The FCC should commit to initiate a subsequent rulemaking together with or immediately after any order that results from this proceeding to determine whether to further extend the deadline and/or establish additional exemptions, and should further commit to rule on whether to extend the deadline or establish additional exemptions prior to the expiration of the general compliance deadline. The FCC often has extended effective dates for small entities in the context of its consumer protection regulations, including: (1) a three-year waiver for certain analog-only cable systems to comply with the emergency information rule; (2) a two-year delay to comply with the User Guide Requirements of the FCC's accessibility rules; (3) a one-year extension of the compliance deadline for the FCC's open Internet enhanced transparency rule, which it subsequently extended for another year; and (4) a six-month extension to implement requirements of the *2007 CPNI Order.*

Moreover, the FCC should rationalize and streamline its proposed rules to ensure that they are not too burdensome for smaller broadband providers by:

- Developing, with industry and other stakeholders, standardized notices with safe harbor protection that small providers can use to reduce enforcement risks, as well as the need to pay for outside counsel, consultants, and developers;
- Streamlining its proposed customer approval requirements to better align with consumer expectations and avoid disrupting existing customer relationships;
- Adopting a general data security standard and working with industry to establish and update best practices rather than imposing prescriptive data security rules;
- Tailoring any data breach notification requirements to ease burdens on broadband providers, including by adopting flexible deadlines for breach notification, limiting notifications to situations where consumer harm is reasonably likely, creating a one-stop-shop for breach reporting, and preempting state breach notification laws; and
- Harmonizing its rules *within* Section 222, but not across statutory provisions including Section 631 of the Cable Act, which would undermine consumer expectations and would upend providers' existing compliance regimes.

While a suite of extensions, exemptions, and rationalized rules would not be as effective as adopting rules consistent with the FTC framework, it would address the concerns of smaller providers and many others in the record—including the SBA—that the FCC's proposed rules go too far without adequately considering the burdens of its proposals on smaller providers.

ACA members have a strong record of protecting consumer data and complying with myriad state and Federal privacy and data security laws. Based on this experience, we urge the Commission to adopt the time-tested privacy framework employed by the FTC. It has proven valuable for consumers and imposes important but reasonable obligations on smaller broadband providers. We look forward to working with the Committee and the Commission as this process moves forward.

The CHAIRMAN. Thank you, Mr. Polka.

Next up is Professor Swire. And I apologize, I mispronounced your name——

Mr. SWIRE. It's happened before.

[Laughter.]

The CHAIRMAN.—during my introduction. That was from me not wearing these (referencing glasses). But, Professor Swire, please proceed.

STATEMENT OF PETER SWIRE, HUANG PROFESSOR OF LAW AND ETHICS, SCHELLER COLLEGE OF BUSINESS, GEORGIA INSTITUTE OF TECHNOLOGY

Mr. SWIRE. Thank you, Chairman Thune, and Ranking Member Nelson and members of the Committee. And thank you for the opportunity to testify today on the FCC's proposed privacy rule. As you said, my name is Peter Swire, not Swine. I teach at George Tech.

Today I'm testifying about a major research project that my coauthors and I issued this year called "Online Privacy and ISPs." It's 125 pages. It has pretty color illustrations. We tried to set out the facts for how this stuff works. Before our report came out, many of those supporting stronger privacy rules signed a letter stating that ISPs, "have a comprehensive view of consumer behavior," and they said, "that ISPs have a unique view in the online ecosystem because they connect the users to the Internet."

And our report documented two factual findings. First, ISP visibility into consumer online information is far from comprehensive

and will likely continue to decline, and the biggest reason is the huge growth in encryption.

Second, ISPs appear to lack unique insights into users' Internet activity. The biggest reason is that the data the ISPs see is generally not as detailed and insightful as that available to others in the Internet ecosystem. These two conclusions are surprising to many people on first encounter for understandable reasons based in history, but the facts have changed over time and will continue to do so.

My own work here began when the FCC invited me to testify over a year ago at their workshop on broadband consumer privacy. That day, the debates were about comprehensive and unique access, and I believe getting more facts would be useful.

I'll say just a word about my own role in this discussion. During 2009 and 2010, I worked in the White House on the National Economic Council. As part of that job, I signed what is sometimes called the "Obama Pledge," I will not engage in any lobbying of Federal officials while President Obama is in office. As a consequence, all of my writing about this privacy rulemaking has been factual, and I do not and have not advocated for any policy outcome.

As a related point, I know why I think our research has been helpful to those with different views about the policy issues here. For those who believe the proposed rule is too strict, and we heard several people today already, our research has corrected important misperceptions that policymakers might have had, and now we can decide based on current facts rather than previous impressions. And for those who support the FCC's proposed rules, such as Professor Ohm, I believe our research has also been useful. Before the working paper, much of the advocacy for the rule was based on factual claims that have not stood up to scrutiny, especially the claim that ISPs, because of their place in the ecosystem, see everything about a user's activity. Without the working paper, supporters of the rule faced a real risk the rule would be based on inaccurate facts, thus exposing the rule to risk of reversal in judicial review. And I believe the factual record now before the Commission is more nuanced and complete than it would have been.

So turning to these facts and the issue of whether there is comprehensive access, the most cited findings in our working paper concern the recent and rapid and historic rise in encrypted communications for the typical user. Just two years ago, in 2014, in February, 13 percent of the bits going through the U.S. backbone were encrypted. By this January, that number had soared to 49 percent, half the bits, and we expect it to be 70 percent by the end of this year.

And with the shift to HTTPS, which is the secure protocol, there are two main effects. First of all, the content gets encrypted. This is again for a majority of bits now today. And for years, the biggest privacy concern about ISPs is what was called "deep-packet inspection," and that was because ISPs technically can go deep into the packet to see the full content and not just the header. For encrypted communications, deep-packet inspection doesn't work anymore, it's encrypted, they can't get in.

Second, blocking of detailed URLs. HTTPS also blocks ISP access to the detailed URLs. With encryption, the ISP sees something like "www.example.com," but along with blocking content, encryption blocks all the details, such as "www.example.com/sensitivemedical condition." So a lot of the details get blocked, and that applies broadly to our e-mails now and social networks and web search.

The other topic is to discuss briefly whether ISPs have unique data, maybe because they're the bottleneck, as Professor Ohm mentioned, and whether they have unique insights. My written remarks discuss five categories of data: domain names, location information, IP addresses, subscriber information, and NetFlow or IPFIX information.

Sticking with domain names as the example, ISPs can see the general domains, such as "example.com," but so can a lot of others, and that's sort of the point here. The user's operating systems see it, the user's browser, the app that he or she is using, the advertising network, all the people with cookies in the system. Advertisers also have third parties who sell profiles based on where people surf. And so the point when it comes to domain names is that compared to other Internet actors, ISPs access only the domain names, that's third best, not as good as the content or the detailed URLs that others see.

So in conclusion, at a factual level, there are greater limits in ISP visibility than most people had assumed, and I had assumed when I began the research, and the FCC should base its conclusions on the ecosystem we have today and going forward rather than a simplified view of what ISPs used to be able to see.

My thanks to the Committee for the opportunity to speak here, and I look forward to your questions.

[The prepared statement of Mr. Swire follows:]

PREPARED STATEMENT OF PETER SWIRE, HUANG PROFESSOR OF LAW AND ETHICS, SCHELLER COLLEGE OF BUSINESS, GEORGIA INSTITUTE OF TECHNOLOGY

Chairman Thune, Ranking Member Nelson, and Members of the Committee, thank you for the opportunity to testify today on "How Will the FCC's Proposed Privacy Regulations Affect Consumers and Competition?" I am Peter Swire, the Huang Professor of Law and Ethics at the Scheller College of Business at Georgia Tech. I have worked intensively on privacy and cybersecurity issues in government, academia, and practice for over twenty years. A biography is attached to the end of this testimony.

In February of this year, my co-authors and I issued the 125-page Working Paper called "Online Privacy and ISPs: ISP Access to Information is Limited and Often Less Than That of Others."[1] My testimony today, based on reply comments filed this week with the FCC,[2] focuses on two principle factual findings arising from that research project:

(1) ISP visibility into consumer online information is far from comprehensive, and will likely continue to decline; and

(2) ISPs appear to lack unique insights into users' Internet activity.

These two conclusions, in my experience, are surprising to many people on first encounter. For understandable reasons based in history, many observers have believed that ISPs do have comprehensive and unique insights into users' Internet activity. Our research has sought to provide an accurate factual basis for consideration by the FCC and other policymakers about these topics. As discussed further below,

---

[1] Peter Swire, Justin Hemmings, and Alana Kirkland, *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others* (Feb. 29, 2016) available at *http://www.iisp.gatech.edu/working-paper-online-privacy-and-isps.*

[2] *https://www.fcc.gov/ecfs/filing/107062066122504/document/10706206612250467ca.*

we have researched the facts about ISP activity, and I do not take any position on the policy issues facing the FCC concerning broadband privacy.

This testimony first discusses the context for our research project. It next discusses the limits on the comprehensiveness of ISP visibility into consumer behavior, notably due to the historic rise in encrypted communications. It concludes by examining claims that ISPs have unique insight into users' Internet activity.

1. The Context for the Research Project

I briefly discuss the origins of the research project in 2015, and the chronology of work product through the testimony today.

A. The Origins of the Research Project

My research into ISP access to user data began with the request from the Federal Communications Commission to participate in its April 28, 2015, Public Workshop on Broadband Consumer Privacy.[3] In connection with that Workshop, I was asked by a senior FCC official about a prominent dispute during the workshop—advocates for stricter privacy regulation essentially argued that ISPs have "comprehensive" access to consumer online information, while the ISPs instead emphasized the limited data to which they have access. In response, I answered that this was actually a factual question—research could illuminate the extent to which ISPs do or do not have "comprehensive" access.

My research project has sought to shed light on the "comprehensive" access and related issues. As disclosed from the start, in addition to funding from Georgia Tech-related sources, funding also came from Broadband for America, a trade association that includes major ISPs. At each stage, my co-authors and I have had complete editorial discretion—the views expressed are our own. To underscore our commitment to accurate research, we have asked for public comments about any factual inaccuracies. Our Working Paper in February 2016 held up very well to scrutiny. Our May 2016 comments to the FCC included detailed responses to comments, including deletion of two sentences (out of the 125-page report) that we concluded we could not support.

As someone who has often previously provided policy recommendations concerning privacy issues, I provide some detail about why my work on this topic has been factual rather than making any policy recommendations about what the FCC should do in its privacy rulemaking. I am under binding obligations that arise from my role as Special Assistant to President Obama for Economic Policy in 2009–2010. As a condition of that employment, I signed what is sometimes called the "Obama Pledge"—I will not engage in any lobbying of Federal officials while President Obama remains in office. *As a consequence, my writing about the FCC privacy rulemaking has been factual, and I do not and have not advocated for any policy outcome in the proceeding.*

As a related point, I note the role that our research has played both for those concerned the FCC's proposed privacy rule is too strict as well as those who support the FCC's proposed rule. For those concerned that the FCC's proposed rule is too strict, I believe our research has served a distinctly useful role—the public debate had often assumed that ISPs have comprehensive insights into user online activity, but in fact that is not so. The research, most clearly concerning the rising use of encryption, thus has corrected important misperceptions, prompting policymakers to decide based on current facts rather than false impressions. For those who support the FCC's proposed rule, I submit that our research has also served a distinctly useful role. Prior to our Working Paper, a substantial part of the advocacy for the rule had been based on factual claims that have not stood up to scrutiny, especially the claim that ISPs, due to their place in the Internet ecosystem, see "everything" about a user's Internet activity. In the absence of our Working Paper, proponents of the rule faced a risk that the rule would be based on inaccurate facts, thus exposing the rule to the risk of reversal during the process of judicial review.

B. The Chronology Related to the Research Project

Here is the chronology related to our research project:

1. As discussed above, in April 2015, the FCC invited me to participate as a panelist in its Public Workshop on Broadband Internet Privacy. The Workshop notably featured the debate about the extent to which ISPs have "comprehensive" access to user online information. Shortly thereafter, we began our research project on the topic.

[3] My statement is at *https://peterswire.net/wp-content/uploads/Swire__FCC-testimony__CPNI__04__27__15.pdf.*

2. In January 2016, over fifty public interest groups signed a letter urging the FCC to enact a broadband privacy rule, stating that ISPs have a "*comprehensive* view of consumer behavior," and "have a *unique* role in the online ecosystem" due to their role in connecting users to the Internet (emphasis supplied).[4]
3. In February, we issued the Working Paper on "Online Privacy and ISPs: ISP Access to Information is Limited and Often Less Than That of Others."[5] We submitted a slightly revised version as initial comments to the FCC, including with an appendix that documents that our initial draft is factually accurate based on expert review.[6]
4. Several comments in the wake of our Working Paper modified the claim that ISPs have a "comprehensive" view to a revised statement that ISPs have a "comprehensive view of *unencrypted* traffic,"[7] (emphasis supplied) an important change because a majority of non-video Internet traffic is already encrypted today and there are strong trends toward greater encryption. Comments also emphasized types of data where ISPs may have unique advantages, such as the time of user log-in and the number of bits uploaded and downloaded.
5. On July 6, we submitted reply comments to the FCC, providing additional facts and insights to support our view that ISPs lack comprehensive knowledge of or unique insights into users' Internet activity.[8] The key parts of the reply comments are laid out in this testimony today. As with our February Working Paper, the reply comments and this testimony take no position on what rules should apply to ISPs and other players in the Internet ecosystem going forward. As we did in February, we will receive comments on the Georgia Tech Institute of Information Security and Privacy Website, and publish edits or corrections if needed.

2. ISP Visibility into Consumer Online Information is Far From Comprehensive, and Will Likely Continue to Decline

Our February Working Paper informed the public debate by documenting how encryption is limiting the possibility of ISP's viewing much of the content and the detailed URLs accessed by consumers. The trend toward greater encryption has continued since February, including the recent Apple announcement that apps in the iOS ecosystem must be encrypted by the end of 2016. The growing use of encryption and other developments mean that ISP visibility is likely to continue to decline during the period when any new FCC broadband privacy rule would go into effect.

A. The Trend Toward Encryption is Continuing

The most-cited findings of our Working Paper concern the recent and rapid rise in encrypted connections for the typical user, most notably by use of the HTTPS (secure HTTP) protocol. As we reported in our Working Paper, HTTPS traffic in the U.S. Internet backbone was 13 percent in February 2014. That number rose to 49 percent by January 2016, an historic shift. Sandvine estimates that figure will grow

---

[4] Letter from Access, *et al.,* to Tom Wheeler, Chairman, Federal Communications Commission (Jan. 20, 2016) available at *https://www.publicknowledge.org/assets/uploads/documents/Broadband_Privacy_Letter_to_FCC_1.20.16_FINAL.pdf.*

[5] 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://www.iisp.gatech.edu/working-paper-online-privacy-and-isps.*

[6] Comment of Peter Swire, In the Matter of: Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16–106 (May 24, 2016) available at *https://www.fcc.gov/ecfs/filing/60001926727.*

[7] *See, e.g.,* FCC Overreach: Examining the Proposed Privacy Rules: Hearing Before the Subcomm. on Commc'ns and Tech. of the H. Comm. on Energy and Commerce, 114th Cong. 3 (2016) (statement of Paul Ohm, Prof., Georgetown University Law Center) ("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."*) (emphasis added) available at *https://energycommerce.house.gov/hearings-and-votes/hearings/fcc-overreach-examining-proposed-privacy-rules, Examining the Proposed FCC Privacy Rules: Hearing Before the Subcomm. on Privacy, Tech. and the Law of the S. Comm. on the Judiciary,* 114th Cong. 1 (2016) (statement of Tom Wheeler, Chairman, Federal Communications Commission) (". . . an ISP has a broad view of all of its customers' *unencrypted* online activity") (emphasis added) available at *http://www.judiciary.senate.gov/meetings/examining-the-proposed-fcc-privacy-rules,* Comments of Public Knowledge, *et al.,* In the Matter of: Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16–106, 19–22 (May 27, 2016) (discussing why traffic remains largely unencrypted) available at *https://www.fcc.gov/ecfs/filing/60001974141/document/60002080037.*

[8] *https://www.fcc.gov/ecfs/filing/107062066122504/document/10706206612250467ca.*

to 70 percent of global Internet traffic by the end of 2016,[9] and encryption will become increasingly ubiquitous in the next five to ten years.[10] Some of the continuing growth in encrypted bits is due to the decision of high-volume video providers such as Netflix to shift to encryption. As discussed in the Working Paper, however, a majority of non-video traffic is already encrypted, including widespread encryption for potentially revealing activities such as e-mail, text messages, video conversations, social networks, and web search.

The Working Paper provides diagrams and detailed explanations of what changes with the shift from HTTP to the encrypted HTTPS protocol. The shift to HTTPS has two main effects, the shift to encrypted content and blocking of detailed URLs.

i. *The shift to encrypted content.* Based on my professional experience, the most prominent privacy concerns about ISPs for the past twenty years have been about "deep-packet inspection" (DPI). When an ISP uses DPI, then the ISP can go "deeply" into the packet, examining the full content in contrast to the header information about where the packet should go. Privacy experts have long expressed concerns that ISP examination of all of a user's content could reveal a great deal of sensitive personal information.[11] Notably, for encrypted communications, DPI does not work. Even if ISPs sought to profile customers based on content, the use of HTTPS blocks the ISP's access to the content.[12] In short, the rise of HTTPS provides technical assurances that address the longest-voiced privacy concern about ISPs.

ii. *Blocking of detailed URLs.* Along with blocking ISP access to content, HTTPS blocks ISP access to detailed URLs. By contrast, ISPs continue to see the domain itself, such as *www.example.com.* Compared to the domain, detailed URLs typically reveal more granular detail about a user's interests and communications. For a news site, the detailed URL is typically more revealing (*www.OnlineNewspaper.com/PoliticalNewsStory*) than the domain itself (*www.OnlineNewspaper.com*). As another example, the major search engines have shifted to HTTPS. With HTTP search, information known as "HTTP refer" would reveal the search terms to the ISP. With HTTPS search, however, ISPs can no longer see the search terms. As Professor Neal Richards has explained, more granular information provides greater risks to what he calls "Intellectual Privacy," or the ability of the organization gathering the data to make inferences about a person's interests and personality.[13] Consistent with this view, Federal courts have found content and detailed URLs deserving of stricter legal protection under the Electronic Communications Privacy Act than the domain itself.[14]

Comments made after release of the Working Paper have agreed with the growth of encryption and the fact that HTTPS blocks content and detailed URLs, and have focused instead on other points. A report from Upturn, for instance, correctly states that while HTTPS is prevalent on some of the most popular websites, the majority

---

[9] "2016 Global Internet Phenomena, Latin America & North America," *Sandvine,* 1, Jun. 2016 ("Sandvine forecasts that 70 percent of global Internet traffic will be encrypted in 2016, with many networks expected to exceed 80 percent") available at *https://www.sandvine.com/trends/global-internet-phenomena/*.

[10] Larry Downes, *The Downside of the FCC's New Internet Privacy Rules,* HARVARD BUSINESS REVIEW (May 27, 2016) available at *https://hbr.org/2016/05/the-downside-of-the-fccs-new-internet-privacy-rules.*

[11] *See, e.g.,* Center for Democracy and Technology, *Online Behavioral Advertising: Discussing the ISP-Ad Network Model* (Sep. 18, 2008) available at *https://cdt.org/insight/online-behavioral-advertising-discussing-the-isp-ad-network-model/,* Declan McCullagh, *Web Monitoring for Ads? It may be Illegal,* C/NET (May 19, 2008) available at *http://www.cnet.com/news/web-monitoring-for-ads-it-may-be-illegal/,* Grant Gross, *ISP Backs off of Behavioral Ad Plan,* PCWORLD (Jun. 24, 2008) available at *http://www.pcworld.com/article/147508/article.html.*

[12] Professor Nick Feamster, in his comments to the FCC, said "DPI is typically not widely deployed in many ISP networks," and, "contrary to some conventional beliefs, ISPs often do not retain much of the data that they collect because the cost of doing so can be substantial." Taken together with the increasing prevalence of HTTPS, these comments from Professor Feamster provide the basis for concluding that DPI going forward is much less of a privacy concern than has often been asserted in ISP privacy debates. Comment of Nick Feamster, In the Matter of: Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16–1606, 6 (May 27, 2016) available at *https://www.fcc.gov/ecfs/filing/60001973502/document/60002079367.*

Professor Feamster discusses other possible privacy risks in his comments, which are discussed below.

[13] Neil Richards, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE (2015).

[14] In Re: Google Inc. Cookie Placement Consumer Privacy Litigation, 806 F.3d 125, 138 (3rd Cir. 2015) available at *http://www2.ca3.uscourts.gov/opinarch/134300p.pdf.*

of total websites remain unencrypted, including a large percentage of health, news, and shopping sites.[15] In considering these statistics, we note that the number of bits transferred is an important measure of whether users' communications are typically encrypted, including for important communications such as e-mails, search, and social networks. Users do a large portion of their Internet activity on the most popular such sites, where encryption has often already been adopted.

News and a wide variety of other sites that rely on display advertising. Change is occurring for sites that rely on display advertising, including news sites, where encryption adoption has been slow to date. The announcement this April that *Wired Magazine* is shifting to HTTPS is instructive. *Wired Magazine* has reported that *every* advertisement placed on a page must be delivered via HTTPS for the page to work properly.[16] *Wired Magazine* is thus staging its deployment of HTTPS, working with its advertising providers to make the transition. This effort by *Wired Magazine* as an early adopter is a promising sign that display advertising-based sites will shift to HTTPS. Once an advertising company has upgraded to HTTPS to serve *Wired Magazine* and other early adopters, there is a positive spillover effect—the advertising company can then support HTTPS for the other news, shopping, health, and other sites where it places display advertisements.

In considering the prevalence of encryption under any FCC broadband privacy rule, policymakers should move beyond a static view of the state of encryption today, and consider the overall trend toward increasingly ubiquitous deployment of encryption, including for the "long tail" of websites that have lower user traffic.

In 2016, signs of the expansion of encryption include:

- *Apple is requiring HTTPS for iOS applications.* In June, Apple announced at its Worldwide Developers Conference that app developers will be required to connect over HTTPS servers when transferring data online.[17] App developers must make these changes by January 1, 2017, and new apps will not be listed on the App Store unless they are encrypted.
- *Progress for the Let's Encrypt Project, to make implementing HTTPS easier.* The Let's Encrypt project is a free, automated, and open certificate authority.[18] The organization hosts a support community for those seeking to implement Let's Encrypt certificates and to navigate the obstacles to encrypting a website.[19] In March, Let's Encrypt issued its one millionth certificate and reported a rate of growth of 100,000 certificates per week.[20] The success of the project, thanks in part to the support of numerous sponsors from public interest groups and technology companies,[21] is raising encryption adoption for smaller websites.[22]
- *WordPress has enabled HTTPS by default for hosted content.* WordPress announced in April that it will provide HTTPS by default for hosted content, providing increasingly available and accessible encryption for the "long tail" of sites.[23] By utilizing the Let's Encrypt project, WordPress was able to automatically deploy and manage HTTPS for the over 1 million custom domains hosted through the company.[24] The announcement by WordPress illustrates the growth of encryption and how encryption is becoming easier to implement. In addition,

---

[15] "What ISPs Can See: Clarifying the Technical Landscape of the Broadband Privacy Debate," *Upturn,* 3–4, Mar. 2016, available at *https://www.teamupturn.com/reports/2016/what-isps-can-see.*

[16] Zack Tollman, *We're Going HTTPS: Here's How Wired is Tackling a Huge Security Upgrade,* WIRED (Apr. 28, 2016) available at *https://www.wired.com/2016/04/wired-launching-https-security-upgrade/.*

[17] Kate Conger, *Apple Will Require HTTPS Connections for iOS Apps by the End of 2016,* TECHCRUNCH (Jun. 14, 2016) available at *https://techcrunch.com/2016/06/14/apple-will-require-https-connections-for-ios-apps-by-the-end-of-2016/.*

[18] *About,* LET'S ENCRYPT (last visited Jun. 24, 2016) available at *https://letsencrypt.org/about/.*

[19] *Let's Encrypt Community Support,* LET'S ENCRYPT (last visited Jun. 24, 2016) available at *https://community.letsencrypt.org/.*

[20] Josh Aas, *Our Millionth Certificate,* LET'S ENCRYPT (Mar. 8, 2016) available at *https://letsencrypt.org/2016/03/08/our-millionth-cert.html.*

[21] *Current Sponsors,* LET'S ENCRYPT (last visited Jun. 24, 2016) available at *https://letsencrypt.org/sponsors/.*

[22] *https://letsencrypt.org/2016/03/08/our-millionth-cert.html.*

[23] *HTTPS Everywhere: Encryption for All WordPress.com Sites,* WORDPRESS (Apr. 8, 2016) available at *https://en.blog.wordpress.com/2016/04/08/https-everywhere-encryption-for-all-wordpress-com-sites/.*

[24] *Id.*

with 26.3 percent of all content management systems running WordPress,[25] the shift would appear to provide a competitive advantage for WordPress compared to other hosting services, incentivizing other services to offer easy-to-use encryption tools.

- *The Federal Trade Commission has emphasized the importance of encrypting Internet of Things (IoT) devices.* In January, an FTC report strongly recommended encryption of confidential consumer information transmitted by IoT devices.[26] The FTC gave notice that companies face the risk of enforcement action if they fail to encrypt their devices and communications.[27] The public threat of enforcement action provides an incentive for companies to deploy encryption for the IOT, where encryption adoption has previously lagged.
- *As discussed above, Wired.com's switch to full HTTPS will make it easier for news and a wide variety of other display advertising-supported sites to follow suit.*

Our original Working Paper provided extensive additional information about the trend toward prevalent use of encryption.[28] As one notable example:

- *Google Search ranks HTTPS higher.* In 2014, Google announced it would use HTTPS as a ranking signal as part of its "HTTPS Everywhere" campaign. In light of Google's large market share in search, website owners thus have an incentive to enable HTTPS in order to gain better search rankings and subsequent page views. Together with developments such as the "Let's Encrypt" campaign, this means that even small website owners: (i) have an incentive to use HTTPS; and (ii) increasingly have the ability to do so.

B. The Rise of Mobile and Other Reasons for Limits on ISP Visibility

Beyond encryption, our Working Paper discussed other limits on ISP visibility into consumer online information, notably the shift toward mobile access to the Internet. Historically, many consumers did most or all of their Internet access from home, using an unencrypted connection through a single ISP. We believe that this mental model of Internet use is a reason that many people have believed that an ISP does have a "comprehensive" view of its customers' Internet activity. The rise of smartphones, tablets, and other mobile computing, however, places limits on an ISP's ability to gain such a view, in addition to the limits that come from prevalent encryption:

- *Mobile is becoming the leading way to access the Internet.* As our Working Paper noted, the number of mobile Internet-enabled devices today is as large as traditional laptops and desktops combined,[29] and the market share of desktop computers is continuing to fall.[30] Today, the great majority of Internet users own mobile devices.[31]
- *Mobile traffic is offloaded to WiFi networks.* By 2014, an estimated 46 percent of all data traffic shifted to WiFi networks,[32] growing to an estimated 60 per-

---

[25] Darren Pauli, *WordPress Pushes Free Default SSL for Hosted Sites,* THE REGISTER (Apr. 11, 2016) available at *http://www.theregister.co.uk/2016/04/11/wordpress_pushes_free_default_ssl_encrypts_26_of_the_webs_cmses/*.

[26] "Internet of Things: Privacy & Security in a Connected World," *Federal Trade Commission,* 27–28 (Jan. 2015) available at *https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.*

[27] *Id.* at 30.

[28] Peter Swire, *et al., Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others,* 28–30 (Feb. 29, 2016) available at *http://www.iisp.gatech.edu/working-paper-online-privacy-and-isps.*

[29] Angela Moscaritolo, *Tablets to Make Up Half the PC Market in 2014,* PCMAG (Nov. 26, 2013) available at *http://www.pcmag.com/article2/0,2817,2427623,00.asp.*

[30] Robert McMillan, *PC Sales Continue to Fall,* WALL ST. J. (Jul. 9, 2015) available at *http://blogs.wsj.com/digits/2015/07/09/pc-sales-continue-to-fall/,* Jordan Weissman, *The End of the Home Computer: Why PC Sales Are Collapsing,* THE ATLANTIC, (Apr. 11, 2013), available at *http://www.theatlantic.com/business/archive/2013/04/the-end-of-the-home-computer-why-pc-sales-are-collapsing/274899/*.

[31] At the beginning of 2015, one study showed that 91 percent of users owned a desktop or laptop. Smartphone use has climbed sharply, to 80 percent. In addition to desktops, laptops, and smartphones, nearly 50 percent of users reported owning a tablet. See Jason Mander, *80 percent of Internet users own a smartphone,* GLOBALWEBINDEX (Jan. 5, 2015) available at *http://www.globalwebindex.net/blog/80-of-internet-users-own-a-smartphone.*

[32] "Cisco Visual Networking Index, Forecast and Methodology, 2014–2019 Working Paper," *Cisco* (May 27, 2015) available at *http://www.cisco.com/cen/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.html.*

cent of all mobile data traffic by 2020.[33] The ISP that connects the WiFi network to the Internet (WiFi ISP) is often different from the ISP that connects the mobile user to the Internet (subscriber ISP). In such cases, the subscriber ISP has no visibility into the subscriber's Internet activity connected through the WiFi network.[34]

- *Consumers switch carriers.* According to FCC statistics, 82 percent of mobile broadband Internet users have a choice of at least four providers, and 98.8 percent have at least two.[35]According to the FCC, between a fifth and a third of wireless subscribers switch their carriers annually.[36] Consumers also switch wireline carriers, with one out of six subscribers switching wireline providers every year, and 37 percent of subscribers switching every three years.[37] Switching carriers cuts off the visibility of the old carrier, splitting the user's Internet history.
- *Consumers access the Internet through multiple mobile carriers.* Any given ISP loses visibility into the subscriber's Internet activity as the user moves between cellular connections and WiFi hotspots during the day. For example, they may connect using their home and work WiFi, then free WiFi in a coffee shop, then WiFi at a friend's house, any of which may use different ISPs.

In conclusion about whether ISPs have "comprehensive" visibility into user Internet activity, the prevalence of encryption and the shift to mobile computing put important limits today on ISPs' visibility. In addition, the role of both encryption and mobile computing will continue to grow in the coming years, during the period when any new rule would enter into effect.

3. ISPs Appear to Lack Unique Insights Into Users' Internet Activity

Public debate about privacy and ISPs has featured comments that ISPs "play a unique role in the online ecosystem"[38] and their position as an Internet "bottleneck" gives them unique access to privacy sensitive insights about users.[39] To clarify the role that ISPs play in the online ecosystem, our Working Paper explained the roles played by other online actors, including their access to sensitive personal information, devoting separate chapters to: social networks; search engines; webmail and messaging; mobile and other operating systems; interest-based advertising; and browsers, Internet video, and E-commerce.

In the reply comments and this testimony, we examine sources of data, raised by commenters, which are potentially available to ISPs. For each source of data, we look at the *visibility to others*—other actors in the online ecosystem often have access to the same or comparable data as that available to ISPs. We also look at the *insights available from data seen by the ISPs.* Looking at each category of data, the data available to ISPs appears to offer the same as or less insight than the data used by other actors. For instance, ISPs sometimes see "third-best" information: they can see the basic domain name a user visits (such as *www.example.com*) but not the encrypted content (what example.com sends to the user) or the detailed Uniform Resource Locator (URL) (such as *www.example.com/InterestingPageTitle*). Others in the Internet ecosystem, meanwhile, see the content and detailed URLs.

---

[33] "Juniper Mobile Data Onload & Offload Report," *Juniper* (Jun. 2015) available at *http://www.juniperresearch.com/researchstore/enablingtechnologies/mobile-data-onload-offload/wifi-small-cell-network-strategies.*

[34] If the Wifi ISP and subscriber ISP are the same, then that ISP can generally detect that the individual is using the same MAC address to connect to the ISP.

[35] "Seventeenth Annual Mobile Wireless Competition Report," *Federal Communications Commission,* DA 14–1862 ¶51, rel. Dec. 18, 2014, available at *https://apps.fcc.gov/edocs__public/attachmatch/DA–14–186 2A1.pdf*; "2015 Broadband Progress Report and Notice of Inquiry on Immediate Action to Accelerate Deployment," *Federal Communications Commission,* FCC 15–10 109, rel. Feb. 4, 2015, available at *https://apps.fcc.gov/edocs__public/attachmatch/FCC-15-10A1.pdf.*

[36] "Annual Report and Analysis of Competitive Market Conditions with Respect to Mobile Wireless, Including Commercial Mobile Services: Fifteenth Report," *Federal Communications Commission* (Jun. 27, 2011) available at *https://apps.fcc.gov/edocs__public/attachmatch/FCC-11-103A1.pdf.*

[37] "Broadband Decisions: What Drives Consumers to Switch-or Stick with-Their Broadband Internet Provider," *Federal Communications Commission* (Dec. 2010) available at *https://apps.fcc.gov/edocs__public/attachmatch/DOC-303264A1.pdf.*

[38] Letter from Access, *et al.,* to Tom Wheeler, Chairman, Federal Communications Commission (Jan. 20, 2016) available at *https://www.publicknowledge.org/assets/uploads/documents/Broadband__Privacy__Letter__to__FCC__1.20.16__FINAL.pdf.*

[39] *FCC Overreach: Examining the Proposed Privacy Rules: Hearing Before the Subcomm. on Commc'ns and Tech. of the H. Comm. on Energy and Commerce,* 114th Cong. 3 (2016) (statement of Paul Ohm, Prof., Georgetown University Law Center) available at *http://docs.house.gov/meetings/IF/IF16/20160614/105057/HHRG-114-IF16-Wstate-OhmP-20160614.pdf.*

Before discussing the relevant categories of data, I note the difference between having access to unique *data* and having access to unique *insights* about users. Any two companies, at some level, have unique *data*—they have at a minimum different customer lists and different specific interactions with their customers. For purposes of informing the record about online privacy, the discussion here provides detail about the uniqueness or lack thereof of several categories of *data* available to ISPs. Our analysis here and in the Working Paper primarily focuses, however, on whether ISPs have unique *insights* about their customers—to what extent their position in the online ecosystem may mean that ISPs can learn more about consumers than others can. For commercial businesses, the focus on insight is key. These insights are what provide economic value, including for internal proprietary purposes, to sell more valuable advertisements, or to sell to other parties such as data brokers. To date, of the top 10 ad-selling companies, which earn over 70 percent of the total online advertising dollars, none gained their current position by providing broadband Internet service.[40] For the reasons discussed below, ISPs, based on our review, appear to lack unique insights about consumer online activity because other players in the Internet ecosystem can collect the same (or equivalent) information.

I next examine categories of Internet activity data identified by commenters, which are sometimes or always available to ISPs. For each category, I provide: (i) the type of data; (ii) a description of who other than ISPs has visibility, including in some cases data being considered already "public"; (iii) discussion of the quality of insights that the available data may provide about users; and, (iv) other discussion.

- *Domain names.* As discussed above, with HTTPS, general domain information is visible to the ISP (such as *www.example.com*), while the content (what *www.example.com* sends to the user) or the detailed URL (such as *www.example.com/InterestingPageTitle*) are not for encrypted traffic.
  - Visibility to others: Many or all of the domain names a user visits are available to others, including the user's operating system, the user's browser or application, and advertising networks and other third parties with cookies or services that are present on the page being visited.[41] Third parties sell profiles of users based on the domains and/or detailed URLs they visit.
  - Insights: The domain names a user visits are not as revealing as the content accessed or full URLs. Some domain names, however, can reveal information that would be considered sensitive by most privacy experts, such as *www.SensitiveHealthSite.com* or *www.UnusualPoliticalViews.com.*
  - Discussion: Compared to other Internet actors, ISP access to domain names can be seen as "third-best" information, less revealing than content or detailed URLs. With HTTPS, ISPs cannot see encrypted content or detailed URLs, whereas that more detailed information is available to others, including the operator of the page being visited, the operating system, and the browser or application.
- *Location information.* As discussed in the Working Paper, mobile carriers can estimate a user's location through the process of "trilateration," based on the distance from the user to three or more cell towers.[42]
  - Visibility to others: Commercial services today principally determine location based on information from the global positioning system (GPS) or Bluetooth. When GPS is switched on, at a minimum the operating system can determine location. A large number of popular mobile apps gather detailed location information. Third parties sell profiles based on location information. Moreover, mobile operating systems and apps can collect trilateration results using the known locations of cell towers and WiFi networks.
  - Insights: Most privacy experts consider precise location history to be sensitive information.

---

[40] Peter Swire, *et al., Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others,* 4 (Feb. 29, 2016) available at *http://www.iisp.gatech.edu/working-paper-online-privacy-and-isps.*

[41] Moreover, the domain resolution process was expressly designed to be public. Comment of Manos Antonakakis, *et al.,* In the Matter of: Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16–106, 6 (May 27, 2016) available at *https://www.fcc.gov/ecfs/filing/60001973444/document/60002079307.*

[42] Peter Swire, *et al., Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others,* 70–72 (Feb. 29, 2016) available at *http://www.iisp.gatech.edu/working-paper-online-privacy-and-isps.*

- Discussion: As discussed in our Working Paper, trilateration results in rough location information compared to GPS or Bluetooth location tracking, which is significantly more precise and available to the user's device, operating system, and any application or service with access to those sensors.[43]

- *Subscriber information.* ISPs often learn subscriber information, such as name, address, credit card information, and Social Security number.
  - Visibility to others: Many players in the online ecosystem gain access to data such as name, address, and credit card information. Companies that seek information under the Fair Credit Reporting Act (such as for lending, employment, or insurance purposes) also learn Social Security number. A company that has name and address can often purchase additional profiling information, a process that Jules Polonetsky of the Future of Privacy Forum calls "the democratization of data."[44]
  - Insights: Many privacy experts, along with the FTC in its report on Data Brokers,[45] have expressed concerns about the amount of personal information that can be purchased when a company knows subscriber information such as name and address.
  - Discussion: The insights that ISPs can gain from subscriber information are available to many others in the Internet ecosystem.

- *IP addresses.* ISPs use Internet Protocol addresses to connect an individual device to the Internet. IP addresses are assigned by the ISP.[46]
  - Visibility to others: IP addresses are visible to every carrier between the customer and the relevant content provider. Operating Systems, websites, applications, content/website providers, browser plug-ins, and software development kits can all collect IP address information.[47] E-commerce sites can combine IP addresses of visiting customers with the names and addresses of those customers, along with purchase history. Logs of IP addresses are commonly used for purposes other than marketing, including for cybersecurity. Third parties sell correlations of IP addresses with cookies and other information. All these channels enable other actors to replicate IP address information that an ISP can access through providing its services.
  - Insights: IP addresses can give clues to information such as a user's location, commonly visited sites, and usage patterns (including time of log-in, amount uploaded and downloaded, and some information on protocols used).
  - Discussion: Many of the insights that ISPs can gain from IP addresses are available to many others in the Internet ecosystem.

- *IPFIX Data/Netflow.* The Internet Protocol Flow Information Export (IPFIX)[48] and NetFlow[49] are protocols for monitoring network traffic.[50] For any individual IP flow, or "sequence of packets sent from a particular source to a par-

---

[43] *Id.*

[44] Comment of The Future of Privacy Forum, In the Matter of: Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16–1606, 14–16 (May 27, 2016) available at *https://www.fcc.gov/ecfs/filing/60001981713/document/60002089525.*

[45] "Data Brokers: A Call for Transparency and Accountability," *Federal Trade Commission,* 47–49 (May 2014) available at *https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.*

[46] Number Resources, INTERNET ASSIGNED NUMBERS AUTHORITY (last visited Jul. 5, 2016) available at *https://www.iana.org/numbers.*

[47] *See, e.g.,* View IP Address, CHROME WEB STORE (last visited Jul. 5, 2016) available at *https://chrome.google.com/webstore/detail/view-ip-address/mfhcchbdblkggcenfmmpgkpgphfhfcbe?hl=en.*

[48] IPFIX is a protocol developed by the Internet Engineering Task Force as an open, universal standard for exporting Internet Protocol flow information and as an alternative to Cisco's proprietary NetFlow protocol. *See* RFC 5102—Information Model for IP Flow Information Export, INTERNET ENGINEERING TASK FORCE (Jan. 2008) available at *https://tools.ietf.org/html/rfc5102.*

[49] NetFlow is Cisco's proprietary protocol for exporting Internet Protocol flow information. The term "NetFlow" is often used interchangeably with IPFIX to refer to this type of protocol. *Introduction to Cisco IOS NetFlow—A Technical Overview,* CISCO (May 29, 2012) available at *https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.html.*

[50] *See id.*

ticular. . .destination,"[51] IPFIX can be used to record and store the start and end time for the flow, the number of bytes and packets in the flow, the protocol/type of connection (*e.g.,* TCP or UDP), and the source and destination of the flow.[52]

- Visibility to others: IP flow information is visible to each: network operator; ISP; transit provider; Internet backbone provider; and edge provider along the path between the end-user and the destination. The same IP flow information, as well as additional information, is visible to the user's operating system and applications. For other members of the ecosystem, this data can be aggregated through purchase from and sale to data brokers, including data linked to the IP addresses of a service's users.[53]
- Insights: Access to IPFIX/Netflow data may in some instances provide "side channel" information from these flows that can help in inferring end-user behavior such as whether they are browsing the web, streaming a video, or chatting with someone online. Comments state it is possible to "identify certain web page visits" or "information about what those packets likely contain"[54] from the IP flow information; to do this appears to require "finger printing" each website of interest[55] and the collection of a high fraction of the flows. In addition, concerning the statement that such information is stored as a "permanent record of these individual transactions,"[56] Professor Nick Feamster reports that IPFIX normally samples one out of every 1,000 packets for traffic statistics.[57] Thus, "many short flows may not be recorded whatsoever." Sampling this data would be an inefficient way to profile users compared to analysis of the actual content available to the operators of pages that users visit and others. Similarly, given the volume of connections and volume of websites, we are not aware of a business justification for creating a "permanent record" of all of IPFIX data for an ISP's users nor for maintaining an archive of website fingerprints (which change often and dynamically).
- Discussion: Professor Feamster also states: "even though IPFIX records contain no information about the actual content of communication, information such as volumes, sources, and destinations can sometimes reveal private information about user behavior." This data, along with other "side channel" inferences, is an example of what we believe is "third-best" advertising data—inferences based on information that provides less insight than content or detailed URLs. We are not aware of any evidence that these methods are currently widely used, let alone profitable,[58] for advertising. This data, however, is useful for purposes including network management, network security, and research.[59]

---

[51] *See* RFC 3697—IPv6 Flow Label Specification, INTERNET ENGINEERING TASK FORCE (Mar. 2004) available at *https://tools.ietf.org/html/rfc3697.*

[52] *Id.*

[53] Oracle, Little Blue Book: A Buyer's Guide, 84 (Dec. 2014) available at *http://www.bluekai.com/bluebook/assets__20150102/bluekai-little-blue-book.pdf.*

[54] "What ISPs Can See: Clarifying the Technical Landscape of the Broadband Privacy Debate," *Upturn,* 8, (Mar. 2016) ("It is possible to uniquely identify certain web page visits or otherwise reveal information about what those packets likely contain.") available at *https://www.teamupturn.com/reports/2016/what-isps-can-see.*

[55] Chen, Shuo; Side-Channel Leak in Web Applications: a Reality Today, a Challenge Tomorrow; *https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/WebAppSideChannel-final.pdf*

[56] *FCC Overreach: Examining the Proposed Privacy Rules: Hearing Before the Subcomm. on Commc'ns and Tech. of the H. Comm. on Energy and Commerce,* 114th Cong. 52 (2016) (testimony of Paul Ohm, Prof., Georgetown University Law Center) available at *http://docs.house.gov/meetings/IF/IF16/20160614/105057/HHRG-114-IF16-Transcript-20160614.pdf.*

[57] Comment of Nick Feamster, In the Matter of: Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16–1606, 3–4 (May 27, 2016) available at *https://www.fcc.gov/ecfs/filing/60001973502/document/60002079367.* Feamster also states: "even though IPFIX records contain no information about the actual content of communication, information such as volumes, sources, and destinations can sometimes reveal private information about user behavior." The discussion here has pointed out that access to the content of communications will provide greater insights than partial information about the types of data Feamster describes. *Id.* at 4.

[58] "What ISPs Can See: Clarifying the Technical Landscape of the Broadband Privacy Debate," *Upturn,* 8 (Mar. 2016) available at *https://www.teamupturn.com/reports/2016/what-isps-can-see.*

[59] Comment of Nick Feamster, In the Matter of: Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16–1606, 4 (May 27, 2016) ("Network operators may also share IPFIX data with researchers. I use IPFIX data collected at interconnection points to analyze utilization patterns. In another project related to DoS mitigation, we are using IPFIX data to better understand traffic attack patterns. In the past, we

Conclusion

In conclusion about whether ISPs have "unique" visibility into user Internet activity, the discussion here has pointed out the many places where other players in the Internet ecosystem receive the same (or equivalent) information about user actions. Concerning unique insights into user behavior, ISPs in many instances have access to data that is less revealing than content or other information about user activity available to the companies providing services to the user.

In conclusion, I thank the Committee for the opportunity to testify today, and would be glad to answer any questions.

Background of the witness

I am the Huang Professor of Law and Ethics at the Georgia Tech Scheller College of Business, with appointments by courtesy with the College of Computing and School of Public Policy. Consistent with university consulting rules, I am Senior Counsel with Alston & Bird, LLP.

I have been immersed in privacy and cybersecurity issues for two decades. In 2015, the International Association of Privacy Professionals, among its over 20,000 members, awarded me its Privacy Leadership Award. In 2013, I served as one of five members of President Obama's Review Group on Intelligence and Communications Technology. Prior to that, I was co-chair of the global Do Not Track process for the World Wide Web Consortium. I am Senior Fellow with the Future of Privacy Forum.

Under President Clinton, I served as Chief Counselor for Privacy, in the U.S. Office of Management and Budget. In that role, my activities included being White House coordinator for the HIPAA medical privacy rule, serving as White House representative to the privacy rulemaking process under the Gramm-Leach-Bliley Act, and helping negotiate the U.S.-E.U. Safe Harbor agreement for trans-border data flows. Under President Obama, I served as Special Assistant to the President for Economic Policy in 2009–2010.

I have testified on privacy and other issues before almost a dozen committees in the U.S. Congress, and worked closely with the Federal Trade Commission and other Federal agencies on privacy and cybersecurity issues. In 2011, the Federal Communications Commission asked me to summarize and comment on the day's proceedings for its Workshop on Location Information. Further information is available at *www.peterswire.net.*

---

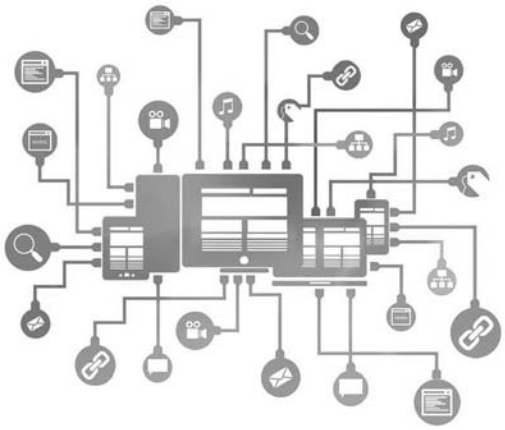
have also used IPFIX traffic traces from access ISPs to design and validate algorithms to detect botnets, large networks of compromised machines. Most recently, I have been using IPFIX data collected at the interconnection points from seven access ISPs in the United States—covering 50 percent of the U.S. broadband subscriber population—to explore the characteristics and patterns of utilization between access ISPs and edge providers. Interestingly, this type of project that provides *exactly* the type of insight and analysis that the FCC is increasingly paying attention to. Preventing ISPs from sharing this type of data with researchers would impede progress on this research.") available at *https://www.fcc.gov/ecfs/filing/60001973502/document/60002079367.*

ATTACHMENT

Complete article can be found at: *http://www.iisp.gatech.edu/sites/default/files/images/online—privacy—and—isps.pdf*

ONLINE PRIVACY AND ISPS:

ISP Access to Consumer Data is Limited and Often Less than Access by Others



Peter Swire, Associate Director, The Institute for Information Security & Privacy at Georgia Tech; Huang Professor of Law, Georgia Tech Scheller College of Business; and Senior Counsel, Alston & Bird LLP

Justin Hemmings, Research Associate, Georgia Tech Scheller College of Business and Policy Analyst, Alston & Bird LLP

Alana Kirkland, Associate Attorney, Alston & Bird LLP

A Working Paper of
The Institute for Information Security & Privacy at Georgia Tech

May 2016


A Working Paper of
The Institute for
Information
Security & Privacy
at Georgia Tech
May 2016

Preface

Online Privacy and ISPs:
ISP Access to Consumer Data is Limited and Often Less than Access by Others

This Working Paper provides a detailed, factual description of today's online ecosystem for the United States, with attention to user privacy and the data collected about individual users. The Working Paper addresses a widely-held, but mistaken view about Internet Service Providers ("ISPs") and privacy. That view asserts that ISPs have comprehensive and unique access to, and knowledge about, users' online activity because ISPs operate the last mile of the network connecting end users to the Internet. Some have cited this view to suggest that ISPs' collection and use of their customers' online data may justify heightened privacy restrictions on ISPs.

This Working Paper takes no position on what rules should apply to ISPs and other players in the Internet ecosystem going forward. But public policy should be consistent and based on an up-to-date and accurate understanding of the facts of this ecosystem. The Working Paper addresses two fundamental points. First, ISP access to user data is not *comprehensive* – technological developments place substantial limits on ISPs' visibility. Second, ISP access to user data is not *unique* – other companies often have access to more information and a wider range of user information than ISPs. Policy decisions about possible privacy regulation of ISPs should be made based on an accurate understanding of these facts.

Technological Developments Place Substantial Limits on ISPs' Visibility into Users' Online Activity:

1. **From a single stationary device to multiple mobile devices and connections.** In the 1990s, a typical user accessed the Internet from a single, stationary home desktop connected by a single ISP. Today, in contrast, the average Internet user has 6.1 connected devices, many of which are mobile and connect from diverse and changing locations that are served by multiple ISPs. By 2014, 46 percent of mobile data traffic was offloaded to WiFi networks, and that figure will grow to 60 percent by 2020. Any one ISP today is therefore the conduit for only a fraction of a typical user's online activity.

2. **Pervasive encryption.** We present new evidence about the rapid shift to encryption, such as the HTTPS version of the basic web protocol. Today, all of the top 10 web sites either encrypt by default or upon user log-in, as do 42 of the top 50 sites. Based on analysis of one source of Internet backbone data, the HTTPS portion of total traffic has risen from 13 percent to 49 percent just since April 2014. An estimated 70 percent of traffic will be encrypted by the end of 2016. Encryption such as HTTPS blocks ISPs from having the ability to see users' content and detailed URLs. There clearly can be no "comprehensive" ISP visibility into user activity when ISPs are blocked from a growing majority of user activity.

3. **Shift in domain name lookup.** One integral function of ISPs has been to match the user's web address request to the correct domain and specific Internet Protocol ("IP") address. Today there is a still small, but growing, trend of Internet users utilizing proxy services that displace this traditional ISP function. Examples include Virtual Private Networks ("VPNs") and new proxy services offered by leading Internet companies. When a user accesses the Internet through an encrypted tunnel to one of these gateways, ISPs cannot even see the domain name that a user is visiting, much less the content of the packets they are sending and receiving.

Non-ISPs Often Have Access to More and a Wider Range of User Information than ISPs:

1. **Non-ISP services have unique insights into user activity.** At the same time that the above technological and marketplace developments are reducing the online visibility of ISPs, non-ISPs are increasingly gathering commercially valuable information about online user activity from multiple contexts, such as: (1) social networks; (2) search engines; (3) webmail and messaging; (4) operating systems; (5) mobile apps; (6) interest-based advertising; (7) browsers; (8) Internet video; and (9) e-commerce. This Working Paper explains the data flows and mechanisms for advertising for each of these contexts, many of which gather insights about users that are not available to ISPs. Traditional ISPs are not market leaders in any of these major areas; rather, they are just starting to compete in some of them.

2. **Non-ISPs dominate in cross-context tracking.** Each of the above-listed services and platforms gathers volumes of data about users, frequently with insights into content (social networks, webmail, etc.) and other information often characterized as sensitive in privacy debates. While it is analytically instructive to understand each service/platform, the real insights come from combining information from multiple services/platforms – what we call "cross-context tracking" linked to a particular user device or across devices. The 10 leading ad-selling companies earn over 70 percent of online advertising dollars, and none of them has gained this position based on its role as an ISP.

3. **Non-ISPs dominate in cross-device tracking.** Yesterday's desktop has evolved into today's tablets and smartphones, and tomorrow's innumerable devices in the Internet of Things. A growing share of advertising tracking targets the user across multiple devices. Market leaders are companies for whom users log in across multiple devices, such as smartphones, tablets, and laptops. Today, cross-device data collection from logged-in and not logged-in users is led by non-ISPs.

In summary, based on a factual analysis of today's Internet ecosystem in the United States, ISPs have neither comprehensive nor unique access to information about users' online activity. Rather, the most commercially valuable information about online users, which can be used for targeted advertising and other purposes, is coming from other contexts. Market leaders are combining these contexts for insight into a wide range of activity on each device and across devices.

Executive Summary

Executive Summary

Online Privacy and ISPs: ISP Access to Consumer Data Is Limited and Often Less than Access by Others[1]

This Working Paper provides a detailed, factual description of today's Internet ecosystem for the United States, with attention to user privacy and the data collected about individual users. For two decades, there have been complex policy discussions about how to protect users' privacy online while also enabling the provision of advertising-supported content and robust commercial activity on the Internet.[2]

This Working Paper is intended to provide information useful to Congress, federal agencies, and the general public in consideration of online privacy issues. Among other relevant fora, in 2015 the Federal Communications Commission ("FCC") issued its Open Internet Order, which brings Internet Service Providers ("ISPs") under the common carrier requirements of Title II of the Telecommunications Act.[3] Title II contains Section 222, which governs how telecommunications service providers use and disclose Customer Proprietary Network Information.[4] In April 2015, the FCC held a hearing on broadband Internet privacy, for which one of the authors of this Working Paper was invited to testify.[5]

This Working Paper grew out of the April hearing, where there were large factual disagreements about important aspects of online privacy for broadband services newly covered by Title II. At the hearing, FCC officials expressed interest in better understanding these facts. *This Working Paper, in response, is intended to provide a factual and descriptive foundation for making public policy decisions about the privacy framework that should apply to ISPs and other companies that collect and use consumers' online data.*[6]

---

1 The authors thank Marie Le Pichon for creating the Diagrams, which are under a Creative Commons Attribution 4.0 license and should be attributed to her. We also thank Brooks Dobbs and Addison Amiri for assistance on technological aspects of this Working Paper.

Research support for this Working Paper comes from Broadband for America, the Institute for Information Security and Privacy at Georgia Tech, and the Georgia Tech Scheller College of Business. The views expressed here are those of the authors.

2 Peter Swire, "Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information," U.S. Department of Commerce, Aug. 15, 1997, (http://papers.ssrn.com/sol3/papers.cfm?abstract_id=11472). This Working Paper addresses issues relevant to law and policy in the United States. Other nations have different privacy regimes, but this Working Paper does not specifically address practices outside of the U.S.

3 This Working Paper uses the familiar term Internet Service Provider ("ISP") in the way it is generally understood – an organization that connects users to the Internet. Discussions of data collected by an ISP refer to information received by a company specifically by virtue of its providing end users a connection to the Internet. In its Open Internet Order, the FCC used a somewhat different term: "Broadband Internet Access Services." The FCC defined these as a "mass-market" retail service by wire or radio that provides the capability to transmit data to and receive data from all or substantially all Internet endpoints, including any capabilities that are incidental to and enable the operation of the communications service, but excluding dial-up Internet access service. "In the Matter of Protecting and Promoting the Open Internet," *Report and Order*, FCC 15-24 app. A (2015) (hereinafter "The Open Internet Order").

4 The statutory cite is 47 U.S.C. §222. The FCC's regulations implementing Section 222 are at 47 C.F.R.§ 64.2001 *et seq.*

5 "Federal Communications Commission Workshop on Broadband Consumer Privacy," *Federal Communications Commission*, April 2015, (https://www.fcc.gov/news-events/events/2015/04/public-workshop-on-broadband-consumer-privacy); Peter Swire, "Comments to the FCC on Broadband Consumer Privacy," presented before the Federal Communications Commission Workshop on Broadband Consumer Privacy, April 2015, (https://transition.fcc.gov/cgb/outreach/FCC-testimony-CPNI-broadband.pdf).

6 Knowing that the facts can be complex and difficult to understand, we are creating a mechanism to receive factual comments, with the intention of correcting mistakes or lack of clarity where such exist. Comments can be submitted to comments@iisp.gatech.edu, and any updates will appear on the website of the Institute for Information Security and Privacy at Georgia Tech.

The Working Paper addresses a widely-held, but mistaken view about ISPs and privacy. The view asserts that ISPs have comprehensive and unique access to, and knowledge about users' online activity because they operate the last mile of the network connecting end users to the Internet. Certain consumer advocates and others have cited this view to suggest that ISPs' collection and use of their customers' online data may justify heightened privacy restrictions on ISPs.

This Working Paper takes no position on what rules should apply to ISPs and other players in the Internet ecosystem going forward. But public policy should be consistent and based on an up-to-date and accurate understanding of the facts of this ecosystem. The Working Paper addresses two fundamental points. First, ISP access to user data is not *comprehensive* – technological developments place substantial limits on ISPs' visibility. Second, ISP access to user data is not *unique* – other companies often have access to more information and a wider range of user information than ISPs. Policy decisions about possible privacy regulation of ISPs should be made based on an accurate understanding of these facts.

Technological Developments Place Substantial Limits on ISPs' Visibility into Users' Online Activity:

1. **From a single stationary device to multiple mobile devices and connections.** In the 1990s, a typical user accessed the Internet from a single, stationary home desktop connected by a single ISP. Today, in contrast, the average Internet user has 6.1 connected devices, many of which are mobile and connect from diverse and changing locations that are served by multiple ISPs.[7] By 2014, 46 percent of mobile data traffic was offloaded to WiFi networks, and that figure will grow to 60 percent by 2020.[8] Any one ISP today is therefore the conduit for only a fraction of a typical user's online activity.

2. **Pervasive encryption.** We present new evidence about the rapid shift to encryption, such as the HTTPS version of the basic web protocol. Today, all of the top 10 websites either encrypt by default or upon user log-in, as do 42 of the top 50 sites.[9] Based on analysis of one source of Internet backbone data, the HTTPS portion of total traffic has risen from 13 percent to 49 percent just since April 2014.[10] An estimated 70 percent of traffic will be encrypted by the end of 2016.[11] Encryption such as HTTPS blocks ISPs from having the ability to see users' content and detailed URLs. There clearly can be no "comprehensive" ISP visibility into user activity when ISPs are blocked from a growing majority of user activity.

3. **Shift in domain name lookup.** One integral function of ISPs has been to match the user's web address request to the correct domain and specific Internet Protocol ("IP") address. Today there is still a small, but growing, trend of Internet users utilizing proxy services that displace this traditional ISP function. Examples include Virtual Private Networks ("VPNs") and new proxy services offered by leading Internet companies. When a user accesses the Internet through an encrypted tunnel to one of these gateways, ISPs cannot even see the domain name that a user is visiting, much less the content of the packets they are sending and receiving.

---

7 "The Zettabyte Era – Trends and Analysis," *Cisco*, May 2015, (www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/VNI_Hyperconnectivity_WP.html).

8 "Cisco Visual Networking Index (VNI) Mobile Forecast Projects Nearly 10-fold Global Mobile Data Traffic Growth over Next Five Years," *Cisco*, Feb. 3, 2015, (http://newsroom.cisco.com/press-release-content?articleId=1578507).

9 *See* Appendix 1 to Chapter 1.

10 *See* Appendix 2 to Chapter 1.

11 "Sandvine: 70% of Global Traffic Will Be Encrypted In 2016," *Sandvine*, Feb. 11, 2016, (https://www.sandvine.com/pr/2016/2/11/sandvine-70-of-global-internet-traffic-will-be-encrypted-in-2016.html).

Non-ISPs Often Have Access to More and a Wider Range of User Information than ISPs:

1. **Non-ISP services have unique insights into user activity.** At the same time that the above technological and marketplace developments are reducing the online visibility of ISPs, non-ISPs are increasingly gathering commercially valuable information about online user activity from multiple contexts, such as: (1) social networks; (2) search engines; (3) webmail and messaging; (4) operating systems; (5) mobile apps; (6) interest-based advertising; (7) browsers; (8) Internet video; and (9) e-commerce. This Working Paper explains the data flows and mechanisms for advertising for each of these contexts, many of which gather insights about users that are not available to ISPs. ISPs are not market leaders in any of these major areas; rather, they are just starting to compete in some of them.

2. **Non-ISPs dominate in cross-context tracking.** Each of the above-listed services and platforms gathers volumes of data about users, often with insights into content (social networks, webmail, etc.) and other information often characterized as sensitive in privacy debates. While it is analytically instructive to understand each service/platform, the real insights come from combining information from multiple services/platforms – what we call "cross-context tracking" linked to a particular user device or across devices. The 10 leading ad-selling companies earn over 70 percent of online advertising dollars, and none of them has gained this position based on its role as an ISP.[12]

3. **Non-ISPs dominate in cross-device tracking.** Yesterday's desktop has evolved into today's tablets and smartphones, and tomorrow's innumerable devices in the Internet of Things. A growing share of advertising tracking targets the user across multiple devices. Market leaders are companies for whom users log-in across multiple devices, such as smartphones, tablets, and laptops. Today, cross-device log-in is led by non-ISPs.

In summary, based on a factual analysis of today's Internet ecosystem in the United States, ISPs have neither comprehensive nor unique access to information about users' online activity. Rather, the most commercially valuable information about online users, which can be used for targeted advertising and other purposes, is coming from other contexts such as social networks and search. Market leaders are combining these contexts for insight into a wide range of activity on each device and across devices.

Meeting Privacy and Other Goals for the Internet

The White House and leading regulatory agencies have expressed strong support both for privacy protection when individuals are online, and for effective uses of data about users' online activity. We briefly give examples of support both for uses of personal information and limits on such uses to frame the later description of modern online data collection and use.

The United States protects privacy with many detailed laws, regulations, enforcement regimes, self-regulatory codes, and in other ways.[13] The Obama Administration has emphasized the importance of privacy online in numerous ways, including in its announcement of a Consumer Privacy Bill of Rights, stating: "Privacy protections are critical to maintaining consumer trust in networked technologies."[14] The Federal Trade Commission ("FTC")

---

[12] "IAB Internet Advertising Revenue Report: 2015 First Six Month Results," *IAB & PwC*, Oct. 2015, (http://www.iab.com/wp-content/uploads/2015/10/IAB_Internet_Advertising_Revenue_Report_HY_2015.pdf).

[13] *See, e.g.*, Peter Swire & Kenesa Ahmad, *U.S. Private Sector Privacy: Law and Practice for Information Privacy Professionals*, International Association of Privacy Professionals (2012).

[14] "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy," *The White House*, Feb. 2012, (http://www.whitehouse.gov/sites/default/files/privacy-final.pdf).

has made privacy protection online a major priority.[15] As mentioned above, the FCC is now carefully studying privacy issues related to broadband Internet access services.

Along with privacy limits on data collection and use, there are benefits in our information age from gathering and using personal information. In its 2014 Big Data report, the Obama Administration discussed multiple benefits, such as improved fraud detection[16] and cybersecurity,[17] and "enormous benefits" associated with "targeted advertising."[18] That report stated: "Consumers are reaping the benefits of a robust digital ecosystem that offers a broad array of free content, products, and services.[19] Regulatory agencies have similarly recognized such benefits.[20]

With these introductory comments in mind, we next outline the 10 Chapters that accompany this Executive Summary, addressing specific parts of the online ecosystem. Appendix 1 to this Executive Summary explains key terms we use in this Working Paper, including: availability vs. use; content vs. meta-data; cross-context tracking vs. cross-device tracking; ISP vs. non-ISP; and visibility and seeing.

Chapter 1: Limited Visibility of Internet Service Providers into Users' Internet Activity

In providing the last-mile connection to the Internet for their customers, ISPs carry users' data traffic on their network. In most cases, ISPs have relatively accurate information about a user's name and billing address, and they may have users' credit card information and phone number. This Chapter explains the technological and market changes that have made ISP visibility into users' Internet activity far from comprehensive. We highlighted this Chapter's major findings above: (1) the shift from a single stationary device and ISP to multiple mobile devices and ISPs, (2) pervasive encryption, and (3) the shift in domain name lookup.

Of these, the recent and rapid shift to HTTPS and other forms of encryption is perhaps the clearest and simplest way to explain why ISPs today and in the future do not have "comprehensive" access to users' Internet activities. HTTPS blocks the possibility of ISP access to the content of users' activities – the technology called "deep packet inspection" does not work on encrypted communications. HTTPS also blocks the possibility of ISP access to detailed URLs, which can reveal granular details of a user's search or other online activities.

Taken together, the three technological developments described in this Chapter show fundamental changes in what information is even theoretically available in providing the last-mile connection – the job of an Internet Service Provider. In addition, the strong trends toward multiple and mobile devices and connections, encryption, and changes in Domain Name System ("DNS") lookup are likely to continue.

---

[15] At the time of writing, the most recent major FTC report is "Big Data: A Tool for Inclusion or Exclusion?" *Federal Trade Commission*, Jan. 2016, (https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf).

[16] Executive Office of the President, "Big Data: Seizing Opportunities, Preserving Value," *The White House*, May 2014, p. 39, (https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf).

[17] *Id.* at 40.

[18] *Id.* at 50.

[19] *Id.* at 41.

[20] As a recent example, FTC Chairwoman Ramirez recently discussed benefits of cross-device tracking, including continuity in services across multiple devices and providing consumers with in-store discounts derived from searches on home computers. FTC Chairwoman Edith Ramirez, "Opening Remarks of FTC Chairwoman Edith Ramirez, Cross-Device Tracking: An FTC Workshop," Nov. 16, 2015, (https://www.ftc.gov/system/files/documents/public_statements/881513/151116cross-devicetracking.pdf).

Diagram E-1 shows a funnel for what information is available about user activity going forward for ISPs. At the top are the multiple contexts discussed in the Working Paper, where different players in the online ecosystem see detailed URLs and content about user activity. Due to pervasive encryption, VPNs, and the other developments discussed here, technology often blocks ISP access to user traffic. Next, users are shifting to multiple devices and ISPs, so an ISP's connection to any one device is far less than complete, especially in the Internet of Things world we are rapidly entering. Finally, especially as WiFi hotspots become the majority of traffic, any one ISP only sees a fraction of the activity on any one device. In short, ISPs have far less than a comprehensive view of any user's Internet activity, and the rich information available to non-ISPs mean that ISPs do not have unique visibility into users' online activity.

Appendix 1 to Chapter 1 shows the widespread use of encryption today by the top 50 Internet sites. Appendix 2 shows data about the recent and substantial shift to HTTPS for Internet backbone traffic.

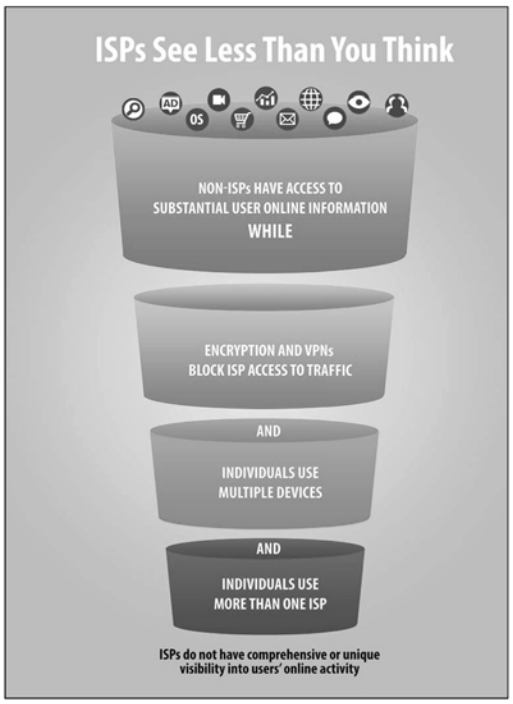


Diagram E-1

Chapter 2: Social Networks

Chapter 2 is the first of several Chapters that discuss certain categories, or "contexts," that are important ways that various players in the Internet ecosystem gather information about users' Internet activity. Each of these Chapters explains the prominent content and metadata that become available about users' activity, especially for advertising purposes. Each Chapter then analyzes how the access of non-ISPs compares with the access of ISPs for this context of data gathering.

Chapter 2 examines the flow of data through social networks, including data to which social networks have privileged or unique access, and the value of that data for advertising services. For social networks, there are three main data streams:

a. **User-Generated Data.** By design, social networks generally include a large amount of data supplied by the users themselves. Users create profiles including personal data such as name, city of birth, relationship status, and place of employment. Depending on the platform, users may post pictures, videos, URLs, and comments on posts of their personal and professional contacts.

b. **Metadata.** Along with data supplied by the user, the social network gains granular information about the user's interaction with the network, such as location data and activities of the user's contacts, which can then be combined with user-supplied data about interests and preferences in various products and services.

c. **Logged-In Users.** Social networks generally require an authenticated login from users, allowing for better tracking of that user. In particular, when a user signs in to the same social network on multiple devices, the social network can link each of those devices to the user for cross-device tracking. Social networks also use "plug-ins" on third-party websites to collect data about a logged-in user's activity on those sites. All of that user's activity can be accurately tied to the social network account and, depending on the amount and accuracy of information shared, to a specific, identified person.

ISPs do not have that level of insight or visibility of user behavior.

Chapter 3: Search Engines

For the past decade, search has generated almost half of all online advertising revenue, based especially on collection of two types of data: 1) user search queries, and 2) search results, including which results users ultimately click through to visit. The specificity of users' search queries can provide key insights into their intent, including the users' likelihood of purchase. When the search is performed over an HTTPS connection, as has become the norm, the ISP can only see which search engine was used and the host domain of the clicked link, but not the search query or the full URL that was clicked.

Chapter 4: Webmail and Messaging

Providers of webmail and other messaging services have the ability to scan the content and metadata of their users' messages for purposes such as security and advertising.[21] Scanning for security can reduce the transmission of spam, malware, and illegal content such as child pornography. Scanning can also identify keywords present in messages that are sent or received, which are then used to target advertising to the user. When webmail is accessed over an HTTP connection, ISPs could have the technical ability to perform deep packet inspection to access user content. Most webmail providers have recently moved to HTTPS by default, however, so ISPs are technologically blocked from this information.

[21] For what is called end-to-end encryption, even the service provider cannot scan the content of the message.

Chapter 5: How Mobile Is Transforming Operating Systems

When it comes to the technical capability of tracking user activity, no software or service is as comprehensive as the operating system ("OS"). Especially with the dramatic rise in mobile computing, the OS today is becoming far more tightly linked with advertising-relevant data, in at least three major ways. First, the leading operate app stores that generate usage data and attract app developers by being advertising-friendly. Second, the OS facilitates collection of location data, available often both to the OS and app developers. ISPs have some capability to access "coarse" location information through triangulation of cell towers, but more precise location information is generally gathered by non-ISPs based on a Global Positioning System ("GPS"), WiFi hotspot, and other sources of location data. Third, personal assistants such as Apple's Siri, Google's Google Now, and Microsoft's Cortana mean that OS systems gather detailed data from across the device in order to answer user queries. Previous separation between the OS and advertising is shifting greatly in the mobile setting.

Chapter 6: Interest-Based Advertising and Tracking

Many players in the online advertising ecosystem gather data about the online activity of users and devices. Going beyond the earlier scope of online behavioral advertising ("OBA"), this Chapter provides new Diagrams and explanation for the system of interest-based advertising ("IBA"), a broader term that includes the increasingly common practice of adding offline information to cookie-based, mobile advertising ID-based, and other online information. Notably, new Diagrams show the roles of publishers, supply-side platforms, advertising exchanges, demand-side platforms, and marketers, for both the mobile and non-mobile advertising ecosystem. ISPs historically have not been leading players in the IBA system, and the leading roles have been played by non-ISPs, who often are leaders as well at cross-context and cross-device tracking.

Chapter 7: Browsers, Internet Video, and E-commerce

This Chapter more briefly examines three additional contexts that are relevant to non-ISP collection of data. Major browsers vary in how extensively they collect user information, but the amount collected can be significant. For instance, most browsers carefully analyze user behavior to suggest search terms while the user is typing and then later use that information to autofill online forms by default. When users are logged-in, their browsing information can be integrated with information from the other contexts engaged in by that browser company. By contrast, ISPs are not developers of any of the major browsers and do not have access to this information.

For Internet video accessed through a browser or a mobile app, the party hosting the video content has the same ability to gain information about the user as any other site hosting content. Third-party ads are served in connection with video content the same as for other content. When Internet video is delivered over a HTTPS connection, the ISP can only see the host domain.

E-commerce sites (first-party retailers) often create long-standing relationships with their consumers. Due to purchases on the site, e-commerce sites usually have relatively accurate and detailed information about a user's name, credit cards, billing and shipping addresses, and phone numbers. E-commerce sites can also develop profiles of what their users purchase, which are more valuable the more often the user comes back to the same site. ISPs, by contrast, are not market leaders in their own e-commerce efforts, and they do not have first-party access to the variety or volume of information other e-commerce sites have.

Chapter 8: Cross-Context Tracking

This Chapter defines cross-context tracking, and discusses two ways that companies can build a context map for users. Cross-context tracking is the combination of different types of data, such as those discussed in the preceding Chapters – ISPs, social networks, search, webmail and other messaging, operating systems, mobile apps, interest-based advertising, browsers, Internet video, and e-commerce. The same company within the advertising ecosystem often plays a role in multiple contexts, such as an operating system company that also provides a search engine, or a social network company that also has an advertising network. These companies often perform cross-context tracking in two ways:

a. **Logged-in (deterministic) cross-context tracking.** When a user logs-in to the same service in multiple contexts, that company can accurately map activity in each context to the logged-in account. For example, if a user searches for a location in a search engine, and then links to a driving navigation service provided by the same company, the company can attribute all of that activity to the individual account.

b. **Not logged-in (probabilistic) cross-context tracking.** Not logged-in context maps are built around an individual user or device, but without the definitive log-in event as a catalyst. Instead, companies can compare data collected in each of their service contexts and use a proprietary algorithm to estimate when different activities are performed by the same user or device. These not logged-in maps can be used independently or to augment an existing logged-in cross-context map with additional data from outside that company's contexts, or as a commodity to be sold to other advertising entities.

The rise of cross-context tracking, often by companies with leading market roles in multiple contexts, heightens the value to advertisers of the insights into users' Internet activities that come from each context. We provide a cross-context chart for major ISPs and other companies, listed by over five percent of the market, market presence, or not in the market. The chart illustrates that the "unique" insights into user online activity most thoroughly is available to companies that have not historically been ISPs.

Chapter 9: Cross-Device Tracking

This Chapter explores the ways in which different entities can create cross-device maps for users. As with cross-context tracking, companies can create cross-device maps based on logged-in (deterministic) tracking or not logged-in (probabilistic) tracking.

Building on the earlier Chapters' discussions of the various technologies, this Chapter provides a summary of how different parts of the ecosystem work together. An accurate device map, especially when combined with an accurate cross-context map, provides distinct advantages for advertisers:

a. **Frequency Capping.** By being able to track each context and device a user engages with, advertisers can make sure that no individual user sees a single advertisement more often than desired.

b. **Attribution.** Cross-device tracking can allow advertisers to accurately attribute sales conversion to previous-in-time advertising impressions, including reduction in fraud. For example, if a user sees an ad on her smartphone and then performs a search on her desktop for that product, an accurate cross-device map demonstrates that the smartphone ad was effective in driving the purchase.

c. **Improved Advertising Targeting.** By collecting data across multiple devices, advertisers have a fuller picture of the user to whom they are targeting advertisements, allowing for a higher likely return-on-investment for each advertisement.

d. **Sequenced Advertising.** Cross-device tracking can enable companies to conduct sequenced advertising campaigns. Regardless of the device used, the advertiser can make sure that each ad in sequence is served to the user in the intended order.

e. **Tracking Simultaneity.** Cross-device tracking can also allow for multi-screen tracking of users. If a user is watching content on their smart TV while also using a tablet, an accurate device map can allow a company to know what ads are being served to the smart TV and sync those ads with the ones served to the user's tablet.

In this emerging ecosystem, ISPs are merely one source of data, and their subscriber relationships provide a diminishing portion of any user's history of Internet activity, as users shift to an expected average of 11.6 devices by 2019.[22] A single cross-device tracking company works with numerous sources of information, few of them related to the ISP function, to gather and analyze data in creating the device map.

Chapter 10: Conclusion

In summary, based on detailed analysis of today's Internet ecosystem in the United States, this Working Paper concludes in Chapter 10 that the evidence does not support a claim that ISPs have "comprehensive" knowledge about their subscribers' Internet activity, for encryption and other technological reasons. Similarly, ISPs lack "unique" insight into users' activity, given the many contexts where other players in the ecosystem gain insight but ISPs do not, and the leading role in cross-context and cross-device tracking played by non-ISPs.

This Working Paper takes no position on what rules should apply to ISPs, or to providers of services in the other contexts (often called "edge providers"). However, public policy should be consistent and based on an accurate understanding of the facts. The following Chapters provide details and citations to further explain today's online ecosystem.

[22] "VNI Forecast Highlights," *Cisco*, (http://www.cisco.com/web/solutions/sp/vni/vni_forecast_highlights/index.html).

The CHAIRMAN. Thank you, Professor Swire.

Before I begin with questions, I want to submit a few items for the record of today's hearing. I received two letters that I believe contribute greatly to this topic. The first letter is signed by constitutional scholar Laurence Tribe and 13 other law professors, economists, and experts. They support strong protections for consumers in the online space, but they have significant concerns with the FCC's proposal, and, instead, they suggest that the Commission adopt rules modeled after the FTC's longstanding and highly successful approach, their words.

The second letter, signed by the heads of eight trade associations representing both the technology sector and the telecom industry, also argues for the FCC to harmonize its effort with the existing FTC framework, in order to minimize consumer confusion and provide flexibility for the marketplace to innovate.

[The letters referred to follow:]

INTERNATIONAL CENTER FOR LAW & ECONOMICS
July 11, 2016

VIA EMAIL

Hon. JOHN THUNE,
Chairman,
Committee on Commerce, Science, and Transportation.

Hon. BILL NELSON,
Ranking Member,
Committee on Commerce, Science, and Transportation.

Hon. FRED UPTON,
Chairman,
Committee on Energy and Commerce.

Hon. FRANK PALLONE,
Ranking Member,
Committee on Energy and Commerce.

Hon. GREG WALDEN,
Chairman,
Subcommittee on Communications and Technology,
Committee on Energy and Commerce.

Hon. ANNA ESHOO,
Ranking Member,
Subcommittee on Communications and Technology,
Committee on Energy and Commerce.

Re: Letter from legal scholars and economists concerning the Federal Communications Commission's Broadband Privacy NPRM

Dear Senators Thune and Nelson, Congressmen Upton, Pallone and Walden, and Congresswoman Eshoo:

We, the undersigned experts in the law and economics of the Internet, have significant concerns with the proposal of the Federal Communications Commission ("Commission" or "FCC") to adopt new data privacy and security rules for broadband Internet access service providers ("ISPs") under Title II of the Communications Act.

We support strong consumer protection and believe that the Commission has a role to play in protecting consumers' data privacy and security. For several reasons, however, we find that the proposed rules take the wrong approach and would harm consumers, competition, and innovation.

As a fundamental matter, the proposed rules do not reflect the technological and economic nature of the Internet environment, in which ISPs are just one of many types of entities that have access to and can use consumers' online information to provide services, including access to ad-supported content. The proposed rules would single out ISPs for heightened regulation, imposing strict opt-in consent requirements on their use and disclosure of customer information.

By contrast, other online entities—such as social media networks, operating systems, browsers, data brokers, and search engines—would operate under the Federal Trade Commission's ("FTC's") strong but flexible opt-out consent regime, which would allow them to continue collecting, using, and sharing information about consumers' online activities for a variety of commercial purposes. The FTC's framework focuses on stopping practices that truly harm consumers, allowing companies ample space to develop innovative and beneficial products and services.

As a result, the FCC's proposed rules would not only distort the marketplace in ways that are likely to increase costs to consumers, but also mark an unprecedented

and unwarranted departure from the successful balance that has governed the Internet economy for the past couple of decades and which has led to substantial innovation, investment, competition, and growth.

Moreover, the asymmetrical regulatory framework that would be created by the proposed rules likely would confuse consumers and negatively affect the Internet economy. Specifically, the Commission's proposal to require ISPs to obtain opt-in consent before using or disclosing consumers' data for most activities is diametrically opposed to the approach that the FTC has taken for decades and to which consumers have become accustomed. Consumers may not understand that the choices they make through their ISPs' opt-in mechanism do not apply to other participants in the Internet ecosystem, even though these other participants will be collecting exactly the same data and using it for exactly the same purposes (*e.g.,* online advertising) as ISPs.

In addition, the free flow of data is the lifeblood of the Internet economy. *The proposed heightened consent requirements, however, would impede consumers' access to information about new online services and cost-savings that may be of interest to them and therefore would reduce ISPs' incentives to develop new services, reducing competition and innovation online.*

The Commission's failure to take these costs into account exemplifies its broader failure to conduct a full economic analysis of the proposed rules.

Finally, the Commission's proposed choice rules are unconstitutional because they would uniquely prohibit ISPs' use and disclosure of information for marketing purposes without obtaining consumers' opt-in consent. *By treating ISPs differently from other online entities, the proposed rules would create a discriminatory, speaker-based regime. Such a regime is presumptively invalid and subject to strict scrutiny, which the proposed rules could not withstand.* Nor could the proposed rules survive intermediate scrutiny: by requiring opt-in consent for most first-party marketing and other activities, regardless of the potential for consumer harm, they are not narrowly tailored to advance a substantial governmental interest.[1]

Fortunately, there is another path forward. *The Commission should adopt rules modeled after the FTC's longstanding and highly successful approach, which the FTC staff highlighted in its comments filed in this proceeding.* This technology-neutral approach—which applies an opt-in consent requirement to the use and sharing of sensitive information such as financial, health, children's, and precise geolocation data as well as social security numbers, plus robust notice and opt-out choice for other data uses—would provide strong, time-tested, and consistent privacy protections for consumers across the Internet ecosystem while fostering continued innovation, competition, investment, and growth.

Respectfully submitted,

(Affiliations provided for identification purposes only)

LAURENCE H. TRIBE
Carl M. Loeb University Professor & Professor of Constitutional Law
Harvard Law School

RICHARD A. EPSTEIN
Laurence A. Tisch Professor of Law, The New York University School of Law
The Peter and Kirsten Bedford Senior Fellow, The Hoover Institution
The James Parker Hall Distinguished Service Professor of Law Emeritus and Senior Lecturer, The University of Chicago

ROBERT CORN-REVERE
Partner
Davis Wright Tremaine LLP

ROBERT D. ATKINSON
President
Information Technology and Innovation Foundation

JANE BAMBAUER
Associate Professor of Law
University of Arizona
James E. Rogers College of Law

---

[1] See also Professor Laurence H. Tribe and Jonathan Massey, "The Federal Communications Commission's Proposed Broadband Privacy Rules Would Violate the First Amendment," WC Docket No. 16–106 (May 27, 2016) (white paper detailing how the FCC's proposed rules would violate the First Amendment in various respects and should not be adopted).

BABETTE BOLIEK
Associate Professor of Law
Pepperdine University School of Law

FRED H. CATE
Distinguished Professor and C. Ben Dutton Professor of Law
Indiana University Maurer School of Law

JAMES C. COOPER
Associate Professor of Law and Director, Program on Economics & Privacy
Scalia Law School, George Mason University

JUSTIN (GUS) HURWITZ
Assistant Professor of Law
Nebraska College of Law

MARK A. JAMISON
Director and Gunter Professor, Public Utility Research Center
University of Florida

DANIEL A. LYONS
Associate Professor of Law
Boston College Law School

GEOFFREY A. MANNE
Executive Director
International Center for Law & Economics

DAVID W. OPDERBECK
Professor of Law, Seton Hall University Law School
Director, Gibbons Institute of Law, Science & Technology

PAUL H. RUBIN
Samuel Candler Dobbs Professor of Economics
Emory University

July 11, 2016

Hon. JOHN THUNE,
Chairman,
Senate Committee on Commerce,
Science, and Transportation,
Washington, DC.

Hon. BILL NELSON,
Ranking Member,
Senate Committee on Commerce,
Science, and Transportation,
Washington, DC.

Dear Chairman Thune and Ranking Member Nelson:

We write to applaud the Committee for your efforts to examine the Federal Communication Commission's ("FCC") proposed broadband privacy rules. Now that the reply comment period in the FCC's proceeding has closed, this hearing is a timely and important venue for considering the deep flaws that we, and many other commenters, have identified in the FCC's lead proposal. In the months since the FCC unveiled its proposed rules, a diverse set of stakeholders has criticized the proposals because they would impose unnecessary costs on consumers, put a drag on innovation and competition, and make it harder for broadband Internet access service providers ("ISPs") to work with the government and third-party partners to ensure the security, reliability, and integrity of the service. The record before the FCC adds depth and breadth to these criticisms and raises additional arguments, including important constitutional concerns. It is clear that the FCC's proposed rules are both inconsistent with consumer expectations and clash with the important policies that have successfully guided the Internet economy for almost two decades under both Democratic and Republican administrations.

Title II of the Communications Act in no way requires the FCC to adopt prescriptive privacy rules that would single out one subset of the broader online ecosystem for heightened and inconsistent regulation that ignores the sensitivity of the information at issue. As comments from current and former Federal Trade Commission ("FTC") Commissioners, civil rights organizations, economists, legal scholars, and companies ranging from advertisers to home efficiency companies have noted, the FTC's consumer privacy framework is much better suited for the dynamic, innovative, and highly competitive Internet economy—in which ISPs play an important but limited role. At the center of the FTC's framework and the Obama Administration's reports and legislative proposals is the idea that companies should be transparent

with consumers, provide them with choices that are appropriate for the sensitivity of data or use in question, and maintain reasonable data security safeguards.

Consistent with that approach, before the FCC initiated the broadband privacy proceeding, a broad industry coalition of ISPs, tech companies, equipment providers, and others joined together to urge the FCC to adopt a framework based on the broad principles of transparency, respect for context, and choice. The coalition's proposal, which is attached to this letter, emphasized that "[c]onsumers should have consistent and predictable privacy protections for the information they deem private and sensitive, no matter how or with whom they share it." In other words, we support privacy protections that address the potential for genuine consumer harm, allow consumers to exercise appropriate control over how information about them is used and shared, and provide the flexibility that is necessary to promote innovation and competition. The FCC's proposed rules, however, are inconsistent with the flexible framework that the FTC enforces against many other players in the Internet economy; and the proposed rules offer no material improvement to consumer privacy protections.

The staff of the FTC's Bureau of Consumer Protection recently made the same point in their comments to the FCC, noting that creating special rules for ISPs "is not optimal" and that the rigid proposed rules "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." We agree: privacy rules that hamper innovation and competition while also failing to meet consumers' expectations are "not optimal," to say the least.

The FCC's proposed rules are also seriously out of step with the technology-neutral approach—applied to both ISPs and non-ISPs—that that has guided the Administration's many efforts on privacy and cybersecurity policy, with great success. For example, the Administration's Consumer Privacy Bill of Rights emphasized the importance of common principles that apply across the ecosystem, in particular the need to harmonize the standards that apply to communications companies with the standards that apply to the rest of the Internet economy. The Consumer Privacy Bill of Rights framework provides a "clear statement of basic privacy principles that apply to the commercial world, and a sustained commitment of all stakeholders to address consumer data privacy issues as they arise from advances in technologies and business models." Similarly, the Administration's Cybersecurity Framework was "created through collaboration between government and the private sector, uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses." This is the right approach for the innovative, dynamic, competitive Internet economy.

The FCC's proposal to go in a radically different direction also raises serious constitutional concerns. Professor Laurence Tribe, a pre-eminent scholar of the U.S. Constitution, concluded that the "profound mis-matches" between the goals of the FCC proposal and its actual effects if adopted would violate the First Amendment in several ways. According to Professor Tribe, because the proposal "singles out broadband ISPs for extremely burdensome regulation" while leaving a wide range of other participants in the Internet economy under different rules, it is the kind of speaker-based restriction that would face strict scrutiny under the First Amendment. Professor Tribe also concluded that the proposal would be unconstitutional even under the more lenient standard that applies to commercial speech. The time-proven effectiveness of the legal standards that the FTC enforces demonstrates that a much less restrictive alternative is available to the FCC.

Put simply, the "profound mis-match" between the FCC's highly restrictive proposal and the surrounding legal, economic, and technological landscape is bad policy and constitutionally problematic.

We appreciate the Committee's important recognition of this issue and the need for Congressional oversight. We are hopeful that your examination of these issues will lead to an FCC approach that closely harmonizes FCC privacy rules with the existing FTC framework and is consistent with the Administration's guiding principles for privacy and security in the Internet economy. Doing so would protect consumer privacy, minimize consumer confusion resulting from inconsistent regulations, permit new entry into the online advertising market, and provide the flexi-

bility the online marketplace needs in order to continue to innovate and evolve as it has done for many years under such a regime.

Sincerely,

GARY SHAPIRO
President and CEO
Consumer Technology Association

JIM HALPERT
President & CEO
Internet Commerce Coalition

JONATHAN SPALTER
Chair
Mobile Future

SCOTT BELCHER
CEO
Telecommunications Industry Association

MEREDITH ATTWELL BAKER
President and CEO
CTIA®

GENEVIEVE MORELLI
President
ITTA

MICHAEL POWELL
President & CEO
National Cable & Telecommunications Association

WALTER B. MCCORMICK, JR.
President & CEO
USTelecom

The CHAIRMAN. There is also a new paper published by Gerard Faulhaber, former Chief Economist at the FCC, and Hal Singer, a Senior Fellow at the George Washington School of Public Policy. Their paper is titled, "The Curious Absence of Economic Analysis at the Federal Communications Commission: An Agency in Search of a Mission." And while it focuses primarily on the Commission's failure to ground its recent regulations in economic reasoning, Faulhaber and Singer offer some valuable insight in this case about the FCC's privacy proposal, and particularly noting the complete lack of any cost-benefit analysis by the Commission in this proceeding.

So I want to as well submit that for the record.

[The information referred to follows:]

The Curious Absence of Economic Analysis at the Federal Communications Commission: An Agency in Search of a Mission

by

Gerard R. Faulhaber[1] and Hal J. Singer[2]

Abstract

By counseling a very judicious use of regulation, including forbearance where appropriate, regulations informed by economic analysis at the Federal Communications Commission (FCC) have positively affected the U.S. economy. From freeing up long-distance telephone from regulation and subjecting it to competition, to enabling the proliferation of enhanced data Internet services, and spurring the growth of new wireless markets, the world has been changed for the better by wise application of regulations informed by economic principles. The failure of the FCC to ground its regulations in economic reasoning in the last few years, however, has led to inefficient policies and proposals that threaten to eviscerate prior benefits. The FCC has made no effort to subject its pending privacy or set-top-box proposals to cost-benefits analysis. The resolution of the FCC's 2015 Open Internet Order illuminates the quagmire for policymakers. Given the D.C. Circuit's willingness to defer to the FCC's expertise in policy, and given the FCC's willingness to eschew econometric evidence and economic theory as it considers new regulations, the most direct way to re-inject economics into FCC policymaking is via a Congressional mandate for the agency to perform cost-benefit analysis, subject to OIRA or judicial review. There is no reason why the Department of Labor, the Environmental Protection Agency, the Consumer Financial Protection Bureau, and a host of other agencies should be required to perform cost-benefit analysis, while the FCC is free to embrace populism as its guiding principle. The tech industries under the FCC's domain are equally if not more important to the U.S. economy and deserve regulations based on rigorous economic analysis.

---

1. Professor Emeritus, Wharton School, University of Pennsylvania and Penn Law School.
2. Senior Fellow, George Washington School of Public Policy; Adjunct Professor, Georgetown's McDonough School of Business; Principal, Economists Incorporated. The authors would like to thank CALinnovates for funding, and Augustus Urschel for research assistance. The views here are those of the authors only, and do not reflect the views of their affiliated institutions.

I. Introduction

Upon leaving the Federal Communications Commission (FCC) in January 2016, outgoing chief economist Tim Brennan remarked that his former agency was operating, with respect to the

issue of net neutrality, in an "economics-free" zone.[3] Professor Brennan offers an insider's view of how economics has been marginalized in the FCC's decision-making process. Even casual observers of recent FCC rulemaking can sense that economics has taken a backseat to politics. In announcing its decision to reclassify Internet service providers as "common carriers" in February 2015, a majority of FCC commissioners routinely cited the four million comments the agency received in favor of net neutrality.[4] The voices—no matter how disconnected from the ultimate policy outcome—trumped whatever the economists had to say.

To an economist with an allegiance to cost-benefit analysis, even 40 million comments could not justify regulatory action that harms the Internet ecosystem on net: What matters is (1) whether there exists a market failure that warrants sector-specific intervention; and if so (2) whether the expected benefits of the intervention (approximated by increase in investment in the "edges" of the network) exceed the expected costs (approximated by the decrease in investment at the "core"); and (3) even if the net benefits are positive, whether there exists a less-restrictive alternative that would achieve even greater net benefits. But the FCC did not perform a rigorous cost-benefit analysis in the proceeding; instead, it released a two-page statement in March 2015 purporting to show annual *gross* benefits of $100 million in edge investment. The perfunctory statement noted that "the Commission is not required to prepare a cost benefit analysis,"[5] which would entail estimating the *net* benefits of the rule. Economists warned that failure to incorporate economic analysis into the agency's decision-making could lead to increased uncertainty due to litigation risk, which in turn could discourage innovation.[6]

In the 2015 *Open Internet Order* ("*2015 OIO*") itself, rather than rely on econometric analysis proffered in the proceeding,[7] the FCC credited the casual empiricism of a consumer advocacy group, which purported to show that common-carrier regulation of DSL providers in the late 1990s and early aughts was the cause of higher telecom investment relative to later periods,

---

3. *See, e.g.*, Gordon Crovitz, *Economics-Free Obamanet*, WALL STREET JOURNAL, Jan. 31, 2016, *available at* http://www.wsj.com/articles/economics-free-obamanet-1454282427#:OXpja3_mPAWUoA.

4. *See, e.g.*, Statement of Commissioner Jessica Rosenwercel, Re: Protecting and Promoting the Open Internet, GN Dkt. No. 14-28 ("This is a big deal. What is also a big deal is 4 million voices. Four million Americans wrote this agency to make known their ideas, thoughts, and deeply-held opinions about Internet openness."), *available at* https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A4.pdf. Statement of Mignon Clyburn, Re: Protecting and Promoting the Open Internet, GN Dkt. No. 14-28 ("I also believe that they never envisioned a government that would include the input and leadership of women, people of color, and immigrants, or that there would be such an open process that would enable more than four million citizens to have a direct conversation with their government."), available at https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A3.pdf. Statement of Tom Wheeler, Re: Protecting and Promoting the Open Internet, GN Dkt. No. 14-28 ("Most significantly of all, we heard from nearly four million Americans, who overwhelmingly spoke in favor of preserving a free and open Internet.").

5. Congressional Review Act Abstract, WG Dkt. No. 14-28, FCC 15-24 (Mar. 12, 2015), *available at* http://www.progressivepolicy.org/wp-content/uploads/2015/04/20150403-CRA-Abstract-Open-Internet-Order.pdf.

6. Gerald Faulhaber, *What Hath the FCC Wrought?*, REGULATION (Summer 2015), *available at* http://object.cato.org/sites/cato.org/files/serials/files/regulation/2015/6/regulation-v38n2-1.pdf.

7. Kevin A. Hassett & Robert J. Shapiro, The Impact of Title II Regulation of Internet Providers On Their Capital Investments, SONECON (Nov. 2014), *available at* http://www.sonecon.com/docs/studies/Impact_of_Title_II_Reg_on_Investment- Hassett-Shapiro-Nov-14-2014.pdf.

when DSL was classified as an information service.[8] Never mind that the capital expenditure (capex) of cable modem providers, which were not subject to common-carrier rules and thus serve as a near-perfect control group for DSL providers, grew at a faster rate than telco capex during the period of asymmetric regulation,[9] casting doubt on the FCC's causal inference. Rigorous economic analysis would immediately uncover the fallacy in this naïve reasoning. Yet the *2015 OIO* contained no such economic evidence, only simple-minded (and false) conclusions. Although the *OIO* was upheld on a 2-1 vote by the D.C. Circuit in June 2016,[10] Judge Williams' dissent (discussed in detail below) vindicated the concerns of many economists, including three former chief economists of the FCC.

2015 marks the nadir of economic influence at the agency. In the prior five years (2010 to 2014), the Commission's Office of Strategic Planning and Policy Analysis hosted an average of 16 economic seminars at the agency per year.[11] In 2015, the FCC conducted just four. Assuming that economic analysis is currently held in low esteem at the FCC, how did we get there? And what are the implications of removing economic analysis from agency rulemakings that impact several critical sectors of the U.S. economy? This paper seeks to answer those questions, by studying the role of economics at the FCC over time, and by seeking to identify what caused the FCC to abandon the dismal science. We hypothesize that the waning influence of economic analysis is correlated to the politicization of the agency and its search for a new mandate. If true, this insight offers crisp policy prescriptions to reinsert dispassionate economic analysis into decision-making at the FCC.

Other researchers have taken notice of the diminution in the *quality* of economic analysis at the FCC, which is a proxy for the *influence* of economics at the agency. For example, Delp and Mayo (2016) find that while the concept of "effective competition" is central to policy formation at the FCC, the Commission's own applications of "effective competition" are inconsistently applied.[12] In the case of video distribution, they explain that "the FCC has alternatively defined 'effective competition' to be a number of competitors greater than or equal to three, six, or two."[13] Hahn, Faulhaber and Singer (2012) similarly take issue with the FCC's shifting standard for assessing competition in mobile telephony.[14] Based on a review of FCC's merger conditions involving spectrum transfers, Manne et al. (2013) find that "the agency's standard of review for spectrum transfers, its use of conditions, as well as the scope of its transaction reviews exceed

---

8. In the Matter of Protecting and Promoting Open Internet, GN Dkt. No 14-28, Report and Order on Remand, Declaratory Ruling, and Order, ¶414 n. 1210 (citing Free Press submission) (released Mar. 12, 2015) (hereinafter *2015 OIO*).

9. Brief for Georgetown Center for Business and Public Policy and Thirteen Prominent Economists, USTA v. FCC, Aug. 6, 2015, at 14, *available at* https://www.ustelecom.org/sites/default/files/documents/15-1063%20Georgetown%20Center%20and%20Economists%20Amicus%20Brief%20080615.pdf.

10. U.S. Telecom Ass'n. et al. v. FCC, No. 15-1063 (D.C. Cir. 2016).

11. Economic Seminars, Office of Strategic Planning & Policy Analysis, *available at* https://www.fcc.gov/general/economic-seminars-office-strategic-planning-policy-analysis.

12. Amanda Delp & John Mayo, The Evolution of Competition: Lessons for 21st Century Telecommunications Policy, Georgetown Working Paper (Apr. 2016).

13. *Id.* at 12.

14. Gerald Faulhaber, Robert Hahn, & Hal Singer, *Assessing Competition in U.S. Wireless Markets: Review of the FCC's Competition Reports*, 64(2) FEDERAL COMM. L. J., 319-370 (2012).

legal limits, impede efficient markets for spectrum, and deter welfare-increasing transactions and investment."[15] They explain how the FCC's reliance on concentration of spectrum as a surrogate for anticompetitive effects conflicts with the approach of the FTC/DOJ *Horizontal Merger Guidelines*.[16]

This is particularly unfortunate because the economics staff at the FCC is of high quality and no doubt the best in Washington in their understanding of the economics of telecommunications and the Internet. The low quality of economic analysis currently going on at the FCC could indicate that the agency is not allocating the appropriate resources for the discipline, or more likely, that the Commission is simply ignoring the analysis they are receiving from their own economists.

This paper, which to our knowledge is the first to characterize the influence of economic analysis at the FCC over time,[17] is organized as follows: In Part II, we chart the rise and fall of economic analysis at the FCC. Our brief history begins with the early years, in which broadband licenses were allocated pursuant to beauty contests—a period of minimal economic influence. Often at the behest of the D.C. Circuit, economics starts to take hold in the 1960s and 1970s, as seen through important FCC rulemakings, including *Carterfone*, *MCI*, and the *Computer Inquiries*. Economic analysis arguably reached its apex at the Commission in the 1990s, with an embrace of auctions to allocate spectrum to mobile carriers, as well as an embrace of antitrust principles to guide regulatory intervention in areas such as wireless telephony and the nascent Internet. The aughts saw a continuation of a light-touch approach guided by economics, with a key decision to unwind the "common carrier" classification scheme for DSL providers in 2005, and to forbear from rate regulation of next-generation broadband access technologies such as fiber to the home.

This streak of economic import was suddenly broken under the leadership of Tom Wheeler, which has been marked by several decisions devoid of economic analysis. The 2015 *Open Internet Order* rejected the original rationale for embracing case-by-case review of "paid prioritization" arrangements—that is, payments by edge providers to Internet service providers (ISPs) for enhanced quality of service—and instead imposed a *per se* ban on the conduct. In 2010, the Commission recognized that case-by-case review was the appropriate rubric for dealing with paid prioritization (or any vertical restraint for that matter) that could be motivated for procompetitive reasons.[18] Indeed, the 2010 *Open Internet Order* relied on economic models of two-sided platforms, which showed that zero-pricing rules (that banned paid prioritization) had ambiguous investment and welfare effects.[19] Accordingly, it was decided that blanket bans would impose certain error costs (denying arrangements that are output-expanding and welfare-increasing), and would make sense only if those error costs were zero. Some economists (and ultimately the D.C.

---

15. Geoffrey Manne, Will Rinehart, Ben Sperry, Matt Starr & Berin Szoka, The Law and Economics of the FCC's Transaction Review Process, at 2, *available at*: http://ssrn.com/abstract=2242681.

16. *Id*. at 3.

17. Extant FCC economists have written on the influence of economics during their tenure. *See e.g.*, Jonathan B. Baker, Mark Bykowsky, Patrick DeGraba, Paul LaFontaine, Eric Ralph, and William Sharkey, The Year in Economics at the FCC, 2010-11: Protecting Competition Online Federal Communications Commission.

18. In the Matter of Preserving the Open Internet, Report and Order (released Dec. 23, 2010), ¶ 76 n. 299.

19. 2010 *Open Internet Order*, ¶ 28 n. 80.

Circuit) objected to the presumption the FCC embraced in its 2010 *Open Internet Order*—namely, that any paid prioritization was presumptively in violation of the Commission's non-discrimination principle—which inefficiently placed the burden of proof on the ISP rather than the excluded content provider. Despite this perceived infirmity, the 2010 *Open Internet Order* was a reasonable *political* compromise that at least respected certain economic considerations. The 2015 *Open Internet Order* however, did no such thing. Part II concludes with a brief review of other decisions in the Wheeler era that were also devoid of economic content.

In Part III, we explain why populism may be preferred to economic analysis in the modern era. In short, we find that the mandate of the 1996 Telecom Act leaves the FCC with a very narrow role. Although the Act expands the FCC's ambit with respect to access lines for voice services, it severely limits the FCC's jurisdiction when it comes to broadband service. The few times the FCC has tried to impose regulation on broadband, the D.C. Circuit has limited the agency's influence even further. As a result, the core business subject to FCC oversight has evaporated, minimizing the agency's relevancy in the Internet Age. Understood in this light, the FCC's embrace of Title II regulation based on populist sloganeering gives the agency a new lease on life as a regulator of a portion of the Internet.

Part IV describes the new battleground for economics-free regulation. Untethered from its customary respect for cost-benefit principles, the FCC moved quickly from reclassification to unbundling video content, regulating the price for business broadband, and imposing marketing restrictions on ISPs (but not on edge providers) in the name of privacy. To launch its campaign for set-top box reform, the FCC issued a "Fact Sheet" that again relied on the economic findings of a consumer advocacy group to suggest (erroneously) that set-top box prices had increased by 185 percent over the past decade.[20] Repeating a coordinated marketing campaign from the Open Internet proceeding, the White House released a video and a policy memo in favor of the FCC's set-top box proposal.[21] Armed with new powers from reclassification, the FCC next intervened to usurp the Federal Trade Commission's privacy enforcement over ISPs. Since the FCC is proposing a set of restrictions unique to ISPs, but is eschewing applying those same restrictions to other market participants that have access to the same and more consumer information, the FCC's foray into privacy has been viewed as protectionism for a politically preferred class of providers.

In Part V, we explore the implications of the FCC's economics-free regulatory agenda on the tech sector. Picking up on the privacy example, asymmetric regulation on only one set of market participants could permit incumbent platform providers (such as Google or Facebook) to raise advertising prices (above the rates that would have prevailed with ISP entry), resulting in less online advertising and inferior information for online shoppers. Subjecting Ethernet prices to price-

---

20. FCC Chairman Proposal to Unlock the Set-Top Box: Creating Choice and Innovation, Jan. 27, 2016, *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0127/DOC-337449A1.pdf. The statistic can be traced to a January 20, 2016 letter by Consumer Federal of America and Public Knowledge to the FCC, *available at* https://www.publicknowledge.org/documents/pk-and-mark-cooper-set-top-box-letter-to-fcc.

21. Jason Furman & Jeffrey Zients, Thinking Outside the Cable Box: How More Competition Gets You a Better Deal, Apr. 15, 2016, *available at* https://www.whitehouse.gov/blog/2016/04/15/ending-rotary-rental-phones-thinking-outside-cable-box. We are not aware of other occasions in which the White House has openly campaigned for an FCC proposal.

cap regulation for the first time could result in fewer buildings being wired for fiber, along with forgone spillover benefits of faster broadband. As with the *Open Internet Order* and the FCC's privacy proposal, which impose no restrictions on edge providers, the FCC's set-top box proposal similarly would constrain one set of market participants (MVPDs) and not others (device makers), thereby skewing the competitive landscape. These are straightforward considerations that an economist would have recognized and taken into consideration when evaluating the FCC's regulatory proposals—had she enjoyed a seat at the FCC's table.

The paper ends by asking how economic analysis could be reinserted into the policy debate. Assuming that the waning influence of economic analysis flows from the politicization of the agency and its search for a new mandate, the solution likely involves Congress. Based on this diagnosis, we advocate that Congress (1) shield the technocrats from political pressure of the kind we observed in net neutrality and set-top boxes proceedings, and (2) clarify the FCC's role over broadband Internet in an update to the Act. With respect to the second policy, Congress could solve the jurisdictional issue regarding net neutrality by giving the FCC the statutory power to regulate blocking and paid prioritization (as well as other forms of preference such as zero-rating) along the lines the agency sought in the 2010 *Open Internet Order*, but without recourse to heavy-handed Title II authority. Perhaps the most important mandate that Congress could give the FCC is to direct the Commission to explicitly include identification of market failure and careful cost-benefit analysis as a necessary condition before imposing *any* regulation.

The failure of the FCC in recent orders to use cost-benefit analysis and economic reasoning leads to inefficient policies that have real-world consequences. Proper use of economics has the intended impact of informing regulatory policy, but the unintended impacts of an economically minded agency are also important—it can lead to the FCC pulling back from regulation (especially Title II regulation) when such regulation is unnecessary. For example, the decision to stand down on regulating the Internet back in the 1990s has been widely recognized as a key reason for the explosive growth of the Internet and concomitant Internet innovation and investment. This growth would simply be impossible in the monopoly-regulated world of the Bell System. As then-Chairman Kennard explained, forbearing from regulation was a deliberate and highly successful policy decision. Without this decision, there would be no commercial Internet as we know it today.

Minimal and informed regulation has also given rise to the second great trend of the past several decades: wireless telecommunications. From the earliest incarnation of wireless in the 1980s to today, the cell phone and smartphone have been subject to minimal regulation and have led to explosive growth. There are more cell phones in the United States than there are people, far outstripping other consumer goods such as the telephone or television. These technologies are prime examples of regulatory successes, where judicious use of regulation, including forbearance where appropriate, has made a huge impact on our country and the world. From freeing up long-distance telephone from regulation to competition, enhanced data Internet services, and new wireless markets, the world has been changed by a wise application of economic principles.

II. The Rise and Fall of Economic Influence at the FCC

The FCC's use of economic theory, thought, and analysis can be broken into three general periods of history. From its inception in the early 1900s to the 1950s, economic consideration was largely absent from Commission policymaking and regulation. This era ends around the time Nobel Laureate Ronald Coase informed the Commission that its "zero-price" spectrum policy was inefficient. Starting in the 1960s we begin to see the Commission use economic theory, if not outright economic analysis, to shape its policies and regulatory reach. The 1990s and early 2000s mark the economic zenith of the FCC, when both theory and analysis play a major role in regulatory decision-making. By the 2010s, populism had reemerged as the primary driver of FCC policy, demonstrated by the agency's embrace of zero-priced (as opposed to paid) priority and interconnection.

A. The Early Years (1910s-1950s)

The FCC's early spectrum allocations were wholly devoid of economics. Licenses were given out for free to whomever could claim the "public interest." Spectrum reallocations created winners and losers based on lobbying and purely technical analysis. Calls to shape practices around economic theory were rejected. The Commission suffered from a degree of regulatory capture, working hand-in-hand with the incumbent interests of the day.

1. FRA and the First Spectrum Reallocation (1927)

From 1912 until 1926, regulation of the airwaves was overseen by the Commerce Department,[22] where broadcasting regulation was largely developed in concert with private enterprise.[23] When Commerce's legal jurisdiction for the growing technology became too thin, the FCC was born as the Federal Radio Commission (FRC) in 1927. Its mandate was to reallocate the chaotic spectrum mess created by a period of regulatory anarchy, following the dissolution of Commerce's mandate.

Critically, the 1912 Radio Act held no specific provision on the way to allocate station licenses. The FRC's mandate was to issue licenses if it "determine[d] that public interest, convenience, or necessity would be served by the granting thereof."[24] The discretion of what the public interest was, or who would be serving it, was left up to the regulators.

The solution to the allocation problem was decidedly noneconomic. The FRA first endeavored to grandfather all existing 733 stations across 90 frequencies.[25] For allocating new licenses, the FRC decided to interpret the "public interest" mandate as allocating licenses to the

---

22. FCC, *Annual Report of the Federal Radio Commission to the Congress of the United States*, at 1 (1927), *available at* https://transition.fcc.gov/Reports/ar1927.pdf

23. ROBERT W. MCCHESNEY, TELECOMMUNICATIONS, MASS MEDIA, AND DEMOCRACY 3 (Oxford University Press 1994).

24. *The Radio Act of 1927*, §11, 69th Congress (1927), *available at* http://www.americanradiohistory.com/Archive-FCC/Federal%20Radio%20Act%201927.pdf

25. MCCHESNEY, *supra*, 20.

broadcaster that could provide the "best possible broadcasting conditions"—meaning the broadcaster with the best equipment.[26] Given out at a zero-price, these licenses largely went to commercial broadcasters, owing to their better equipment.[27] The FRC eventually came to rule that a "general public service broadcaster" had preference over a "propaganda station," or any nonprofit station with a policy position.[28]

Accordingly, the FRC's *ad hoc* allocation was mostly to the benefit of existing commercial networks, which descended on Washington to participate in a series of hearings about the future of radio. Meetings were generally private and closed to the press and public, and there was a revolving door between the employment at the FRC and its main beneficiaries.[29] Of the 25 "clear" (national) channels created, 23 were owned by the National Broadcasting Company (NBC).[30] Although it had not done so intentionally, the FRC admitted in later years that its initial allocation technique effectively cleared the airwaves of noncommercial radio.[31] By 1934, nonprofit broadcasting accounted for only two percent of all air time.[32]

2. FCC and the Second Spectrum Reallocation (1945)

The Communications Act of 1934 rolled the FRC into a reformed FCC. The FCC was given the broader mandate of "regulating interstate and foreign commerce in communication by wire and radio so as to make available, so far as possible, to all the people of the United States… a rapid, efficient, Nationwide, and world-wide wire and radio communication service with adequate facilities at reasonable charges."[33]

The second major spectrum conflict arose in 1945 over the band of VHF spectrum occupied by FM radio stations. The Radio Corporation of America (RCA), one of the largest manufactures of black-and-white televisions, desired that band of spectrum for its TV sets. RCA's competitor and upstart manufacturer, CBS, wanted television allocations to rest on the UHF band, which could support its color broadcasting.[34]

Faced with these competing interests, the FCC split the differences in an ultimately harmful way. TV was allocated 12 channels within the black-and-white VHF band, and FM had its allocation moved up from the 42-50 MHz to 88-108 MHz band. However, the 12 TV channels soon became congested. The FCC put a freeze on issuing TV licenses in 1948, until it allocated additional 70 channels in the UHF band years later. This fragmentation between two different areas

---

26. *Id.* at 25.
27. *Id.* at 26.
28. *Id.* at 28.
29. McChesney, Telecommunications, Mass Media, and Democracy, 22.
30. *Id.* at 20.
31. Sherille Ismail, *Transformative Choices: A Review of 70 Years of FCC Decisions*, 3, FCC Staff Working Paper 1 (2010), *available at* https://www.fcc.gov/reports-research/working-papers/transformative-choices-review-70-years-fcc-decisions
32. *Id. at* 30-31.
33. *Communications Act of 1934,* §1 73rd Congress (1934), *available at* https://transition.fcc.gov/Reports/1934new.pdf.
34. Ismail, *supra*, at 5.

of spectrum led to headaches for TV broadcasters in the coming decades, as UHF channels struggled to compete against their incumbent VHF competition.[35]

The FCC made these decisions "based on the testimony and data before it," but the Commissions reasoning was again devoid of economics.[36] Instead of economic analysis, the matter was decided by hearings and commentary. The major vested interests came to Washington to plead their case. A total of 231 witnesses testified, generating some "4,559 pages of testimony" and "543 exhibits."[37] Part of the FCC's rationale for moving the spectrum was based on a faulty technical analysis of the FM band.[38]

Although the FCC commissioned statistical studies of the telephone and telegraph industries and their associated rates and tariffs, there is no evidence of any economic analysis of the TV versus FM Radio question. Accordingly, the reallocation of FM radio spectrum rendered obsolete nearly 500,000 FM radio sets. This shock to the industry effectively arrested FM radio growth for over a decade.[39]

3. The FCC Hears an Economic Critique of Zero-Price Spectrum Licenses (1959)

In this early period, licenses were awarded in what could pleasantly be described as "spectrum beauty pageants." The FCC simply distributed spectrum licenses for free if there were no competing requests. In the event that there were two applicants for the same spectrum, the FCC would set up "comparative hearings," where the competing applicants used "a quasi-judicial forum in which to argue why they should be awarded a license over competitors, and allowed other interested parties to argue for or against an applicant."[40] Instead of being informed by economics, this process was wholly based on rhetoric. For example, in the first grant of cellular service licenses, 30 licenses generated 200 requests with each request being over 1,000 pages of argument.[41] Congress reformed the system into a lottery in 1981, but this did not address the underlying issue of inefficiency.[42]

In his landmark 1959 paper "The Federal Communications Commission," Nobel Laureate Ronald Coase argued that giving out valuable spectrum for free was incredibly wasteful.[43] He was not the first to notice this: There had been at least eight different instances between 1927 and 1959

---

35. *Id.*
36. FCC, *Eleventh Annual Report of the Federal Communications Commission,* 20 (1945), *available at* https://apps.fcc.gov/edocs_public/attachmatch/DOC-308662A1.pdf.
37. *Id.*
38. Ismail, *supra*, at 6.
39. *Id.* at 8.
40. FCC, *The FCC Report to Congress on Spectrum Auctions,* 6 (1997), *available at* http://wireless.fcc.gov/auctions/data/papersAndStudies/fc970353.pdf
41. *Id.*
42. *Id.* at 7.
43. See Ronald H. Coase, *The Federal Communications Commission,* The Journal of Law & Economics, Vol 2, pp1-40 (1959).

where the FCC's zero-price policy had been questioned.[44] Coase's paper was prompted in part by a feeble rejoinder by former FCC chief economist Dallas Smythe against a previous proposal to sell spectrum to the highest bidder.[45] When Coase presented his analysis to the FCC, one commissioner asked, "Are you spoofing us? Is this all a big joke?"[46]

Why did the FCC resist economics in these early years? One theory is that the FCC's initial policies were "not merely inefficient but illogical, error-prone, [and] a mere accident of history."[47] Another is that this was not a naïve mistake in undervaluing spectrum, but a deliberate *quid pro quo* between regulators and incumbent radio broadcasters.[48] Regardless of the cause, the evidence of any economic thinking in the FCC prior to the 1960s is scant. Although the organization managed to bring order to the airwaves, it did so in a bureaucratic, cabal-like manner, where winners were chosen upon nebulous public-interest grounds and persuasive presentations in Washington conference rooms.

B. The Rise of Economic Analysis in the 1960s and 70s

The FCC's non-economic doctrines did not break down of their own accord. Lacking any internal pressure to economically liberalize its policies, the FCC would require external stimulus to reform. Outside of Congressional action, this came in the form of "court-assisted liberalizations," which had the effect of pushing the FCC towards using economic theory as a principal of regulation. The decisions helped shape the FCC's treatment of the growing computer services industry in a series of decisions called the "Computer Inquiries."

1. The Hush-A-Phone Decision (1956)

The first real evidence of economic thinking at the FCC was the reluctant acknowledgement of consumers benefiting from third-party phone attachments. Prior to 1968, the FCC had routinely suppressed peripheral devices that attached to AT&T-owned phones or to the telecommunications networks themselves. At the time, only AT&T equipment could be attached to AT&T's networks, leading to a *de facto* monopoly in telecom equipment.[49] The FCC took the suppression of third-party devices to "ridiculous extremes," banning add-on devices that had no

---

44. Thomas W. Hazlett, *Assigning Property Rights To Radio Spectrum Users: Why Did FCC License Auctions Take 67 Years?*, 534, The Journal of Law & Economics, Vol XLI (1998).

45. Dallas W. Smythe, *Facing Facts about the Broadcast Business*, 20 U. CHICAGO L. REV. 100 (1952) ("Surely it is not seriously intended that the noncommercial radio users (such as police), the nonbroadcast common carriers (such as radio-telegraph) and the nonbroadcast commercial users (such as the oil industry) should compete with dollar bids against the broadcast users for channel allocations."), *available at* http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2752&context=uclrev

46. Thomas W. Hazlett, *Economic Analysis at the Federal Communications Commission*, 13 Prepared for an RFF Conference (April 7, 2011), *available at* http://www.rff.org/files/sharepoint/WorkImages/Download/RFF-DP-11-23.pdf

47. Thomas Hazlett, *Assigning Property Rights To Radio Spectrum Users: Why Did FCC License Auctions Take 67 Years?* 41 J. LAW & ECON. 569 (1998).

48. *Id.* at 541.

49. PETER HUBER, MARK KELLOGG & JOHN THORNE, 2 FEDERAL TELECOMMUNICATIONS LAW 664 (Aspen Law & Business 1991).

demonstrable harm to the telephone network.[50] This was the case with an automatic rotary dialing device invented in 1940, and a prototype answering machine named the "Jordaphone."[51]

The largely unfounded rationale for these bans was that "the unrestricted use of foreign attachments… may result in impairment to the quality and efficiency of telephone service, damage to telephone plants and facilities, or injury to telephone company personnel."[52] As a result, all third-party devices would have to be analyzed one case at a time.[53] This blanket ban was anathema to innovation, as it curtailed the ability of private entities to innovate with the existing technology without explicit permission of the owning company.

The pivotal change occurred in November 1956, when the Court of Appeals for the District of Columbia Circuit (D.C. Circuit) reversed the FCC's decision on Hush-A-Phone. The product was a metal device attached to the receiver of a phone, which effectively functioned in a similar manner to cupping a hand to a receiver for the purposes of speaking privately. The FCC had argued that use of this attachment would, somehow, negatively influence "the whole 'telephone system,'" but the appeals court saw no evidence of this outlandish claim.[54] Critically, the ban on Hush-A-Phone was found to be an "unwarranted interference with the telephone subscriber's right reasonably to use his telephone in ways which are privately beneficial without being publicly detrimental."[55] Although it may not have been intentional, the D.C. Circuit had set a new standard of analysis for the FCC.

With the court's decision rendered, the FCC revised its policy and directed AT&T to allow customers to use any device that "does not injure [AT&T's] employees or facilities, the public in its use of [AT&T's] services, or impair the operation of the telephone system."[56] Although AT&T still had the monopoly on the phones themselves, third-party equipment could be attached. This crack in the dam was practically insignificant in the near term, but it affected the FCC's monopoly logic in the coming years.

2. The Carterfone Decision (1968)

This economic liberalization was made plain in 1968, when the FCC permitted non-telephone devices (though not third-party telephones themselves) to be connected to the network.[57] The cause for this change was the Carterfone, a two-way radio device that used the existing phone line to connect to other Carterfone owners. AT&T had banned the use of the Carterfone, calling it

---

50. *Id.* at 665.
51. *Id.*
52. *Id.* at 665-66.
53. *Id.*
54. *Hush-A-Phone Corporation and Harry C. Tuttle, Petitioners, v. United States of America and Federal Communications Commission, Respondents, American Telephone and Telegraph Company et al., and United States Independent Telephone Association, Intervenors,* 99 U.S. App. D.C. 190; 238 F.2d 266 (1956).
55. *Id.*
56. Huber, Kellogg, & Thorne, Federal Telecommunications Law, Issue 2; 667.
57. Ismail, *Transformative Choices: A Review of 70 Years of FCC Decisions,* 17.

a "prohibited interconnecting device."[58] The FCC found that "Carterfone fills a need and that it does not adversely affect the telephone system."[59]

This was an important shift from the Commission's earlier policy. The decision was in part based on *Hush-A-Phone*, but it also contained nods to economic reasoning. The FCC concluded that a private manufacturer of devices could connect to the telephone system, provided that they met reasonable network standards.[60] In the long run, this opening would eventually enable the development of modems and the Internet.[61] For the moment, though, it meant that the FCC was open to competition in ancillary markets that functioned alongside the monopoly network.

3. The FCC Gives MCI Authority To Offer Long Distance Services in Select Markets (1977)

Final evidence of court-assisted liberalization can be seen in the 1977 opinion in *MCI v. FCC*. Microwave Communications, Inc. (MCI) had operated a point-to-point microwave-based long-distance telephone service starting in 1972. (It had taken ten years for the FCC to allow such a service).[62] Local users of this private "point-to-point" service could dial an MCI facility using a local phone, enter an access number to reach a foreign facility, and be connected to a local telephone on the other side.[63]

Concerned that this new service was posing a threat to their traditional long-distance telephone monopoly, AT&T first informally[64] and then formally complained to the FCC that MCI was offering long-distance telephone service under the guise of their "Execunet" point-to-point microwave service.[65] Within a few months, the FCC suspended MCI's tariff "without holding a hearing or even disclosing the details of AT&T's arguments concerning the unlawfulness of

---

58. FCC, *In The Matter of Use of the Carterfone Device in Message Toll Telephone Service; In the Matter of Thomas F. Carter and Carter Electronics Corp., Dallas, Tex. (Complainants), v. American Telephone and Telegraph Co., Associated Bell System Companies, Southwestern Bell Telephone Co., and General Telephone Co. of the Southwest (Defendants).* Docket No. 16942; Docket No. 17073, 13 F.C.C.2d 420 (1968); 13 Rad. Reg. 2d (P & F) 597.

59. *Id.*

60. *Id.*

61. Ismail, *supra*, at 14.

62. Kagami, Tsuji, & Giovannetti, Information Technology Policy and the Digital Divide: Lessons for Developing Countries, 72 (Edward Elgar Publishing Limited 2004)

63. *Id.* at 72.

64. An important anecdote from the court ruling illustrates the incredible regulatory capture AT&T had within the FCC. See MCI v. FCC below: "AT&T… complained orally to the Commission that MCI was offering interstate long distance message telephone service (MTS) under the guise of Execunet and that no such service could properly be tariffed by MCI. *Apparently AT&T representatives approached individual commissioners and various Commission staff personnel with this complaint and even held a demonstration of Execunet in the Commission's offices.* Subsequent to the ex parte complaints, AT&T filed with the Commission a letter which repeated the allegations previously made."

65. *MCI Telecommunications Corporation, Microwave Communications, Inc., and N-Triple-C Inc., Petitioners, v. Federal Communications Commission and the United States of America, Respondents, American Telephone and Telegraph Company, United States Independent Telephone Association, Data Transmission Company (DATRAN), and Southern Pacific Communications Company, Intervenors.* 561 F.2d 365 (D.C. Cir. 1977).

Execunet."[66] MCI sought for a legal stay of the order, and the issue eventually went to the D.C. Circuit.

Once again the D.C. Circuit forced the FCC to abandon its monopolistic tendencies. The court found that there was no mandate suggesting that "that every time a carrier seeks to start a new service over existing facilities it must petition the Commission," and that there was "no affirmative determination of public interest need for restrictions."[67] Much like *Hush-a-Phone* and *Carterfone*, *MCI v. FCC* reinforced the notion that a "mother may I" policy towards innovating within the FCC's area of jurisdiction was inappropriate.

The court poignantly explained that it was troubled with the FCC's implicit notion that AT&T was a monopoly to be protected:

> As a final and somewhat collateral point, we are concerned with a thread running through the Commission's analysis that the Specialized Carrier decision granted AT&T a de jure monopoly … which would be undermined were MCI allowed to provide Execunet because any such assertion is plainly incorrect and may have influenced the Commission's disposition of the instant case.
>
> ...The question whether AT&T should be granted a de jure monopoly was not among those proposed to be decided in Specialized Carriers, and nowhere in that decision can justification be found for continuing or propagating a monopoly… Of course, there may be very good reasons for according AT&T de jure freedom from competition in certain fields; however, one such reason is not simply that AT&T got there first.[68]

It is important to note that this decision in 1977 came in the midst of United States v. AT&T, which had been filed by the Department of Justice in 1974 and would eventually lead to the structural divestiture of AT&T's equipment and long-distance arms in 1984 (mandated in 1982). In *MCI v. FCC*, we can see the evolving concern of a publicly sanctioned monopoly on telecom.

What were the effects of these three decisions on the FCC's economic leanings? Prior to *Hush-a-Phone*, the FCC effectively functioned as a monopoly-sanctioning agency rather than a regulator of free commerce, working hand-in-hand with incumbents to support the industry standard. The court-mandated liberalization of the FCC's rigid monopoly polices forced the Commission to acknowledge that a moderate deregulation of control could lead to positive consumer benefits.

The FCC was still not at a point of using explicit economic theory to reach their conclusions for these matters. In the following years, there would be some evidence of an economic-oriented mindset at the agency. These decisions, coupled with the breakup of AT&T, likely changed the FCC's attitude towards economic analysis.

---

66. *Id.*
67. *Id.*
68. *Id.*

4. Computer Inquiry I (1970)

Perhaps the most notable example of the agency's early use of economic analysis to inform its policy was the FCC's treatment of the emerging technology of computer networking. By 1966, mainframe computers were an American reality. Not only were computers being used to process data in previously impossible ways, but they were also being used to support the telecom network. Complications began to arise when it became clear that computers could perform both functions simultaneously, and the FCC needed to understand where regulation of these devices and services would fall.

There were two main problems: The first was that the computers performed an unregulated function similar to an existing regulated service: telegrams. The telegram network would operate in a fashion similar to modern-day servers. Living operators, upon receiving a message, would pass along the message to the next node until finally reaching its destination. Mostly provided by Western Union, the FCC had regulated this service since the Communications Act of 1934.[69] Mainframe computers, which could be connected to the ends of existing telephone lines, could do this automatically using the existing phone-line infrastructure.

The second problem was how to regulate common carriers, which often had excess computing power from computers normally used to support their telecom networks. Naturally, these carriers desired to sell this surplus as a service. Under normal circumstances, this would be a non-issue to the FCC, but AT&T was a protected monopoly under their jurisdiction. The FCC had to address public concerns that common carriers could "subsidize their data processing operations with revenues and resources available from their regulated services."[70]

As in previous scenarios, the FCC called for public commentary on the matter. Instead of relying solely on public commentary, as it had in the past, the FCC additionally commissioned the Stanford Research Institute (SRI) to study the problem in detail from an economic and technical perspective.[71] After reviewing the public commentary, SRI conducted their own economic analysis of the issues and presented their findings to the FCC in a series of seven reports. They reached three conclusions: (1) That "data communication services" were rapidly growing and FCC action may not be required (but should be studied further); (2) that data processing services would benefit from free entry and unregulated competition by non-carriers; and (3) that allowing common carriers to enter the data processing field could be problematic.[72]

SRI's economic analysis of the emerging markets was critically important, because the FCC's policy prescriptions were based on the market in which each service was perceived to exist.

---

69. Robert Cannon, *The Legacy of the Federal Communications Commission's Computer Inquiries*, 55(2) FED. COMM. L. J. 170 (2003).

70. *Id.* ¶25.

71. *In the Matter of Regulatory and Policy Problems Presented by the Interdependence of Computer and Communication Services and Facilities, Tentative Decision,* ¶3 (Computer I, Tentative) (1970), *available at* http://hdl.handle.net/2027/msu.31293012269308.

72. *See* Donald Dunn, *Policy Issues Presented by the Interdependence of Computer and Communications Services*, __ LAW & CONTEM. PROBLEMS 369-88 (1969), *available at* http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=3248&context=lcp.

Largely following the SRI report's recommendations, the FCC concluded "that the offering of data processing services is essentially competitive and that… there is no public interest requirement for regulation by government of such activities."[73] Computer services were to be put into two categories: "Pure communication" and "pure data processing." The former was where a message was transmitted over the network with no change in content or form, while the latter involved computers that stored, retrieved, sorted, merged, and calculated data.[74] The FCC was unsure what to do with marginal cases, where there was "an offering of service which combines Remote Access data processing and message-switching to form a single integrated service."[75] To address this ambiguity, they created a "hybrid" category that they would evaluate on a case-by-case basis. This grey area eventually consumed the rule and lead to Computer Inquiry II.

On the issue of common carriers competing in the data processing market, the FCC reasoned it was within their powers to bar AT&T from competing in a non-regulated market, but elected not to do so. The agency instead required that a common carrier could offer data processing only under a fully separate subsidiary.[76]

Computer Inquiry I is thus a clear example of the FCC calling for an impartial economic analysis of a technical situation, and then basing policy on the estimated costs and benefits of intervening in a market. Their economic reasoning was also outlined in a statement of principles within the *Inquiry*:

> In this country, we rely upon the 'free enterprise' system with the maximum possible latitude for individual initiative to enter into any given enterprise and compete for the available business… Government intervention and regulation are limited to those areas where there is a natural monopoly, where economies of scale are of such magnitude as to dictate the need for a regulated monopoly, or where such other factors are present to require governmental intervention to protect the public interest because of a potential for unfair practices exists.[77]

We can see an intriguing rationalization at play: Based on the SRI reports, the FCC concluded that computers had no natural monopoly, although they were predicated on the existence of a telecom network. This meant that they were outside the ambit of the FCC. However, the network itself was still a natural monopoly under AT&T, and thus needed the FCC's guiding hand.

5. Computer Inquiry II and the Office of Plans and Policy (1980)

Perhaps the most significant indicator of the growing popularity of economic analysis at the FCC was a staffing change that would shape *Computer Inquiry II* and all policy that followed it. Under the direction of FCC Chairman Charles Ferris, the Commission officially embraced economics by retooling the Office of Plans and Policy (OPP) to be the in-house, economic think-

---

73. Computer I, Tentative ¶20
74. *Id.* at 174.
75. *Id.* ¶15.
76. Cannon, *supra*, 178.
77. Computer I, Tentative ¶19

tank of the FCC, which previously had no real internal economic division. Derthick and Quirk (1985) describe the economic enlightenment as follows:

> [Ferris] enlarged the functions of the FCC's Office of Plans and Policy and naming an economist to head it. Both this economist, Nina W. Cornell, and Ferris's general counsel, Robert R. Bruce, were strongly critical of traditional public utility regulation; as such, they exemplified the 'latest and best thinking.' … When Cornell and Bruce, as generalist in favor of procompetitive deregulation were joined by a Common Carrier Bureau chief who shared that objective, the way was prepared for the outcome of the Computer II inquiry in the spring of 1980. This outcome represented a sweeping retreat from traditional public utility regulation, with its focus on rate setting, and the embrace instead of a structural approach to preventing predatory conduct…"[78]

OPP was a major contributing force to the FCC's shift to embracing economic analysis. OPP immediately set to work and began production of the FCC's 46 economic working papers—a practice that continued until 2012 (a potential end of economics at the FCC).[79] In its first year of operation under its new mandate, OPP produced four working papers alone that centered on the themes of deregulation, competition, and analyzing telecom policy from an economic standpoint.[80] OPP would form the economic core of the FCC, and would produce economic analysis until 2003, when it would be rebranded as the Office of Strategic Planning and Policy Analysis.[81]

Meanwhile, the "hybrid" cases outlined in *Computer Inquiry I* had become a problem for the FCC. Not only were there a multitude of services that fell into this category, but the cost of computer equipment began to plummet as its complexity exploded. Microcomputers began to appear in consumer phones. The first demonstrations of what ultimately would become the Internet were debuted to the public in 1972. A new framework was needed.[82]

The FCC responded by redefining the market into two categories: Basic and Enhanced Services. Basic transmission services were defined as those that were "limited to the common

---

78. MARTHA DERTHICK & PAUL QUIRK, THE POLITICS OF DEREGULATIONS 79 (Brookings Institution Press 1985).

79. *See the FCC's Repository of Working Papers, available at* https://www.fcc.gov/reports-research/working-papers

80. *See* Cornell, Kelly & Greenhalgh, *Social Objectives and Competition in Common Carrier Communication: Incompatible or Inseparable?*, FCC OSP Working Paper 1 (1980); Douglas Webbinick, *Frequency Spectrum Deregulation Alternatives*, FCC OSP Working Paper 2 (1980); Duvall & Pelcovits, *Reforming Regulatory Policy for Private Line Telecommunications Services: Implications for Market Performance*, FCC OSP Working Paper 4 (1980); Brown & Gordon, *Economics and Telecommunications Privacy: A Framework for Analysis*, FCC OSP Working Paper 5 (1980)

81. *See FCC 2002 Annual Program Performance Report* and *FCC 2003 Annual Program Performance Report*, available at https://transition.fcc.gov/Reports/ar2002.pdf and https://transition.fcc.gov/Reports/ar2003.pdf

82. In the Matter of Amendment of Section 64.702 of the Commission's Rules and Regulations (Second Computer Inquiry), Tentative Decision and Further Notice of Inquiry and Rulemaking ¶10-12 (Computer II, Tentative) (1979), in Federal Communications Commission Reports, Volumes 72 Second Series 358 (1979), available at http://hdl.handle.net/2027/msu.31293012269761

carrier offering of transmission capacity for the movement of information."[83] In other words, "the direct analog or digital transmission of voice, data, video, etc."[84] Storage or alteration of data was only appropriate to facilitate the reliable movement of the information. Anything that offered more than that basic service was considered to be an enhanced service.[85]

As before, basic services would fall under the regulation of the FCC, whereas enhanced services would not. Enhanced services were thought to be competitive, as they occupied the same "truly competitive" market as "data processing" did in *Computer Inquiry I*.[86] The FCC also doubled down on its treatment of common carriers in the data-processing market. If AT&T and GTE wished to offer enhanced services, they were required to establish a subsidiary as before.[87] This "relatively clear-cut" line between basic and enhanced services was intended to end any regulatory ambiguity associated with *Computer Inquiry I*'s hybrid cases.[88]

The FCC reached this decision "based on the voluminous records compiled in this proceeding."[89] Although it did not directly commission an analysis as it did in *Computer Inquiry I*, the FCC did rely on economic theory for its major decisions. The Commission routinely cited economist Alfred Kahn, "one of our country's leading authorities in regulatory economics," for his work *The Economics of Regulation* (1971), which examined how competition affected innovation.[90] The FCC also cited academic literature on predatory-pricing practices,[91] other economic papers on monopoly and innovation,[92] and on how bundling restricts the choices of consumers.[93]

6. Computer Inquiry III (1986)

A similar, if less revolutionary, economic approach was used for *Computer Inquiry III*. Following a settlement with the Department of Justice, by 1984, AT&T had divested its local service operations, forming the Regional Bell Operating Companies (RBOCs). The Domain Name System (DNS) was introduced in 1985, and the Internet was on the cusp of becoming a reality.

The problem this time was not the definition of services, but the inability of the newly formed RBOCs and other carriers to enter the enhanced services market. *Computer Inquiry II* required the structural separation of AT&T and GTE from any enhanced services. Originally the FCC had applied this policy to the RBOCs, but the Commission "found that the costs of those

---

83. In the Matter of Amendment of Section 64.702 of the Commission's Rules and Regulations (Second Computer Inquiry). Final Decision, ¶93 (Computer II, Final) (1980), in Federal Communications Commission Reports, Volumes 77 Second Series 384 (1980), *available at* http://hdl.handle.net/2027/msu.31293000344147
84. *Id.*
85. *Id.*
86. *Id.* ¶128
87. Cannon, *supra*, 184.
88. Computer II, Final ¶97
89. *Id.* ¶5
90. Computer II, Final ¶212
91. Computer II, Final ¶153
92. Computer II, Final ¶212, n. 84, 85.
93. Computer II, Final ¶149, n. 55.

requirements in lost innovation, inefficiency, and delay outweigh their benefits."[94] The FCC also sought to prove more "competition-oriented" regulation, which would allow dominant carriers to offer enhanced services. The short term solution to this was to allow the RBOCs to offer services, but only if they provided a "Comparatively Efficient Interconnection (CEI) of third party enhanced service option to the customer.[95] The longer-term solution was the implementation of "Open Network Architecture" (ONA), which would require the RBOCs to unbundle their basic service offerings for all enhanced service providers.[96]

All of these decisions were based on a practical cost-benefit analysis of maintaining structural separation, a reflection of economics' newfound influence at the Commission. The FCC not only investigated the costs and benefits of structural separation,[97] but it also used economic analysis to investigate alternative regulatory approaches and their potential effects.[98] Although several of the Commission's decisions in *Computer Inquiry III*, including the ONA ruling, faced legal hurdles in the Ninth Circuit Court of Appeals, and the ONA ruling was eventually sent back to the FCC, the Commission maintained its overall deregulatory thrust.[99]

C. Peak of Economic Analysis in the 1990s and Aughts

The 1990s were the high water mark of economics at the FCC. Through Congressional action, the standard method of assigning radio spectrum licenses by regulatory fiat (often with strong political influence) gave way to allocating spectrum by auction, as suggested by FCC economists Evan Kwerel and Alex Felker[100] (based on earlier work by Ronald Coase). The FCC adopted a light-touch regulation of rapidly growing wireless service and held fast to the strict separation between regulated basic service (voice telephony and pure data transmission) and unregulated "enhanced" services (data processing, especially Internet), established by the earlier *Computer Inquiry I, II,* and *III*. This economic mindset was built into the Telecommunications Act of 1996, which was designed to create a procompetitive deregulatory framework intended to encourage private-sector competition by opening all markets to competition and relying on market forces instead of regulation wherever possible.[101]

---

94. FCC, *In the Matters of Amendment of Sections 64.702 of the Commission's Rules and Regulations (Third Computer Inquiry); and Policy and Rules Concerning Rates for Competitive Common Carrier Services and Facilities Authorizations Thereof Communications Protocols under Section 64.702 of the Commission's Rules and Regulations*, ¶2 (Computer III) (1986), in Federal Communications Commission Reports, Volumes 104 Second Series 958 (1986), *available at* http://hdl.handle.net/2027/inu.30000038968941.

95. *Id*.

96. Cannon, *supra*, at 201.

97. Computer III, ¶80-99.

98. Computer III, ¶102.

99. Cannon, *supra*, at 202

100. Evan Kwerel & Alex Felker, *Using Auctions to Select FCC Licensees* (1985), FCC OSP Working Paper #16, *available at* https://www.fcc.gov/reports-research/working-papers/using-auctions-select-fcc-licensees.

101. At this time, only voice access line service was arguably a monopoly; most other voice services were substantially competitive (or getting there). Hence, the emphasis in the Telecommunications Act on voice access line policy.

1. Auctions Replace Beauty Pageants (1993)

Economic influence at the Commission would mark the end of zero-price spectrum. The key to arriving at the right price was auction design. Not only had economists steered the FCC toward the efficient policy, the implementation of that policy also required the input of economists. Although the FCC's lotteries technically satisfied the Coase Theorem—in which an improperly allocated good can eventually end up in the hands of the entity that values it the most if transaction costs are low—it took years for the secondary markets to distribute these licenses accordingly.[102] One paper estimated that the "ten year delay in cellular licensing cost the U.S. economy the equivalent of two percent of Gross National Product."[103]

In 1993, Congress amended the Communications Act of 1934 to require the FCC to award spectrum based on competitive bidding.[104] Congress specifically required the FCC to design the allocations in a way to fulfill its objectives of "promoting economic opportunity and competition and ensuring that new and innovative technologies are readily accessible to the American people by avoiding excessive concentration of licenses and by disseminating licenses among a wide variety of applicants."[105] The Commission developed a simultaneous multiple-round bidding system, which successfully fulfilled the new mandate.[106] This would allow firms to intelligently shift their bids to other areas of spectrum if their first choice became untenable.[107] The new system was widely considered a success and is used today.

The first auction took place in 1994, and concerned nationwide licenses for narrowband personal communications services such as paging; six bidders won ten licenses, and auction receipts totaled $650 million.[108] One indication of the program's success is the decline of the secondary market transactions. Between 1994 and 1996, only 12 licenses were resold, compared to 75 resales in the 1991 cellular license lottery.[109] Another sign of success is that between 1994 and 1997, over half of all spectrum licenses went to small business and new entrants to the telecommunications markets.[110]

It is important to remember that while the FCC was given the mandate to shift to an auction system by the legislature, the system was largely based on the work of the OPP economists who called for an auction system in previous years.

---

102. *Id.*
103. *See* Jeffrey Rohlfs, Charles Jackson & Tracey Kelley, Estimate of the Loss to the United States Caused by the FCC's 14 Year Delay in Licensing Cellular Telecommunications, National Economic Associates, Inc. (1991).
104. H.R. 2264 §6002 (a) ("If mutually exclusive applications are accepted for filing for any initial license or construction permit which will involve a use of the electromagnetic spectrum described in paragraph (2), then the Commission shall have the authority, subject to paragraph (10), to grant such license or permit to a qualified applicant through the use of a system of competitive bidding that meets the requirements of this subsection").
105. *Id.*
106. *The FCC Report to Congress on Spectrum Auctions*, at 3 (1997) (hereinafter *FCC Spectrum Report*).
107. *Id.* at 25.
108. FCC, Auction 1: Nationwide Narrowband (PCS), *available at* http://wireless.fcc.gov/auctions/default.htm?job=auction_summary&id=1.
109. *FCC Spectrum Report*, at 23.
110. *Id.*

2. The Telecom Act of 1996 Places Competition on the Pedestal

The passage of the 1996 Telecommunications Act fundamentally reshaped the way the FCC approached regulation. The Act had a single goal: "To promote competition and reduce regulation in order to secure lower prices and higher quality services for American telecommunications consumers and encourage the rapid deployment of new telecommunications technologies."[111] The word "competition" and its derivatives appear 61 times throughout the 106 page document. To implement these objectives, the FCC would be forced to incorporate economics into the heart of its decision-making.

The Act noted specifically that "The Internet and other interactive computer services have flourished, to the benefit of all Americans, with a minimum of government regulation," and charged the FCC with a number of objectives in promoting the deployment of "advanced telecommunications" across the United States"[112] The FCC's new mandate was to promote policies favoring "vigorous economic competition, technological advancement, and promotion of the public interest, convenience, and necessity."[113]

3. Regulatory Humility Part 1: Hands Off the Internet

The unregulated treatment of the Internet was not an accident. It stemmed from the view developed from the Computer Inquiries that the "the Internet" in composite was a collection of enhanced services, based upon the physical structure of regulated basic services. In 1999, OPP economist Jason Oxman published a working paper to identify what the agency had done right.[114] Oxman noted that the Internet owed much of its success to the FCC's consistent refusal to regulate any part of it. He presciently noted that there would be pressures in the future to regulate:

> Although the FCC has a long tradition of encouraging the growth and development of the Internet by nonregulation, deregulation, and certain affirmative market-opening policies, there are frequent calls from many sources for the FCC to become more heavily involved in Internet regulation. …The challenge to the FCC… is to … further the Commission's longstanding goal of promoting competition, not regulation, in the marketplace.[115]

There are a few concrete examples of the FCC taking direct "un-regulatory" action. Before Internet Service Providers (ISPs) were a reality, the FCC decided in 1983 to exempt "enhanced service providers" from usage-based access chargers, so that access to the network would not face charges similar to long distance calls. Because the FCC decided that these providers were not

---

111. 47 U.S.C.Preamble.
112. *Id.* §706 (c)
113. *Id.* §257 (b)
114. Jason Oxman, *The FCC and the Unregulation of the Internet*, FCC OPP Working Paper #31 (July 1999), *available at* http://www.fcc.gov/Bureaus/OPP/working_papers/oppwp31.pdf.
115. *Id.* at 21.

common carriers, they did not warrant the same per-minute pricing treatment, and instead mandated essentially a flat end-user rate.[116]

Another example occurred in 1997, when the FCC decided that ISPs were not required to make contributions to the Universal Service Fund USF, a public-works program to bring physical telecommunication lines to rural areas. This reinforced the notion that ISPs were to remain unregulated.[117]

Most importantly, the FCC decided that it would not regulate the deployment of cable modem services as common carriers.[118] (Alas, telco-based DSL services were not so fortunate.) This decision would have profound implications for the growth and development for cable-based Internet services. This would have a profound effect on investment. Between 1998 and 1999, cable modem connections had grown from 100,000 to 750,000.[119] Following a legal battle culminating in 2005, the FCC would extend this deregulation to DSL services, bringing it on equal footing as the "Commission's light regulatory treatment of cable modem service."[120]

As final testament to the FCC's un-regulatory policy towards the Internet, in 1999, then-Chairman William Kennard declared:

> The best decision government ever made with respect to the Internet was the decision that the FCC made 15 years ago NOT to impose regulation on it. This was not a dodge; it was a decision NOT to act. It was intentional restraint born of humility. Humility that we can't predict where this market is going. [121]

This sentiment is in concert with Oxman, who concludes that part of the success of the Internet was thanks to the FCC's policy of free competition. This decision to un-regulate was based on the economic philosophy that flowed from a number of factors, including *Carterfone*, *Hush-A-Phone*, and *Computer Inquiries*.

4. Regulatory Humility Part 2: Wireless

A similar un-regulation story played out in the nascent wireless industry. In the 1970s, the FCC had no notion of how popular wireless telephony would become. The Commission had initially planned to license only one cellular telephone service, which would be operated by the

---

116. *See* FCC, In the Matter of MTS and WATS Market Structure, Memorandum Opinion and Order (1983), in Federal Communications Commission Reports, Volumes 97 Second Series 682 (1983), available at http://hdl.handle.net/2027/msu.31293106457686

117. *Id.* at 18.

118. *Id.* at 21.

119. William E. Kennard, *The Road Not Taken: Building a Broadband Future for America*, remarks at the National Cable Television Association, (June 15 1999), *available at* https://transition.fcc.gov/Speeches/Kennard/spwek921.html

120. *FCC Eliminates Mandated Sharing Requirement on Incumbents' Wireline Broadband Internet Access Services*, FCC News (August 5, 2005), *available at* https://apps.fcc.gov/edocs_public/attachmatch/DOC-260433A1.pdf

121. *Id.*

local telephone company. To "promote competition" in their monopoly market, in 1981, the FCC increased the number of licenses allocated to two—adding a completely unaffiliated company in addition to the local one.[122]

Unsurprisingly, this intervention did not yield competitive outcomes. Later, the FCC somewhat humorously noted that "The duopoly nature of cellular service made it less than fully competitive."[123] In 1995, the Commission awarded new licenses by auction.[124] They allocated enough spectrum to ensure "at least three, and possibly as many as six" new competitors in each market.[125]

In addition to this measure, the FCC systematically removed regulatory barriers to wireless deployment. Similar to the deployment of cable (and later broadband), the FCC decided not to regulate cellular service under Title II, and pre-empted state regulation of entry and rates.[126] This was a part of the FCC-wide trend towards reduced regulation.

The results were tremendous. In the FCC's first Commercial Mobile Services Report to Congress in 1995, there were 25 million cellular subscribers.[127] By the fifth report in 2000, that number was over 86 million.[128] The 2000 report also noted that the cellular industry was not only competitive, but that prices to consumers had fallen by 10 to 20 percent from the previous year.[129]

This decision was reached on clear economic grounds. The 1995 Memorandum and Order on wireless reads like an economic report. After an executive summary of the technology, market, and decision, the paper launches into a technical and economic study of the markets of each wireless category. In the discussion of competition, the report incorporates analyses of prices, tax returns, volumes, cash flows, and even regression analysis on estimated rates of returns.[130] It is clear from this document that the justification for the liberalization of the wireless markets was based on a pragmatic economic analysis of competition.

5. The TELRIC Quagmire (1996-2005)

One provision of the 1996 Act was the unbundling of local carriers' networks, requiring carriers to offer competitors access to its network elements, who in turn could resell access under

---

122. In the Matter of Implementation of Section 6002(B) of the Omnibus Budget Reconciliation Act of 1993 Annual Report and Analysis of Competitive Market Conditions with Respect to Commercial Mobile Services (First Report), 1 (1995), *available at* http://wireless.fcc.gov/auctions/data/papersAndStudies/fc95317.pdf.

123. Id. ¶4.

124. *Id.*

125. *Id.*

126. *Id.* ¶5.

127. *Id.*

128. In the Matter of Implementation of Section 6002(B) of the Omnibus Budget Reconciliation Act of 1993 Annual Report and Analysis of Competitive Market Conditions with Respect to Commercial Mobile Services (Fifth Report), 87 (2000), *available at* http://wireless.fcc.gov/auctions/data/papersAndStudies/fc000289.pdf

129. *Id.* at 4-5.

130. In the Matter of Implementation of Section 6002(B) of the Omnibus Budget Reconciliation Act of 1993 Annual Report and Analysis of Competitive Market Conditions with Respect to Commercial Mobile Services (First Report) (1995).

their own brand name and price.[131] This provision required the FCC to develop a pricing method that approximated competitive outcomes, which the FCC interpreted to mean prices that approximated the incumbent local exchange carrier's total element long-run incremental cost (TELRIC). Homogeneous-product competition among resellers was intended to drive retail prices down to the TELRIC rate.

To induce an incumbent to voluntarily cede a retail customer to a rival, the access price would have to make the incumbent indifferent between serving as a wholesaler and serving as a retailer. Mathematically, the access price must be set equal to the incumbent's forgone retail margin. While the FCC could compel a local carrier to set its access price below its forgone retail margin—that is, below the market-determined access price—doing so would dampen incentives on all parties (access provider and access seeker) to innovate and invest.[132] Forcing the resale of network at below-market rates necessarily means there is less of an incentive to develop networks for the future, in addition to other negative consequences.[133]

The FCC's initial report developed national TELRIC pricing principals as a methodology that each state could adjust for its specific use.[134] Notwithstanding the potential dynamic efficiency losses from unbundled access, we see the clear influence of economics in the rate-setting process. Section VII of the FCC's document, which is dedicated to the pricing methodology of TELRIC, draws from a wide range of commentary and economic literature to inform its methodology.[135] In particular, the Commission took into account a host of cost variables, including forward-looking common costs, reasonable returns on investment, and profit.[136] The model they developed included price ceilings for each state,[137] and specifically listed the resale-pricing standard.[138]

In 1999, this unbundling regime was expanded to require local exchange carriers (LECs) to share a portion of their lines with resellers of DSL service at regulated rates ("line sharing"). Although DSL was not reclassified as an information service until August 2005, the appeals courts largely disemboweled the FCC's common-carrier regime well before 2005. The D.C. Circuit vacated the FCC's *Line Sharing Order* in May 2002,[139] and the FCC eliminated line sharing as an unbundled network element in August 2003.[140] Other portions of the FCC's unbundling rules were vacated even earlier. While TELRIC was ultimately a legal and regulatory quagmire brought on

---

131. Tom Jorde, Gregory Sidak & David Teece, *Innovation, Investment, and Unbundling*, 2 YALE J. ON REG. 1-37 (2000) *available at* http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1283&context=facpubs.

132. *Id.* at 4-5.

133. *See* Robert S. Pindyk, *Mandatory Unbundling and Irreversible Investment in Telecom Networks*, (2003), MIT Sloan School of Management Working Paper 4452-03, *available at* http://digilander.libero.it/vergalli/pdf/19.pdf.

134. In the Matter of Implementation of the Local Competition Provisions in the Telecommunications act of 1996, Interconnection between Local Exchange Carriers and Commercial Mobile Radio Service Providers, First Report and Order, ¶¶6, ¶625 (1996), *available at* https://transition.fcc.gov/Bureaus/Common_Carrier/Orders/1996/fcc96325.pdf.

135. *Id.* ¶618.

136. *Id.*

137. *Id.* Tables A, D.

138. *Id.* §51.609.

139. US Telecom Ass'n v. FCC, 290 F. 3d. 554, 585 (D.C. Cir. 2004).

140. Review of the Section 251 Unbundling Obligations of Incumbent Local Exchange Carriers, CC Docket Nos. 01-338 et al., FCC 03- 36, 18 FCC Red 16978 (Aug. 21, 2003) (Triennial Review Order), ¶199.

by provisions of the 1996 Act, the FCC can be credited with attempting to determine mandated prices in an economically coherent way.

6. The Brewing War Over Net Neutrality (2005-10)

As Oxman predicted, the FCC was constantly showered during the aughts with recommendations from self-styled consumer interest groups. Around the turn of the century, the burning issue was "Open Access"—establishing rules that cable systems had to open up their facilities to virtual ISPs, similar to how mandated unbundling at regulated rates opened telephone access lines (including DSL service) to competitive local exchange carriers.[141] One author (Faulhaber) recalls his time as Chief Economist at the FCC (in 2000), when he found a television crew filming a group of about fifteen young people parading around the FCC's front door with signs and placards demanding the FCC mandate Open Access. Upon questioning, group members had only a hazy understanding of the issues, admitting they were students at local universities who had been hired by a consumer group (again, hazy on the name) to parade around with said signs. The television crew soon packed up and left, and the protestors left soon afterwards. At the time, such pressure was routine, but if there were no supporting economic data to back up the demands, the FCC gave those efforts short shrift.

Fast forward five years, and "Open Access" had morphed into "Network Neutrality," largely based on the seminal article by Wu.[142] Under Chairman Michael Powell, the FCC published four principles of net neutrality[143] under the agency's Title I authority. The first net neutrality case involved the Madison River Telephone Company, which had blocked a provider of voice telephony over the Internet in its North Carolina operations. The FCC resolved the issue quickly, with a fine and commitment from the firm not to engage in further blocking. A second case, involving Comcast blocking BitTorrent (a peer-to-peer video file sharing application) was much more prominent in the news in 2007-08. Comcast voluntarily agreed to change its network management practice, but the Commission nonetheless proceeded months later to find Comcast's practice to be unlawful.

Comcast sued the FCC, arguing that the four "principles" it had adopted earlier did not have the force of regulation. The D.C. Circuit did not reach that conclusion but agreed with Comcast that the FCC had not established legal authority to regulate Internet practices,[144] much to the chagrin of consumer groups who had lobbied hard for network neutrality regulation. The FCC understood that an actual regulation was required to put network neutrality in place, and opened the Open Internet proceeding, to satisfy the Court's requirement that an actual regulation, as opposed to an informal statement of principle, was needed for enforcement purposes.

---

141. The requirement that telephone companies had to unbundle and resell DSL service was eventually rescinded. However, most European countries mandate resale of broadband facilities (often a state-owned monopoly) to virtual ISPs.

142. Tim Wu, *Network Neutrality, Broadband Discrimination*, 2 J. TELECOM. & HIGH TECH. 141 (2003).

143. In brief, the principles were: Transparency, No blocking or unreasonable discrimination, reasonable network management, and lighter rules for mobile.

144. Comcast v. FCC, ___ F.3d ___ (D.C. Cir. 2010).

The FCC responded to this loss with a curt and curious statement: "Today's court decision invalidated the prior Commission's approach to preserving an open Internet. But the Court in no way disagreed with the importance of preserving a free and open Internet; nor did it close the door to other methods for achieving this important end."[145] In other words, the FCC was committed to its position. It would find a way to enforce its version of net neutrality, one way or another.

The 2010 *Open Internet Order* (*2010 OIO*) was the FCC's codified rulemaking on the matter. After seeking a public commentary period in which "100,000 commenters have provided written input," the Commission stated that their "economic analysis demonstrate, however, that the openness of the Internet cannot be taken for granted, and that it faces real threats."[146]

What were these threats? In the FCC's initial inquiry, the Commission cited developments in network technology that allowed providers to "offer different qualities of service to different traffic (service differentiation), which enables charging different prices for different traffic (price differentiation)."[147] Such disparate treatment would allow ISPs to prioritize packets either based on origin or on class. The example given was Skype, which required low latency and reliable delivery.

There was general concern that, "absent appropriate oversight, broadband Internet access service providers could make the Internet less useful for some users or applications by differentiating traffic based upon the user, the application provider, or the type of traffic."[148] Critically, these potential problems were not realized. For example, in the *2010 OIO*, the FCC wrote that "the record in this proceeding reveals that broadband providers potentially face at least three types of incentives to reduce the current openness of the Internet."[149] These claims were not grounded in economic analysis done by the Commission or any economist, but instead were based on the comments of DISH, Google, Netflix, Skype, and other vested interest groups.[150] Critics of the Commission's approach pointed to the fact there was no evidence of this practice adversely affecting users; they asserted that net neutrality is "a solution in search of a problem."[151]

Lacking evidence of harm, the Commission nonetheless determined that the benefits of pursuing an "Open Internet" policy exceeded the costs. Harkening back to the FCC's early years, the issue was settled on public commentary of non-economic, vested entities. No economic analysis of the situation took place. Of the 24 citations the Commission lists in its "cost and benefit analysis" in the *2010 OIO*, not a single citation links to any economically rigorous study of the

---

145. FCC Statement on Comcast v. FCC Decision (April 6, 2010), *available at* https://apps.fcc.gov/edocs_public/attachmatch/DOC-297355A1.pdf.

146. In the Matter of Preserving the Open Internet Broadband Industry Practices, Report and Order (hereinafter *2010 OIO*), ¶4 (2010), *available at* https://apps.fcc.gov/edocs_public/attachmatch/FCC-10-201A1_Rcd.pdf

147. FCC, *In the Matter of Preserving the Open Internet Broadband Industry Practices, Notice of Proposed Rulemaking* (2010 Open Internet Order Proposed Rulemaking), ¶57 (2009)

148. *Id.* ¶60.

149. *2010 OIO* ¶21 (emphasis added).

150. *Id.* n.11-21

151. *Id.* See Dissenting Statement of Commissioner Meredith Attwell Baker at 193.

situation.[152] The Commission's analysis rested on the basis of casual logic and the court of public opinion.

Despite its flaws, one redeeming quality of the *2010 OIO* was its treatment of "reasonable discrimination." The Order did not flat-out ban network shaping, so long as the broadband provider was transparent and gave the end-user some control over this shaping.[153] In addition, the Commission did not prevent tiered or usage-based pricing packages, so that lighter users of Internet services would not subsidize heavy ones.[154] In sum, the Commission offered a discrimination policy of "reasonableness" based on "achieving a legitimate network management purpose."[155] This reluctance to ban practices that might be motivated for pro-competitive reasons would melt away in the FCC's subsequent populist period.

III. The Stripping of Economics from FCC Decision-Making

When it comes to regulating broadband, the Telecom Act's mandate leaves the FCC with a narrow role. The Act could not be clearer regarding regulation of the Internet: "The Internet and other interactive computer services have flourished, to the benefit of all Americans, *with a minimum of government regulation.*"[156] In light of this finding, the Act declares the policy of the United States is "to preserve the vibrant and competitive free market … for the Internet and other interactive computer services *unfettered by Federal or State regulation*."[157] Congress also made clear that information services are among the interactive computer services that should remain free from regulation, and that services that "provide[] access to the Internet" are information services.[158]

The focus of the Act was regulating wireline voice services, once the centerpiece of communications but now a dying industry. Soon after the Act's passage, landline connections began to be displaced by wireless ones.[159] Even voice over wireless is being replaced with VoIP, text messages, emails, and direct messaging through social media sites. This shift in the way we communicate severely limits the FCC's jurisdiction and thus its reason for being. Put differently, the evaporation of the core businesses subject to FCC oversight minimizes the relevancy of the FCC in the Internet era. Without a new mandate from Congress, the agency chose in its 2015 *Open Internet Order* to embrace populism, grounding its newfound "authority" in the will of the people.

A. The Shunning of Cost-Benefit Analysis in the Wheeler Era

Economics guides regulators to act only when confronted with an empirically demonstrated

---

152. *Id*. at 23-27.
153. *Id*. at 40.
154. *Id*.
155. *Id*. ¶82.
156. 47 U.S.C. § 230(a)(4)(1996) (emphasis added).
157. 47 U.S.C. § 230(b)(2)(1996) (emphasis added).
158. 47 U.S.C. § 230(c)(2)(1996).
159. Kevin Caves, *Quantifying Price-Driven Wireless Substitution in Telephony*, 35 TELECOM. POL'Y 984-998 (2011).

market failure (such as monopoly or an externality). If there is no market failure to correct, then there can be no benefit to any new regulation, only costs, and the regulator should stay out. After identifying a perceived market failure and proposing a remedy to address it, economics teaches us that the proposed remedy must pass a cost-benefit test. A regulatory agency may fail a cost-benefit test in three ways. First, the agency can overstate the benefits of its proposed remedy. Second, the agency can understate the costs of its proposed remedy. Third, and a bit less obvious, the agency can ignore a less-restrictive alternative that would generate the same purported benefits but at a lower cost, thereby rendering its proposed remedy inefficient. For example, if the net benefits of a proposed remedy are $10 million per year, but a less-restrictive alternative generates net benefits of $15 million, then the proposal fails a cost-benefit test, even though the proposed remedy would have generated benefits in excess of costs.

Eschewing the lessons of cost-benefit analysis in particular and economics generally, the FCC has steered towards a new era of populism during the Wheeler administration. Three decisions from 2013-15 make clear that economics has been all but removed from the FCC's decision-making process. We briefly review those decisions, contrasting the policies implied by economic reasoning to those adopted by the FCC.

1. The *2015 Open Internet Order*

Paid prioritization arrangements, which involve a payment by an edge provider to an ISP for special handling, could be beneficial for all parties, including end users, so long as edge rivals that forgo such offers are not worse off in *absolute* terms; by design, edge rivals that forgo paid prioritization are worse off in *relative* terms. This recognition puts the lie to the "zero-sum hypothesis" peddled by net neutrality proponents—namely, that any priority arrangement must come at the expense of non-prioritized traffic.[160] Paid prioritization has existed in other portions of the network, and can be readily engineered to keep others whole.[161]

There are four options to dealing with paid prioritization arrangements: (1) no sector-specific regulation, with a reliance instead on antitrust; (2) case-by-case adjudication, with a presumption against any such deals; (3) case-by-case adjudication, with a presumption in favor of any such deals; and (4) a blanket prohibition on all paid prioritization deals. Assuming the case for regulation were satisfied, an economist would tend to favor case-by-case treatment over blanket bans, as paid prioritization arrangements can be motivated for legitimate business reasons. By extinguishing procompetitive arrangements—the proverbial tossing the baby with the bathwater—a blanket ban would generate an intolerably high number of errors (alongside the associated error costs). With respect to the optimal setting of the presumption, antitrust dictates that the presumption should be in favor of vertical arrangements, with the burden of proof on some outside party (typically, an excluded rival). Economics dictates that the burden (and hence the proper presumption) should fall on the party in the most efficient position to gather the evidence. From

160. For an accessible technical explanation of how priority on the Internet works, see George Ou, Oct. 11, 2014, available at https://plus.google.com/+GeorgeOu/posts.

161. *See*, e.g., Peter Rysavy remarks, at 26:40, *available at* http://www.c-span.org/video/?322383-1/discussion-mobile-telephony-regulation.

this vantage point, an edge provider claiming that its packets were degraded (in an absolute sense) as a result of not taking a paid-priority offer, would be in the best position to prove it.

From this list of policy options, the FCC's *2010 OIO* elected option (3), by rejecting a blanket prohibition in favor of case-by-case treatment,[162] but declaring that paid prioritization deals "would raise significant cause for concern" and were "unlikely [to] satisfy the no-reasonable-discrimination standard."[163] This presumption, among other part of the *2010 OIO*, was appealed by Verizon. In *Verizon v. FCC*, the D.C. Circuit ruled that such a presumption effectively barred pay-for-priority deals and was tantamount to common carriage: "If the Commission will likely bar broadband providers from charging edge providers for using their service, thus forcing them to sell this service to all who ask at a price of $0, we see no room at all for 'individualized bargaining.'"[164]

Critically, the D.C. Circuit laid out a legal path for the FCC to regulate pay-for-priority deals without resort to common carriage:

> Given these principles, we concluded that the data roaming rule imposed no per se common carriage requirements because it left "substantial room for individualized bargaining and discrimination in terms." The rule "expressly permit[ted] providers to adapt roaming agreements to 'individualized circumstances without having to hold themselves out to serve all comers indiscriminately on the same or standardized terms.'" Id. That said, we cautioned that were the Commission to apply the "commercially reasonable" standard in a restrictive manner, essentially elevating it to the traditional common carrier "just and reasonable" standard, see 47 U.S.C. § 201(b), the rule might impose obligations that amounted to common carriage per se, a claim that could be brought in an "as applied" challenge.[165]

So long as broadband providers were free to bargain individually with edge providers, the court signaled, these arrangements could be regulated under the FCC's 706 authority along the lines of *Cellco*, a case distinguished by the D.C. Circuit from common carriage in 2012.[166]

How can such freedom be established? By flipping the presumption around, so that priority deals are reasonable until a complaining edge provider can prove otherwise. One can envision two types of complaints arising under this case-by-case framework: (1) an edge provider was denied a priority offering that was extended to its rival, or (2) an edge provider who declined priority from a broadband provider suffered an absolute degradation in its quality of service. After a complaining edge provider demonstrates discrimination or degraded service, the burden should shift back to the

---

162. *2010 Open Internet Order*, ¶76 n. 229 ("The Open Internet NPRM proposed a flat ban on discrimination and interpreted that requirement to prohibit broadband providers from "charg[ing] a content, application, or service provider for enhanced or prioritized access to the subscribers of the broadband Internet access service provider." Open Internet NPRM, 24 FCC Rcd at 13104–05, paras. 104, 106. In the context of a "no unreasonable discrimination" rule that leaves interpretation to a case-by-case process, we instead adopt the approach to pay for priority described in this paragraph.").

163. *2010 Open Internet Order*, ¶76.

164. Verizon v. FCC, 740 F.3d ___ (D.C. Cir. 2014) [[at 59-60]]

165. *Id.* at ___ (citing Cellco, 700 F.3d at 548–49).

166. Cellco Partnership v. FCC, 700 F.3d (D.C. Cir. 2012).

broadband provider, thereby sparing the edge provider of significant legal expense.

Quarantined from political forces, smart lawyers at the FCC set about drafting rules that would thread this needle—again, without resort to Title II reclassification. The agency released a Notice of Proposed Rulemaking (NPRM) in May 2014, a few months after the D.C. Circuit's ruling, which explained that pay-for-priority deals would be subjected to a "commercially reasonable" standard, and "prohibited under that rule if they harm Internet openness."[167] In other words, such deals were presumed to be commercially reasonable unless an edge provider could prove otherwise. The NPRM also proposed to adopt a rebuttable presumption that a broadband provider's exclusive pay-for-priority deal would be commercially unreasonable. From an economic perspective, those two strokes were brilliant, as they efficiently placed the burden on the appropriate party.

Not so, said John Oliver[168] and millions of angry letters ostensibly submitted to the FCC. (Given the esoteric language of those letters, which invoked Title II authority, a great many likely were form letters generated by public-interest groups clamoring for Title II-based solutions. In November 2014, President Obama called on the FCC to take up the "strongest possible rules to protect net neutrality."[169] Ever since that political groundswell, Wheeler backpedaled from the elegant, light-touch solution of the NPRM, and instead imposed a blanket ban on paid prioritization.[170]

By banning paid prioritization, the FCC violated the standards of cost-benefit analysis in its *2015 OIO* in several ways. First, the *2015 OIO* fails to provide an empirically supported finding of market failure. Second, the *2015 OIO* overstates the benefits of the ban. The *2015 OIO* fails to consider that the profitability of (and thus the incentive to engage in) discriminatory conduct vis-à-vis content providers depends on whether the Internet service provider (ISP) could generate higher profits from the promoted (affiliated) products to cover the lost margins from departing broadband customers. The anticompetitive behavior feared by the Commission has simply not come to pass, which explains why the *2015 OIO* is hard-pressed to cite any recent examples of consumer harm. A very limited number of service disruptions or degradations have actually occurred—among literally millions of opportunities for such behavior—and many of these have been dealt with expeditiously through private negotiations.[171]

Third, the *2015 OIO* understates the costs of the ban. The *2015 OIO* ignores or dismisses

---

167. See Protecting and Promoting the Open Internet, GN Docket No. 14-28, Notice of Proposed Rulemaking, 29 FCC Rcd ____ (2014) [¶97] (hereinafter *2014 Open Internet NPRM*).

168. *See, e.g.*, Ben Brody, *How John Oliver Transformed the Net Neutrality Debate Once and For All*, BLOOMBERG POLITICS, Feb. 26, 2015, *available at* http://www.bloomberg.com/politics/articles/2015-02-26/how-john-oliver-transformed-the-net-neutrality-debate-once-and-for-all.

169. Net Neutrality: President Obama's Plan for a Free and Open Internet, *available at* https://www.whitehouse.gov/net-neutrality.

170. *2015 OIO*, *supra*.

171. *See, e.g.*, Hal Singer, Mandatory Interconnection: Should the FCC Serve as Internet Traffic Cop?, PPI Policy Brief, May 2014, *available at* http://www.progressivepolicy.org/wp-content/uploads/2014/05/2014.05-Singer_Mandatory-Interconnection_Should-the-FCC-Serve-as-Internet-Traffic-Cop.pdf.

the economic evidence of the impact of Title II on investment in the late 1990s and early 2000s, and thereby dismisses the real threat to ISP investment. Rather than ground its findings on economic scholarship, the *2015 OIO* relies instead on the casual empiricism of an advocacy group that operates outside of the constraints of academic reputations, to reach the extraordinary conclusion that telco investment was "55 percent higher under the period of Title II's application" than in the later period.[172] These results hinge on which years are included in the Title II era: If one includes the years 1999 and 2000 as part of the pre-2005 period, then removal of Title II appears to have caused a decline in Bell investment.[173] But those early years are associated with the dot.com boom and long-haul fiber glut, and it is difficult to remove Bell investments in backbone infrastructure from the capex figures.

Fourth, the *2015 OIO* casually dismisses a less-restrictive alternative for handling paid prioritization disputes—namely, case-by-case enforcement—as being too "cumbersome"[174] to enforce, despite the fact that: (1) the *2015 OIO* itself embraces case-by-case review to address interconnection disputes[175] and other conduct such as zero-rating;[176] (2) the *2010 OIO* embraced case-by-case to address paid prioritization disputes; (3) the FCC's May 2014 Notice of Proposed Rulemaking would have permitted ISPs and content providers to engage in "individualized bargaining" subject to ex post review; and (4) the FCC relies upon case-by-case to adjudicate discrimination complaints against traditional video distributors. Why is this form of mild preference different from any other favoritism?

Recognizing this disparate treatment of paid prioritization and interconnection, the *2015 OIO* argues that case-by-case enforcement "is an appropriate vehicle for enforcement where disputes are primarily over commercial terms and that involve some very large corporations. . ."[177] But interconnection disputes can involve small content providers as well. And if the concern is an asymmetry in litigation resources, the case-by-case regime can level the playing field by shifting evidentiary burdens and providing interim relief. Interestingly, FCC staff economists opined in 2015 that leaving interconnection to market forces could raise or lower welfare, which supports

---

172. *2015 OIO*, ¶414 n. 1210 (citing Free Press Comments).

173. *See, e.g.*, Hal Singer, Three Ways The FCC's Open Internet Order Will Harm Innovation, PPI Policy Brief, May 2015, *available at* http://www.progressivepolicy.org/publications/policy-memo/three-ways-the-fccs-open-internet-order-will-harm-innovation/ (hereinafter *Three Ways*).

174. *2015 Open Internet Order*, ¶19.

175. *Id.* ¶29 ("As a result, commercial arrangements for the exchange of traffic with a broadband Internet access provider are within the scope of Title II, and the Commission will be available to hear disputes raised under sections 201 and 202 on a case-by-case basis: an appropriate vehicle for enforcement where disputes are primarily over commercial terms and that involve some very large corporations, including companies like transit providers and Content Delivery Networks (CDNs), that act on behalf of smaller edge providers.").

176. *Id.* ¶108 ("This no-unreasonable interference/disadvantage standard will operate on a case-by-case basis and is designed to evaluate other current or future broadband Internet access provider policies or practices—not covered by the bright-line rules— and prohibit those that harm the open Internet.").

177. *2015 Open Internet Order*, ¶29 ("As a result, commercial arrangements for the exchange of traffic with a broadband Internet access provider are within the scope of Title II, and the Commission will be available to hear disputes raised under sections 201 and 202 on a case-by-case basis: an appropriate vehicle for enforcement where disputes are primarily over commercial terms and that involve some very large corporations, including companies like transit providers and Content Delivery Networks (CDNs), that act on behalf of smaller edge providers.").

the case-by-case approach.[178] This same logic would apply equally to the case of paid prioritization. But it did not.

The *2015 OIO*'s embrace of a ban presumably pushed the FCC towards its dreaded reclassification decision. Logic dictates that a ban could not be sustained under section 706 of the Communications Act so long as case-by-case with a presumption against such deals could not be sustained under section 706, as indicated by *Verizon*. This dramatic policy reversal begs the question: What happened in the intervening five years that caused the Commission to lose confidence in case-by-case adjudication for paid prioritization? The *2015 OIO* does not give an answer.

It would seem that an overt and pronounced shift in regulatory policy would necessitate a clear and confident finding that such an alternative policy approach toward the Internet would produce better results—more innovation, more investment, and more consumer benefits. When viewed with an economic lens, the *2015 OIO* fails a basic cost-benefit analysis.

Although the *Order* was upheld in a 2-1 opinion by the D.C. Circuit in July 2016,[179] Judge Williams' dissent vindicated our concerns relating to the absence of serious economic analysis. The majority of three-judge panel refused to question the *OIO* on policy grounds or on the economics:

> Critically, we do not inquire as to whether the agency's decision is wise as a policy matter; indeed, we are forbidden from substituting our judgment for that of the agency." Nor do we inquire whether "some or many economists would disapprove of the [agency's] approach" because "we do not sit as a panel of referees on a professional economics journal, but as a panel of generalist judges obliged to defer to a reasonable judgment by an agency acting pursuant to congressionally delegated authority."[180]

With economic considerations off the table, the majority narrowly focused on whether the FCC had the legal authority to subject ISPs to common-carrier rules under *Brand X* and *Chevron*.

In another show of deference to the expert agency, the D.C. Circuit declined to criticize the FCC's findings on likely investment effects, asserting that "we ask not whether [the FCC's predictions] 'are correct or are the ones that we would the ones that we would reach on our own, but only whether they are reasonable.'"[181] The majority further noted that such "predictive judgments about areas that are within the agency's field of discretion and expertise are entitled to

---

178. D. Bring, et al., *Year in Economics at the FCC: 2014-15*, 47 REV. IND. ORG. 437-62, 404 (2015) ("Going forward, the Commission could choose to allow the interconnection market to work freely, with the possible benefit of lower broadband access rates for consumers, but also the possibility of anti-competitive interconnection rates charged by ISPs due to excessive market power.").

179. U.S. Telecom Ass'n. et al. v. FCC, No. 15-1063 (D.C. Cir. 2016).

180. *Id.* at 23 (citations omitted).

181. *Id.* at 44.

particularly deferential review, as long as they are reasonable."[182]

Judge Stephen Williams offered a blistering 69-page dissent, filled with citations to the economics literature, which might prove pivotal in any future challenge by the ISPs. The dissent forcefully explained why a blanket ban on paid prioritization cannot be legally sustained even under Title II, and why such a ban makes no economic sense, particularly when paid peering arrangements were treated by the Order under a "wait-and-see" approach:

> The Commission's disparate treatment of two types of prioritization [paid peering versus paid prioritization] that appear economically indistinguishable suggests either that it is ambivalent about the ban itself or that it has not considered the economics of the various relevant classes of transactions. Or perhaps the Commission is drawn to its present stance because it enables it to *revel in populist rhetorical flourishes* without a serious risk of disrupting the net.[183]

Economists recognize that some and perhaps most episodes of paid prioritization could improve the lots of ISPs (more revenues), edge providers with applications that need quality of service to function properly (more revenues), and broadband customers (greater quality of service). A ban denies those benefits. If the FCC is permitted to ignore the teachings of economics, then populism—the antithesis of economics—will fill the void.

Judge Williams lamented how the *OIO* gave three of its former chief economists "the silent treatment."[184] He noted that two of those (Michael Katz and Tim Brennan) offered less-restrictive alternatives to the ban on paid prioritization, but that the FCC casually dismissed those alternatives.[185] The FCC offered no serious explanations as to why case-by-case treatment (offered by Dr. Katz) or a requirement that ISPs meet minimum-quality standards (offered by Dr. Brennan) were inferior to the ban.

Any economist tasked with assessing whether a blanket ban on payments from edge providers to ISPs would appeal to the economics literature on two-sided markets in justifying their policy prescription. Yet as Judge Williams remarked, "[t]wo-sided markets are barely discussed at all, with the only mentions of any sort in the Order"[186] relegated to three footnotes. The Commission "nowhere develops any particular consequences from that classification or taps into the vast scholarly treatment of the subject."[187] Had it done so, it would have been forced to grapple with the fact that contributions from edge providers puts downward pressure on access prices for broadband users through what economists call the "topsy-turvy" or "seesaw" effect,[188] expanding

---

182. *Id.* (emphasis in original).
183. Dissent at 50 (emphasis added).
184. *Id.* at 43.
185. *Id.* at 39.
186. *Id.* at 20.
187. *Id.*
188. *See, e.g.*, E. Glen Weyl, The Price Theory of Two-Sided Markets, University of Chicago Working Paper, Dec. 2006, available at http://economics.uchicago.edu/pdf/Weyl_011507.pdf.

broadband penetration and deployment.

Finally, Judge Williams explained how the Commission can reach "arbitrary and capricious" decision when it eschews economic analysis:

> Given the Commission's assertions elsewhere that competition is limited, and its lack of economic analysis on either the forbearance issue or the Title II classification, the combined decisions to reclassify and forbear—and to assume sufficient competition as well as a lack of it—are arbitrary and capricious. The Commission acts like a bicyclist who rides now on the sidewalk, now the street, as personal convenience dictates.[189]

To foster confidence among ISPs to continue investing billions in broadband infrastructure,[190] the FCC needs to stay in its designated bike lane; swerving across lanes in response to political winds signals to investors that broadband infrastructure is not worthy of continued investment.

2. The 2015 *Muni-Broadband Order*

In March 2015, the FCC also granted the petition of the City of Chattanooga, Tennessee to preempt a state law that restricts municipal broadband (muni-broadband) deployment.[191] As was the case for the *2015 OIO*, the FCC's *Muni-Broadband Order* was preceded (and potentially caused) by a direct request from the White House.[192] Much of the debate concerning this action was whether the FCC has authority to preempt state laws that restrict or prohibit muni-broadband development. Some legal scholars argue that the only preemption authority at the FCC's disposal, which derives from section 253 of the 1996 Telecommunications Act, concerns preempting state laws that deter entry for private-sector network deployment.[193] As the Supreme Court noted in *Nixon v. Missouri*, the issue of preemption "does not turn on the merits of municipal telecommunications services."[194] To an economist, however, the merits should dictate FCC policies; authority to act is essential, but not something that lends itself to economic analysis. In response to the D.C. Circuit's ruling in *Verizon*, which provided a potentially alternative source of preemption authority in section 706, Chairman Wheeler stated that "I believe the FCC has the power—and I intend to exercise that power—to preempt state laws that ban competition from

---

189. Dissent at 66.

190. USTelecom, Broadband Investment, *available at* https://www.ustelecom.org/broadband-industry/broadband-industry-stats/investment.

191. In the Matter of City of Wilson, North Carolina, Petition for Preemption of North Carolina General Statute Sections 160A-340 et seq.; The Electric Power Board of Chattanooga, Tennessee, Petition for Preemption of a Portion of Tennessee Code Annotated Section 7-52-601, FCC 15-25, Memorandum Opinion and Order, 30 FCC Rcd 2408, (rel. March 12, 2015) (hereinafter *2015 Preemption Order*). As of the time of this writing, the *Preemption Order* is on appeal is on appeal before the Sixth Circuit as *The State of Tennessee et al. v. FCC & USA* (Case No. 14-3291).

192. Fact Sheet: Broadband That Works: Promoting Competition & Local Choice In Next-Generation Connectivity, The White House, Office of the Press Secretary, Jan. 13, 2015, *available at* http://tinyurl.com/ks2eyod.

193. Lawrence J. Spiwak, Why the FCC Can't Preempt States on Muni-Broadband, Bloomberg BNA, Feb. 2015, *available at* http://www.phoenix-center.org/oped/BloombergBNAMuniBroadbandPartII20February2015.pdf.

194. Nixon v. Missouri Municipal League, 541 U.S. 124 (2004).

community broadband."[195]

Setting aside the issue of authority, an economist can ask whether it makes sense for the FCC to preempt state laws that deter entry for muni-broadband projects in the first place. Put differently, could a state have *any* reasonable economic basis for discouraging its municipalities from entering the broadband business? If so, then FCC preemption seems to undercut those reasonable bases. And if economics dictates that the best policy is for the FCC to stay out of these affairs, the question of legal authority vanishes.

Economists have broadly recognized that broadband investment generates spillover effects into related markets that rely on broadband access.[196] These spillovers have been measured to be roughly equal in magnitude to the direct employment effects generated by broadband investment.[197] Yet Deignan (2014) shows that, in contrast to earlier findings of significant employment effects attributable to private broadband,[198] muni-broadband deployment has *no discernible impact* on private sector employment.[199] Using a difference-in-difference regression on panel data consisting of 23 years of observations from core-based statistical areas (CBSA), Deignan finds that after ridding the data of time-constant unobserved heterogeneity and temporal shocks via CBSA and yearly fixed effects, the private-sector employment effect from muni-broadband is not statistically significant.[200] To address this paradox, he posits that "physical capital is an important input into the production process, but it does not create economic growth by itself. Therefore, public investment plans that focus on end-states, such as attracting a certain business

---

195. Remarks of Tom Wheeler, before the National Cable & Telecommunications Association, Apr. 30, 2014, *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2014/db0430/DOC-26852A1.pdf.

196. *See, e.g.*, Justin Horner, Telework: Saving Gas and Reducing Traffic from the Comfort of your Home, Mobility Choice, *available at* http://www.mobilitychoice.org/MCtelecommuting.pdf ("By taking more than 4.7 million cars off the road every day, telecommuting already has a positive effect on congestion."); Ted Balaker, The Quiet Success: Telecommuting's Impact on Transportation and Beyond, Reason, Nov. 2005, *available at* http://reason.org/files/853263d6e320c39bfceddde642d1e16fe.pdf ("In fact, an analysis of Washington D.C. commuting by George Mason University's Laurie Schintler found that traffic delays would drop by 10 percent for every 3 percent of commuters who work at home."); Joseph Fuhr and Stephen Pociask, Broadband and Telecommuting: Helping the U.S. Environment and the Economy, Low Carbon Economy, 2011, 41-47, available at http://file.scirp.org/Html/4227.html ("Studies show that telecommuters reduce daily trips on days that they telecommute by up to 51% and automobile travel by up to 77%.").

197. Raul Katz & Stephan Suter, Estimating the Economic Impact of the Broadband Stimulus Plan, NTIA Papers, Feb. 2009, at 20, *available at* https://www.ntia.doc.gov/legacy/broadbandgrants/comments/1EA7.pdf. They estimate that this (net) spillover multiplier can range from 0.07 to 7.28 of the direct effects, with a mid-point estimate of 3.65. Expressed as a multiple of the total multiplier effect (direct, indirect, and induced effects combined), their midpoint estimate is slightly above one.

198. Raul Katz & Fernando Callorda, Assessment of the Economic Impact of the Repeal of the Tax Exemption on Telecommunication Investment in Minnesota (Feb. 2014), *available at* http://www.mncca.com/doc/minnesota-study-final-version.pdf; David Sosa and Marc Van Audenrode, Private Sector Investment and Employment Impacts of Reassigning Spectrum to Mobile Broadband in the United States, Analysis Group (August 2011), *available at* http://www.analysisgroup.com/uploadedFiles/News_and_Events/News/Sosa_Audenrode_SpectrumImpactStudy_Aug2011.pdf.

199. Brian Deignan, Community Broadband, Community Benefits? An Economic Analysis of Local Government Broadband Initiatives, Mercatus Graduate Policy Essay, Summer 2014, *available at* http://grad.mercatus.org/sites/default/files/MGPE_Deignan_0.pdf.

200. *Id.* at 32 (Table 5).

or building a fiber network, are focusing on the inputs of economic growth rather than a root cause, which could end up misallocating resources and encouraging rent-seeking."[201]

Why does muni-broadband investment not result in the customary lift in private-sector employment? Public investment in a service that is competitively provided could perversely discourage future private investment, which would have a depressing effect on private employment.[202] The reason is that publicly owned firms are not profit-maximizers, and thus can be expected to engage in predation.[203] From the perspective of an incumbent private ISP (or potential private entrant), the prospect of competing against a publicly-owned ISP could be sufficient to discourage the next round of investment. Ford (2016) notes that "[t]his deterrence effect is particularly pernicious at a time when private providers are undergoing widespread and costly upgrades to their networks. Paradoxically, the resulting lack of private supply may then be used to justify the municipal entry that caused the perceived lack of competition in the first place."[204] Accordingly, there can be legitimate economics bases for a state to limit how one city may seek to induce economic migration from another city. As Ford notes, "While it is easy to see a city's leadership wanting to advantage its city over others, it is not clear why the federal and state governments should be complicit in the act."[205] Although it might be welfare reducing on net in cities currently served by private ISPs, muni-broadband may still have a role to play in broadband deployment in markets where private entry is not profitable. Ford concludes that muni-broadband "may be a symptom of the lack of a coherent, economically-informed federal (and state) policy for broadband deployment and adoption in economically-marginal communities."[206]

In a complete disregard of these economic considerations, the FCC pressed forward in March 2015 by preempting certain laws in the states of Tennessee and North Carolina at the request of cities in those states. In the FCC's 2015 Preemption Order, the FCC claimed, *without citation to any evidence*, that "threat of entry or actual entry of a municipal provider spurs positive responses by the incumbent broadband provider [which] serves the goals of section 706."[207] While it is documented that incumbent ISPs react positively (by increasing speeds) to new entry by Google Fiber and other *private* competitors that take profits into consideration when setting prices, there is no evidence in the record to suggest the same reaction follows muni-broadband deployments. Based on the economics, we would expect (but are not aware of any evidence indicating) that ISPs would be inclined to reduce their investment when a muni-broadband entity enters their market. Indeed, the FCC acknowledged in its National Broadband Plan that

---

201. *Id.* at 36.

202. George Ford, The Impact of Government-Owned Broadband Networks on Private Investment and Consumer Welfare, State Government Leadership Foundation, Apr. 2016, *available at* http://sglf.org/wp-content/uploads/sites/2/2016/04/SGLF-Muni-Broadband-Paper.pdf.

203. *See, e.g.*, J. Gregory Sidak & David E.M. Sappington, *Are Public Enterprises the Only Credible Predators?*, 67 U. CHICAGO L. REV. 271-292 (2000).

204. Ford, *supra*, at 9.

205. *Id.* at 10.

206. *Id.* at 11.

207. *2015 Preemption Order*, ¶49.

"[m]unicipally financed service may discourage investment by private companies."[208]

As noted by Ford, the root cause of (any perceived) under-investment in broadband infrastructure is the existence of a positive externality (not captured by ISPs nor broadband consumers). ISPs will not deploy to neighborhoods where the private returns do not exceed the cost of capital, even when the social returns might exceed the cost of capital. More competition in the form of muni-broadband does not treat the problem of under-investment; instead, to increase the private returns, the solution should involve a subsidy to any willing provider, and incumbent providers likely have the lowest costs of serving unserved homes. To an economist, this is second nature. But when economics is not part of the discussion, such wisdom may go unnoticed.

3. The 2013 *Inmate Calling Service Order*

Due to its compensation structure, prisons have incentives to restrict competition in support of a monopoly concession for telephone service, a portion of which is remitted to the prison as a concession fee. This fee-based compensation is precisely what induced group purchasing organizations and local cable franchise authorities to restrict competition in the supply of medical devices[209] and cable television service,[210] respectively, despite the purported mandate of those "gatekeepers" to promote the welfare of their customers. This is not to say that consumer welfare does not enter their utility functions; instead, the revenue-sharing component of their compensation, which increases with prices, is in conflict with consumer welfare, which decreases as prices are increased.

To see why, consider the following simple example. Suppose the monopoly price for long-distance phone service is $5 per minute, the marginal cost of providing phone service is zero (so that revenues maximization and profit maximization are the same), and that an incumbent telephone provider offers the prison at a concession fee (often referred to as a "site commission") of 10 percent. In response to this offer, an entrant has little incentive to offer a lower price for its competing telephony service, holding the concession fee constant, as doing so would reduce the revenue share for the prison. The only remaining lever by which entrants may compete is through higher site commissions. The equilibrium outcome for this concession is the monopoly price for phone service with a site commission equal to 100 percent less X, where X is the residual share that will allow the provider to cover its fixed costs. Recognizing this distortion, New York, among other states,[211] barred kickbacks in 2008, which—as predicted by economics—resulted in newfound competition along the pricing dimension. Prior to ending its commission payments, New York's prison phone rates were $2.30 for a 15-minute call; after banning site commissions, New

---

208. *See, e.g.*, FCC, Connecting America: The National Broadband Plan, Mar. 16, 2010, at 153 n. 2, *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC- 296935A1.pdf.

209. Litan et al., *An Empirical Analysis of Aftermarket Transactions by Hospitals*, 28 J. CONTEMP. HEALTH L. & POL'Y. (2011).

210. Crandall et al., *Does Video Delivered Over a Telephone Network Require a Cable Franchise?*, 59 F.C.C. L. J. 251 (2007).

211. *See* Letter from Lee G. Petro, Counsel to Petitioners, to Marlene H. Dortch, Secretary, FCC, CC Docket No. 96- 128, Exh. A, at 16 (filed July 27, 2011).

York rates fell to $0.72 for a 15-minute call, a decline of 69 percent.[212] The Commission itself has previously recognized how competition for these kickbacks decreases incentives for cost-reduction and technological innovation.[213]

As an externality causes under-provision of broadband service, excessive fees for Inmate Calling Services (ICS) is caused by a distortion of a different sort—namely, site commissions. The clear implication from economic theory is to attack the source of the distortion. Ignoring this economic counsel, the FCC imposed rate regulations on ICS providers in its 2013 Inmate Calling Services Order (*2013 ICS Order*).[214] Indeed, the FCC recognized in the *Order* that New York has "already accomplished reforms, and thereby shown that rates can be reduced to reasonable, affordable levels,"[215] and noted that New York exhibits "one of the lowest" rates for a 15-minute collect call in the nation ($0.72).[216]

That the FCC may not have authority to ban site commissions is irrelevant. If the root of the problem is something outside of the FCC's discretion, then economics dictates that the FCC stands pat. The FCC could educate other states, similar to how the Federal Trade Commission files comments in state proceedings, explaining the need to end site commissions. But adding rate regulation as a bandage when the forces pushing toward higher rates are still active (in certain states) threatens the viability of the ICS industry. In particular, prisons will still be in position to extract the (now modest) surplus from site concessions, leaving ICS providers scraping for profits.

Through the lens of cost-benefit analysis, the incremental benefits from the FCC's intervention in states that have adopted a ban on site commissions is zero; to the extent the regulated rates generate *any* costs (fewer services, less innovation, or otherwise), the *2013 ICS Order* fails. Even in states that have yet to ban site commissions, the FCC's rate controls could lead to inefficient outcomes, and could perversely perpetuate the system of kickbacks.

Assuming counterfactually that some intervention beyond the banning of site commissions by states is warranted, the form of rate regulation in the *2013 ICS Order* also fails to heed the teachings of economics. The *Order* essentially imposed full-scale rate-of-return (ROR) regulation on ICS providers.[217] By eschewing price caps (or no intervention at all) in favor of ROR regulation, the FCC will be required to sort out a provider's legitimate costs from illegitimate costs, and to separate intrastate costs from interstate costs. The *ICS Order* commences a mandatory data collection effort on ICS rates, an admission that regulation precedes data that would inform the

---

212. Rates for Interstate Inmate Calling Services, Report and Order and Further Notice of Proposed Rulemaking, WC Dkt No. 12-375, Sept. 26, 2013, ¶ 38 (hereinafter *2013 ICS Order*), *available at* https://apps.fcc.gov/edocs_public/attachmatch/FCC-13-113A1.pdf.

213. *See, e.g.*, Implementation of the Pay Telephone Reclassification and Compensation Provisions of the Telecommunications Act of 1996, CC Docket No. 96-128, Order on Remand & Notice of Proposed Rulemaking, 17 FCC Rcd 3248, 3253, ¶ 12 (2002).

214. *2013 ICS Order*, ¶¶60, 71.

215. *Id.* ¶4; n. 15 (noting that call volume in New York increased by 36 percent following the decline in rates).

216. *Id.* ¶36.

217. *Id.* ¶73.

nature of the rates. As noted by Commissioner Pai in his dissent,[218] the ICS NPRM made no mention of rate-of-return regulation, which could represent a violation of the Administrative Procedures Act. As a result, the record does not contain any comments on the efficacy of a rate-of-return pricing regime, nor does it contain comments on how the requisite inputs (cost data) to implement such a regime could be acquired.[219]

The *ICS Order* also established an across-the-board safe harbor of 12 cents a minute and an across-the-board cap of 21 cents a minute for debit calls at all correctional institutions.[220] This uniform rate erroneously presumes that all facilities, regardless of size or type (prisons versus jails), face the same costs in providing ICS. But as Commissioner Pai pointed out, one ICS provider's cost study showed that it costs 12 cents more a minute to serve midsize jails than statewide prisons or the largest jails, while another provider's study shows that the average cost of serving jails is almost 20 percent higher than that of serving state prisons.[221] Costs may vary over different institution for several reasons, including (1) the majority of costs for ICS service are fixed, permitting larger facilities to achieve lower average costs;[222] (2) jails experience a significantly heavier turnover of inmate populations than do prisons, leading to higher set-up costs relating to debit account creation;[223] and (3) inmates in jails are more likely than inmates in prison to use free telephone services (such as attorney calls), leading to higher uncompensated costs.[224] By establishing a uniform rate, the *ICS Order* ignored these economic realities, potentially causing some ICS providers to operate below average costs.

The rate caps for debit and pre-paid calls, as well the FCC's restriction on ancillary fees, were challenged by prison phone companies and several states, which argued that the FCC had exceeded its statutory authority and failed to consider the carriers' costs. In March 2016, the D.C. Circuit put on hold the rate caps for (local and in-state) calling rates and fees for single-call services, but allowed the elimination of ancillary fees to take effect, and left in place interim rates for interstate calls.[225] As with the *OIO* and the *Muni-Broadband Order*, the *ICS Order* is yet another example in which the FCC failed to heed the lessons of economics.

B. A Dispassionate Expert Agency Becomes Politicized

The *2015 OIO* was the FCC's major turning point away from economic analysis toward "economics-free," politically driven decision-making. As noted above, at no point in the Order was reference made to any market failure to justify imposing regulations, nor did the FCC conduct a cost-benefit analysis of the impact of its regulation. The Order explained that in the history of the broadband industry, there were only a handful incidents of violations of network neutrality

218. *Id.* Pai Dissent at 113.
219. *Id.*
220. *Id.* ¶60.
221. *Id.* Pai Dissent at 116.
222. *Id.* Pai Dissent at 117 (citing Wood Study).
223. *Id.* Pai Dissent at 117 (citing Trathen Letter).
224. *Id.* Pai Dissent at 117 (citing Telmate Comments).
225. GlobalTel*Link v. FCC, No. 15-1461 (D.C. Cir. 2016).

principles.[226] The agency's actions were, to use their term, "prophylactic" in the sense that there was minimal evidence to suggest a current problem, but regulations were to be adopted to ensure no such problems occurred in the future. There was no evidence adduced to empirically demonstrate that such problems may in fact occur, other than references to what *might* happen based on unsupported claims of consumer groups. The expressed concerns, which echo those outlined by law professor Barbara van Schewick,[227] are concerns about the economics of broadband ISPs, but nowhere in the Order (nor in the van Schewick paper) can we find anything approaching an economic analysis of these hypotheses (or allegations).[228]

The FCC paid significant lip service to its economic traditions. For example, the 2014 Open Internet NPRM sought the "best strategy to implement data-driven decision-making."[229] Chairman Wheeler was also clear that the FCC would use "tools [given by Congress] in a fact-based, data-driven manner."[230] Far from being "fact-based," the *2015 OIO* appears to be based on speculation, fears, and scare-mongering by advocates, pundits, and law school professors. So much for economic principles.

The point is not whether the FCC made a good decision regarding net neutrality. (We happen think it was not a good thing based on our balancing of the costs and benefits of the rule.) Rather, the point is that the FCC abandoned economic analysis entirely in its decision process, relying instead on advocates and pundits to carry the day. Much has been written about the economics of net neutrality, both pro and con, but none of that analysis entered into the FCC's decision.

By the time the D.C. Circuit vacated the FCC's *2010 OIO* in January 2014, consumer advocacy groups were in an absolute frenzy. They added to their demands that net neutrality should include forbidding paid prioritization. The FCC quickly complied, again without any evidence that this would produce a desirable economic outcome. But the demands kept coming; the FCC had indicated in its second-round deliberations that it would justify regulation under Section 706 of the 1996 Act.[231] However, activists were not satisfied; they demanded that the FCC adopt Title II regulation, the very regulation imposed on the old monopoly Bell System from 1934. They mounted demonstrations at the FCC and even picketed the Chairman's driveway to press their point. The FCC received more than four million letters weighing in on net neutrality under Title II. President Barak Obama sent a clear message to Chairman Wheeler via YouTube that the

---

226. *2015 OIO*, ¶65 n. 69.

227. Barbara Van Schewick, *Towards an Economic Framework for Network Neutrality Regulation*, 5(2) J. TELECOM. & HIGH TECH. L. 329 (2007).

228. For a full critique of this order, see Gerald Faulhaber, *The Economics of Net Neutrality: Are 'Prophylactic' Remedies to Nonproblems Needed?*, REGULATION (Winter 2011-2012), at 18; Gerald Faulhaber & David Farber, *The Open Internet: A Customer-Centric Framework*, 4 INT'L J. OF COMM. 302 (2010).

229. *2014 Open Internet NPRM*, 29 FCC Rcd at 5619, ¶ 163.

230. Testimony of Thomas Wheeler, Before the Subcommittee on Communications and Technology Committee on Energy and Commerce, U.S. House of Representatives, "Oversight of the Federal Communications Commission," Dec. 12, 2013, *available at* https://apps.fcc.gov/edocs_public/attachmatch/DOC-324644A1.pdf.

231. *2014 Open Internet NPRM*, ¶ 4 ("Per the blueprint offered by the D.C. Circuit in its decision in *Verizon v. FCC*, the Commission proposes to rely on section 706 of the Telecommunications Act of 1996.").

"strongest possible regulation" was needed in the form of Title II.[232] The result: the new order imposed net neutrality via Title II.[233]

What was the role of economics, if any, in this outcome? According to one sympathetic source, this was the result of "one of the most sustained and strategic activist campaigns in recent memory," which successfully "framed net neutrality as a social justice issue, warning about how an Internet with fast lanes would harm the ability of activists to spread their message."[234] Financial analysts have suggested that Title II regulation will cause substantial reductions in investment in broadband, various Internet innovators have said that Title II will dry up innovation in the Internet.[235] It is highly unlikely that this is what most activists wanted, but unconstrained by solid facts and economic analysis, this is what they will get.

The FCC is now in charge of ISPs using the blunt tool of Title II. While the agency can claim they have no interest in regulating any part of the Internet except ISPs, the FCC has already expanded their purview to include interconnection agreements among Internet networks.[236] It has also taken on the job of monitoring privacy on the Internet.[237] The history of regulation suggests that regulation will inevitably expand, as this regulation already is, generally due to requests by interested parties who see expanded regulation as a way to further their organization's interest, be they advocates or corporations.

IV. The New Battleground for Economics-Free Regulation

The absence of economic analysis can be seen in several new FCC initiatives. A common theme that emerges is that the FCC appears to be acting in the private interest of certain entities, and that there is no serious empiricism that undergirds the FCC's proposals. As in the case of the *2015 OIO*, the FCC's set-top box (STB) campaign received a boost from the White House, when the Counsel of Economic Advisers' Jason Furman prepared a video and a blog, claiming the FCC's initiative would "allow for companies to create new, innovative, higher-quality, lower-cost products."[238] Rather than acting like a dispassionate, independent expert agency, the FCC appears to have become a political extension of the White House.

A. Unbundling Set-Top Boxes: The FCC's "Unlock the Box" Campaign

In the spring of 2016, the FCC announced its intention to unbundle set-top boxes (STBs)—

---

232. Edward Wyatt, *Obama Asks FCC to Adopt Tough Net Neutrality Rules*, NEW YORK TIMES, Nov. 10, 2015, *available at* http://www.nytimes.com/2014/11/11/technology/obama-net-neutrality-fcc.html?_r=0

233. *2015 OIO*, ¶ 5.

234. Jay Cassano, *The FCC Just Adopted Strong Net Neutrality Rules – Thanks to Activists*, IN THESE TIMES, Feb. 26, 2015, *available at* http://inthesetimes.com/article/17687/the-fcc-just-adopted-strong-net-neutrality-rulesthanks-to-activists.

235. Gerald Faulhaber, *What Hath the FCC Wrought?* REGULATION at 50 (2015).

236. *2015 OIO*, ¶ 31.

237. *2015 OIO*, ¶ 53.

238. Jason Furman & Jeffrey Zients, Thinking Outside the Cable Box: How More Competition Gets You a Better Deal, White House Blog, Apr. 15, 2016, *available at* https://www.whitehouse.gov/blog/2016/04/15/ending-rotary-rental-phones-thinking-outside-cable-box.

those anachronistic devices that are collecting dust in your cabinets connecting the outside cable to your TV—from cable television service. The FCC claims it is seeking to encourage entry in STBs, thereby reducing the rental prices and expanding consumer choice. The facts of the matter belie a different motivation.

First, the FCC's proposal is predicated on a fictitious factoid about the consumer costs to rent STBs. Second, programmers, pay-TV providers, privacy advocates and network security experts have erupted in opposition to the FCC's proposal having nothing to do with the STBs but rather the mandate to unbundle content and dis-intermediate the consumer relationship. Clearly the FCC's proceeding is about more than what a dwindling set of American consumers are paying to rent a STB.

1. Reliance on Fictitious Factoids

According to an April 2016 FCC "Fact Sheet," cable customers are experiencing runaway inflation for leasing STBs at a nominal clip of 185 percent since 1994.[239] The eye-popping figure comes from a study co-authored by Consumer Federation of America (CFA) and Public Knowledge (PK).[240] Did any FCC economists vet this claim?

The immediate challenge in constructing an inflation index for STBs is that nobody knows what cable subscribers are paying *on average* for the equipment. To this end, the CFA/PK study leans on a July 2015 query of the nation's top ten cable providers, conducted by Senators Markey and Blumenthal.[241] Question 2 of the Senators' query asked respondents "What is the monthly leasing cost of each set-top box that your company offers?" Question 3 asked "What was the total revenue your company earned from leasing set-top boxes to customers in fiscal year 2014?" The cable providers held this information close to the vest, and the answers they did provide do not permit one to compute an average price for STBs. Table 1 summarizes the data the Senators compiled.

TABLE 1: CURRENT PRICES FOR SET-TOP BOXES

Respondent	*Question 2*	*Question 3*
AT&T	$0 for the first STB; $8 for non-DVR STBs thereafter	"Commercially sensitive information"
Bright House	$1 limited service STB; $8 standard STB; $2 Digital adapter	"Not publicly available"
Cablevision	$6.95 (with some individualized discounts)	"Not publicly available"
Charter	$6.99 (not including promotional discounts)	"Confidential information"
Comcast	$1-$2.50 for standard-definition STBs; $2.20-$2.50 for high-definition STBs	"Not Publicly available"

239. FCC Chairman Proposal to Unlock the Set-Top Box: Creating Choice and Innovation, *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0127/DOC-337449A1.pdf.

240. PK and Mark Cooper Set-top Box Letter to FCC, Jan. 20, 2016, *available at* https://www.publicknowledge.org/documents/pk-and-mark-cooper-set-top-box-letter-to-fcc

241. Markey, Blumenthal Decry Lack of Choice, Competition in Pay-TV Video Box Marketplace, July 30, 2015, *available at* http://www.markey.senate.gov/news/press-releases/markey-blumenthal-decry-lack-of-choice-competition-in-pay-tv-video-box-marketplace.

Cox	$1.99 for Mini Box; $8.50 for all others (with some individualized discounts)	"Confidential and proprietary"
DIRECTV	$6 (not including fees for advanced services)	"Not publicly available"
DISH	$0 for the first STB; $7 thereafter (not including advanced service fees)	"Not publicly available"
Time Warner Cable	$7-$11.25 (with some individualized discounts)	"Confidential and proprietary"
Verizon	$11.99 for the first STB; $7.99 for the second and third; $6.99 for the fourth and fifth (not including DVR service)	"Competitively sensitive"

While the answers to Question 2 serve as a useful rate card, they would need to be married with data on how many customers take each flavor of STB to be helpful. How the Senators used these data to arrive at an average monthly price of $7.43 (or $231 per year based on an assumed average 2.6 boxes per home) is a mystery. Ford revisited the questionnaire, assigning weights to prices based on subscriber shares and noting that two large providers (AT&T and DISH) give away the first STB; he arrives at a weighted average monthly price of $5.15.[242]

Not to be deterred by this black-box method, the CFA/PK study compares the "average" STB rental price in 2015 per the Senators' letter ($7.43) to the "average" STB rental price in 1994 per an FCC study ($2.60). Ignoring any changes in quality of STBs over the intervening two decades, the CFA/PK study derives the 185 percent inflation figure (equal to $7.43/$2.60 – 100%).

Of course, the 2015 version of STBs include an array of new features (such as DVR, high-definition, two-way interactive support) not available in the plain-vanilla boxes of yesteryear (offering descrambling only). The fact that the modern STB can pause live TV and be effortlessly programmed to record (or even intuitively suggest) hours of programming, (remember what it used to be like to program a VCR to record even one show?) arguably represents *more* than a 185 percent improvement. In any case, to control for this difference in quality, as the Bureau of Labor Statistics does for its price indices,[243] the authors could have compared 1994 STB prices to the 2015 prices of *standard* STBs. But that apples-to-apples comparison would have yielded STB inflation of close to zero or even slightly negative (using Bright House's or Comcast's prices).

2. Unintended Consequence

The unbundling of STBs from cable television service is expected to upend the entire content industry and the relationship between multi-video programming distributors (MVPDs) and advertisers. Spot cable ads sold by pay-TV providers allow local businesses to show their television ads on national cable networks without having to buy airtime from those networks. The prices are based on time of day, the program on which your ad airs, size of the audience, and length of the ad. Implicit in the price charged and paid is the operator's *control over channel placement*

242. George Ford, *The Obama Administration is misleading consumers on set-top boxes*, THE HILL, Apr. 21, 2016, available at http://thehill.com/blogs/pundits-blog/technology/276969-the-obama-administration-is-misleading-consumers-on-set-top-box.

243. BLS, Hedonic Quality Adjustment to the CPI, *available at* http://www.bls.gov/cpi/cpihqaitem.htm.

and other delivery options, which could no longer be guaranteed under the new regime. For example, TiVo (or some other third-party box provider) would control how the channels are displayed to the customer, and it could insert additional advertisements that would vie for the viewers' attention. The problem here is that TiVo is not the party in contract with the advertiser.

What is the potential cost to pay TV providers of losing control over channel placement? According to Statista, local cable advertising revenue was approximately $5 billion in 2015.[244] Because the television advertising business is built on guaranteed placement in programs and narrow time windows on specific networks, as well as guaranteed impressions on delivery of audience levels in these purchased ad placements, the inability to offer such guarantees could significantly diminish the value of those ads.

As a second unintended consequence, the proposed rulemaking would also introduce new and serious privacy concerns. Under the current rule proposal, third party device manufactures would be able to gather a consumer's television viewing data and then use that data to sell targeted ads outside of the restrictions currently in place for MVPDs. In addition, features like voice recognition on third party STBs could capture distribute any spoken personal information at will.[245] Outside of the protected contract between the consumer and the MVPDs, consumers would have no expectation of privacy outside of their trust in the device manufactures, some of whom have a dicey track record of misusing personal information.[246]

Unbundling STBs would also jeopardize intellectual property licensing and disrupt the agreements that underpin the current television market. Under the current NPRM, device manufacturers would have neither incentive nor reason to comply with the terms of content distribution agreements painstakingly negotiated between MVPDs and content providers. Copyright owners will have no preventative measure or immediate legal recourse to prevent STB manufactures from pirating or modifying their copyrighted content.[247] Inserting an unwanted, uncontracted party into the delivery of copyrighted content needlessly lowers the security of that content opens it up to theft, misuse, and unintended distribution.

In addition, the loss of control over the promoting content and advertising will bring forth its own host of problems. The placement and organization of channels in STB features such as "Guide" would be stripped away. The ability to strategically place certain channels into "channel neighborhoods" and groups would interfere with channel navigation and the strategic placement

---

244. Statista, Local cable television advertising revenue in the United States from 2010 to 2019 (in billion U.S. dollars), *available at* http://www.statista.com/statistics/411648/local-cable-tv-advertising-revenue-us.

245. *See* Comments of the National Cable & Telecommunications Association, In the Matter of Expanding Consumers' Video Navigation Choices, MB Docket No. 16-42, CS Docket No. 97-80 (April 22, 2016) *at 83*, *available at* https://www.ncta.com/sites/prod/files/NCTA%20Comments%204-22-16%20FINAL.pdf

246. *Id.*

247. *See* Comments of Comcast Corporation and NBCUniversal Media, LLC, In the Matter of Expanding Consumers' Video Navigation Choices, MB Docket No. 16-42, CS Docket No. 97-80 (April 22, 2016), *available at* https://www.fcc.gov/ecfs/filing/60001655594/document/60001688881

of content.[248] As some content providers will often pay for strategic channel placement in the guide, the lack of this option may lead to higher overall prices. The rules would also remove the ability of a content provider to favor or disfavor advertisements and branding it deems appropriate for its content.[249] This would enable thematically inappropriate content to be displayed despite potential objections of the content provider, for example, life insurance ads appearing between content depicting a tragic loss of life.

This is yet another example of the FCC setting up rules for one set of market participants (MVPDs) but not their direct competitors (device makers), a form of protectionist regulation that we see again in the FCC's privacy rules and *Open Internet Order*.

B. Unbundling Fiber Connections from Business Broadband Service

In 2015, the FCC also embarked a multi-pronged regulatory agenda that seeks to manage the inner workings of one segment of the broadband Internet access market aimed at business customers ("business broadband market"). Although this regulated segment of the larger business broadband market is largely quarantined to relatively slow connections running over a fading technology (copper), the agency's recent efforts threaten to expand its foothold into a much larger and growing segment of the business broadband market, allowing the agency to regulate high-speed Ethernet services running over fiber lines.[250]

Regulatory intervention in competitive markets to push prices downward is likely to generate costs (dynamic inefficiency from less investment and innovation, allocative inefficiency from prices that do not cover marginal costs) in excess of benefits (static welfare gains from lower prices). And the business broadband market is competitive by most measures.

For example, monthly Ethernet prices (per unit) of a leading broadband business provider (Zayo) declined between seven and seventeen percent from December 2013 to June 2015.[251] Gartner Group expects the price of Ethernet access to fall by about nine percent per year from 2015 to 2018.[252]As of April 2016, nearly 30 competitive broadband providers had lit at least 1,000 buildings each with fiber. Collectively, these competitors serve over 267,000 buildings with fiber, laying over 650,000 route miles of fiber, or 2.42 route miles per building.[253] AT&T, Verizon, and CenturyLink, the three largest ILECs, collectively accounted for only 47 percent of Ethernet

---

248. Michael L. Katz, An Economic Assessment of the Commission's Proposed MVPD Access Device Regulation, MB Docket No. 16-42 (April 22, 2016), at 63, *available at* https://www.fcc.gov/ecfs/filing/60001657214/document/60001690487

249. *See* Comments of the National Cable & Telecommunications Association at 20.

250. Unlike TDM-based DS-1 and DS-3 service, Ethernet service is not tariffed.

251. Zayo FY2015 Supplemental Earnings Information, *available at* http://investors.zayo.com/~/media/Files/Z/Zayo-IR/earnings-releases/2015/zgh-fy2015q4-pricing-trends.pdf.

252. Danielle Young, U.S. Ethernet WAN Access Enables Digital Business Strategies, Gartner Group, Oct. 6, 2015 ("Compared to broadband, T1 or T3 access, fiber-based Ethernet access is more reliable and agile. Ethernet can support higher bandwidths at lower cost.").

253. Metro Fiber and On-Net Buildings List, Telecom Ramblings, *available at* http://www.telecomramblings.com/metro-fiber-provider-list/.

service revenue in the first half of 2013[254]—the future of the business broadband market—and for only 39 percent of U.S.-based, browser-based business Internet traffic as of September 2011.[255]

Those competitive outcomes were driven by robust competitive entry by cable business service providers and CLECs. Price controls aimed at both incumbents and entrants will discourage further competitive entry. The policies envisaged by the FCC will not only impose net costs, but are wholly unnecessary.

1. The Special Access NPRM

The segment of the business broadband market currently regulated by the FCC is referred to as "special access" services. As its name suggests, the FCC compels incumbent local exchange carriers (ILECs) to provide access at regulated rates to their copper-based lines used to serve businesses, including wholesale access to competitive providers, such as resellers,[256] mobile operators,[257] and middle-mile providers.[258] Competitive providers can exploit two regulated entry paths: (1) purchase an ILEC's DS-1 or DS-3 service for resale at a term- or volume-based discount from the tariffed retail rate; or (2) purchase an ILEC's unbundled network elements (for example, a copper loop) at regulated rates, which in turn can be combined and used to provide DS-1 or DS-3 service.[259] Like mandatory access or mandatory unbundling, special access allows competitive providers to obtain an ILEC's network elements or services on a wholesale basis, at terms and conditions that are superior to those that would be achieved under a voluntary access arrangement.

Over the last decade, since the FCC granted forbearance from regulating Ethernet services, special-access obligations have been limited to an ILEC's time-division multiplexing (TDM)-based services running on copper networks, which are typically used to provision DS-1 and DS-3 connections to business customers.[260] Relative to these TDM-based services running on copper networks, fiber-based connections give business customers greater flexibility, as they can be

---

254. Business Services Grab Spotlight, LightReading, *available at* http://www.lightreading.com/ethernet-ip/ethernet-services/business-services-grab-spotlight-at-esdn-/d/d-id/705860. This figure does not distinguish an ILEC's revenue from that of its out-of-region affiliates. On the other hand, some portion of the out-of-region revenue may be retail revenue for services using wholesale last-mile inputs, and some of those wholesale inputs may be purchased from one of these other ILECs.

255. Sean Buckley, *AT&T, Verizon carry most U.S. business traffic, but competitors gain ground*, FIERCE WIRELESS, Nov. 15, 2011 (citing comScore data), *available at* http://www.fiercetelecom.com/story/att-verizon-carry-most-us-business-traffic-competitors-gain-ground/2011-11-15.

256. Competitive local exchange carriers rely on special access to supply or supplement capacity for resale to their own business customers. For a review of the history of special access regulation, see Larry Downes, The Losing Case for Special Access Regulation, Georgetown Center for Business and Public Policy Paper, Nov. 2015, *available at* http://cbpp.georgetown.edu/sites/cbpp.georgetown.edu/files/Larry_Downes_PolicyPaper_SpecialAccess%2012.14.15.pdf.

257. Mobile operators rely on special access to provide backhaul for mobile voice and data traffic.

258. Middle-mile providers rely on special access to provide last-mile connections for their business customers.

259. FCC, Special Access Data Collection—Glossary of Terms, *available at* https://www.fcc.gov/general/special-access-data-collection-glossary-terms.

260. DS-1 and DS-3 connections offer users (in this case, employees of a firm) bandwidth of 1.5 Mbps and 45 Mbps, respectively.

configured to accommodate any desired bandwidth (typically over 10 Mbps). Because business customers increasingly demand greater speed[261] and flexibility,[262] fiber connections offering IP-based services are displacing TDM-based services.[263] One analyst conservatively projects that access providers could discontinue selling DS-1 and DS-3 lines in seven years at the current rate of substitution.[264] Recent regulatory developments threaten to expand the scope of special-access obligations considerably, including into areas of the business broadband market for which the FCC granted forbearance and other regulatory relief less than a decade ago.[265]

In December 2012, the FCC released an order calling for the mandatory collection of data from entities that provide or purchase special access services.[266] Rather than limit its inquiry to TDM-based services, however, the FCC sought information on "the full array of traditional special access services, including DS1s and DS3s, and packet-based dedicated services such as

---

261. For example, Comcast advertises that its "Business Ethernet Network Services can seamlessly network you with 10 Mbps, 100 Mbps, 1 Gbps, or 10 Gbps Ethernet User-to-Network Interfaces (UNI) that are Certified MEF Compliant." Comcast Business Ethernet Network Services, *available at* http://business.comcast.com/ethernet/products/network-services (accessed Dec. 30, 2015).

262. Danielle Young, U.S. Ethernet WAN Access Enables Digital Business Strategies, Gartner Group, Oct. 6, 2015 ("Compared to broadband, T1 or T3 access, fiber-based Ethernet access is more reliable and agile. Ethernet can support higher bandwidths at lower cost.") [hereafter *Gartner Group*].

263. Roger Entner, *Special access—How government preference for some may mean higher prices for all*, FIERCE WIRELESS, Oct. 21, 2015 ("Zayo's data shows a *massive shift to Ethernet connections*, which are both faster and cheaper than DS1/DS3, and where the marketplace is essentially even as new entrants and incumbents are building capacity at the same time.") (emphasis added), *available at* http://www.fiercewireless.com/story/entner-special-access-how-government-preference-some-may-mean-higher-prices/2015-10-21; Vertical Systems, Mid-Year 2015 U.S. Carrier Ethernet Leaderboard, Aug. 24, 2015 ("Primary drivers for growth [in the Ethernet segment] are *massive migration from TDM to Ethernet services*, robust demand for higher speed Ethernet private lines and rising requirements for connectivity to public and private Clouds.") (emphasis added), *available at* http://www.verticalsystems.com/vsglb/mid-year-2015-u-s-carrier-ethernet-leaderboard/. See also Report of Dennis Carlton, Mark Israel, Allan Shampine & Hal Sider, In the Matter of Investigation of Certain Price Cap Local Exchange Carrier Business Data Services Tariff Pricing Plans, WC Dkt. No. 15-247, Jan. 7, 2016, ¶ 19 (noting that between January 2013 and October 2015, AT&T's sales of TDM DS-1 services to non-affiliates declined rapidly).

264. Entner, *supra* ("If we take Zayo's data and project out the current decline rate then they will have stopped selling DS1s in three and a half years and DS3s in less than seven years. But these projections are deceiving, and likely too conservative, as declines are accelerating as the DS1/DS3 technology becomes increasingly obsolete.").

265. In 2003, the FCC relieved ILECs of most obligations to lease advanced fiber-to-the-home (FTTH) network facilities to competitors at a regulated, cost-based price. In the Matter of Review of the Section 251 Unbundling Obligations of Incumbent Local Exchange Carriers, CC Dkt. No. 01-338 (released Aug. 21, 2003). However, until December 2015, ILECs were still required to provide unbundled access to a voice grade equivalent channel and high capacity loops utilizing TDM technology, such as DS-1s and DS-3s. *Id.* at 11. In 2006, the FCC granted Verizon's petition for forbearance from Title II for certain business broadband services, including "packet-switched broadband services, such as Frame Relay and Asynchronous Transfer Mode Cell Relay (ATM) as well as non-time division multiplexing-based (non-TDM-based) optical networking, optical hubbing, and optical transmission services." Joint Statement of Chairman Kevin J. Martin and Commissioner Deborah Taylor Tate, Petition of the Verizon Telephone Companies for Forbearance under 47 U.S.C. § 160(c) from Title II and Computer Inquiry Rules with Respect to Their Broadband Services, WC Dkt. No. 04-440 (released Mar. 21, 2006). In 2007, the FCC granted similar relief to AT&T. In Petition of AT&T Inc. for Forbearance Under 47 U.S.C. § 160(c) from Title II and Computer Inquiry Rules with Respect to Its Broadband Services, Memorandum Opinion and Order, WC Dkt. No. 06-125 (released Oct. 12, 2007).

266. In the Matter of Special Access for Price Cap Local Exchange Carriers, WC Dkt. No. 05-25, Report and Order and Further Notice of Proposed Rulemaking, released Dec. 18, 2012.

Ethernet."[267] By including Ethernet in its investigation, the FCC blurred the traditional lines that segmented regulated from unregulated enterprise services, and thereby raised the specter of expanding price regulations to fiber-based connections. The FCC concurrently issued a *Further Notice of Proposed Rulemaking*, which sought comment on, among other things, the terms and conditions offered by ILECs for the sale of special access services.[268] In particular, the NPRM asked whether "is it *still* appropriate to grant Phase I and Phase II pricing flexibility and, if so, what factors should guide the level of relief granted."[269] Phase I flexibility permits price-cap LECs to lower their rates, while Phase II flexibility permits price-cap LECs to raise or lower their rates throughout an area. The NPRM was agnostic as to the ILEC's technology—copper versus fiber—used to establish a connection to a business.[270]

How would price regulation of Ethernet services manifest itself? Although the FCC's December 2012 NPRM was opaque, comments by Competitive Local Exchange Carriers (CLECs) in the proceeding make clear precisely what they are after. For example, a coalition of CLECs including Level 3 lamented that "[d]ue to the Commission's forbearance decisions, the major incumbent LECs are not subject to dominant carrier regulation in the provision of certain Ethernet-based services."[271] They urged the FCC to "apply price cap regulation to incumbent LECs' DSn-based dedicated services subject to Phase II pricing flexibility and to their packet-based dedicated services (i.e., by adding these services to the price cap basket for special access services)."[272] With regard to wholesale rates, they proposed "that each incumbent LEC provide dedicated services to wholesale customers at prices that are no higher than the incumbent LEC's retail price minus the costs that are 'avoided' when the services are offered at wholesale."[273] Similarly, Sprint asked the FCC to take action by "returning services subject to Phase II pricing flexibility to the price cap regime and taking steps necessary to include Ethernet services under the price cap regime."[274] With regard to pricing, Sprint proposed "using existing models that measure costs of service to set appropriate caps on prices."[275]

Another indication of price regulation of Ethernet services can be gleaned from the FCC's *Technology Transition Order*, which sought to extend the FCC's purview into an ILEC's fiber-based connections for business customers.[276] In particular, the FCC adopted a rule that required ILECs "that discontinue a TDM-based service to provide competitive carriers *reasonably comparable wholesale access* on reasonably comparable rates, terms, and conditions during the

---

267. *Id.* ¶17.
268. *Id.* ¶57.
269. *Id.* ¶85 (emphasis added).
270. *Id.* ¶15 n.38 ("We note that this definition [of a connection] does not depend on the medium used (e.g., whether it is fiber, copper, or coaxial cable), but instead on the capability of the facility.").
271. Comments of Birch, BT Americas, EarthLink and Level 3, In the Matter of Special Access Rates for Price Cap Local Exchange Carriers, WC Dkt. No 05-25 (filed Jan. 27, 2016), at 8.
272. *Id.* at 9.
273. *Id.*
274. Comments of Sprint Corporation, In the Matter of Special Access for Price Cap Local Exchange Carriers, WC Dkt. No. 05-25 (filed Jan. 27, 2016), at vi.
275. *Id.*
276. In the Matter of Technology Transitions Policies and Rules Governing Retirement Of Copper Loops by Incumbent Local Exchange Carriers, Report and Order, Order on Reconsideration, and Further Notice of Proposed Rulemaking, GN Dkt. No. 13-5, released Aug. 7, 2015 [hereafter *Tech Transitions Order*].

pendency of the special access proceeding."[277] If an ILEC seeks to replace its copper-based connections to a business, it now faces a fresh disincentive to invest in fiber, in that the wholesale-access requirements will extend to its Ethernet services provided over a fiber-based network. The FCC clarified that "the reasonably comparable wholesale access condition that we adopt applies to two categories of service: (1) special access services at DS-1 speed and above; and (2) commercial wholesale platform services such as AT&T's Local Service Complete and Verizon's Wholesale Advantage."[278] Put differently, the FCC plans to regulate both entry paths—special access *retail* services (acquired at a discount) and the *wholesale* inputs (or platforms) used to provide those services—for competitive providers.

For the first time, these wholesale-access requirements would implicate an ILEC's fiber connections. In his dissent, Commissioner Pai explained that "the Commission now leverages its discontinuance authority to get a foothold in the Ethernet market, exporting its legacy economic regulations into an all-IP world."[279] Commissioner O'Rielly similarly recognized the threat to fiber investment: "Providers that had voluntarily agreed to offer a commercial wholesale platform service to ease the transition for competitive carriers after the obligation to provide UNE-P was struck down by the Courts are now being forced to carry it forward into an IP world for a to-be-determined duration."[280]

In October 2015, the FCC launched an investigation of the non-price terms in ILECs' special-access contracts with competitors.[281] The Order sought to determine whether, for example, the use of percentage commitments, shortfall fees, overage penalties, and long-term commitments in certain tariffed pricing plans is just and reasonable or unreasonably discriminatory under various section of the Communications Act.[282] Because the FCC signaled a willingness to unwind contracts between ILECs and access seekers, potentially invading the purview of antitrust laws designed to address these very non-price terms, the investigation exposed special access providers to a new regulatory risk.

In April 2016, the FCC adopted the Tariff Investigation Order,[283] which declared unlawful certain terms and conditions in tariff pricing plans deemed to decrease competition.[284] It also adopted a *Further Notice of Proposed Rulemaking (FNPRM)* in which it proposed "a tailored set of rules to safeguard customers in non-competitive markets, including the use of price regulation and the prohibition of certain tying arrangements that harm competition."[285] If adopted, these price regulations would apply to all access technologies, including the facilities of new entrants in

277. *Id.* ¶101 (emphasis added).
278. *Id.* ¶132.
279. Dissenting Statement of Commissioner Ajit Pai, at 175.
280. Dissenting Statement of Commissioner Michael O'Rielly, at 177.
281. In the Matter of Investigation of Certain Price Cap Local Exchange Carrier Business Data Services Tariff Pricing Plans, Order Initiating Investigation and Designating Issues for Investigation, WC Dkt. No. 15-247 (released Oct. 16, 2015).
282. *Id.* ¶¶30-105.
283. In the Matter of Business Data Services in an Internet Protocol Environment, WC Dkt. No. 16-143 (released May 2, 2016).
284. *Id.* ¶11.
285. *Id.*

business broadband such as cable providers.[286] The *FNPRM* proposed to retain the existing price-cap regulation for TDM business data services in so-called non-competitive markets,[287] and to restore the use of a productivity-based X-factor and a corresponding inflation measure to inform the price-cap structure.[288] The *FNPRM* also proposed that rates for Ethernet business data services in so-called non-competitive markets be just and reasonable,[289] by anchoring those rates to regulated TDM service prices.[290] Finally, the *FNPRM* signaled that wholesale rates in excess of retail rates for business data services could be considered *per se* unreasonable.[291]

2. Unintended Consequences

Singer (2016) models the likely impact of the FCC's effort to preserve and extend its special access rules on broadband deployment by incumbent telcos.[292] The deployment impact of expanded special access rules can be measured as the difference between (1) how many buildings would have been lit with fiber by telcos in the absence of the rules and (2) how many buildings will be lit with fiber by telcos in the presence of the rules. With an estimate of the cost per building, the deployment impact can be converted into an investment impact. And with estimates of broadband-specific multipliers, the fiber-to-the-building network investment impact can be converted into job and output effects.

The model shows that a significant number of buildings in Charlotte would qualify for investment in the absence of any expanded special access regulation. The model then measures the extent to which regulation—including price-cap and/or wholesale requirements (that reduce expected revenues)—erodes the ILEC business case for fiber extension. Assuming this scenario reduces an ILEC's expected Ethernet revenue by 30 percent—the typical price effect associated with prior episodes of price-cap regulation[293] and unbundling[294]—the model predicts that an ILEC

---

286. *Id.* ¶344.
287. *Id.* ¶351.
288. *Id.* ¶356.
289. *Id.* ¶420.
290. *Id.* ¶422.
291. *Id.* ¶444.
292. Hal Singer, Assessing the Consequences of Additional FCC Regulation of Business Broadband: An Empirical Analysis (on behalf of USTelecom), April 2016, *available at* http://www.ei.com/wp-content/uploads/2016/04/assessingtheconsequences.pdf.
293. *See, e.g.*, OECD, Price Caps for Telecommunications: Policies and Experiences (1995), *available at* http://www.oecd.org/sti/ieconomy/1909801.pdf. *Id.* at 34 (showing BT's prices under various price cap systems fell by 26 percent between 1984 and 1992); *id.* at 35 (showing connection charges for BT fell by 32 percent from 1990-1994); *id.* at 36 (showing AT&T's private line price cap index decline by 21 percent from 1989 to 1991).
294. *See, e.g.*, Lisa Wood, William Zarakas, and David Sappington, Wholesale Pricing and Local Exchange Competition, Jan. 2004, at 3 n.7 ("Casual observation suggests the rate for wholesale services (i.e., resale) is roughly 20% less than retail services. (For example, the wholesale discount in New York is 19.1% with telephone company-provided operator services and 21.7% without these services.) Across all states (excluding Alaska), UNE-P prices averaged about $18 per line as of July of 2003, while revenue per access line per month averaged about $34. This $15 difference is approximately 44% of average revenue."). *See also* Kevin Hassett, Zoya Ivanova, Laurence J. Kotlikoff, Increased Investment, Lower Prices—the Fruits of Past and Future Telecom Competition, Sept. 2003, at 5 ("Unfortunately, only a few PUCs have, thus far, set their UNE-P rates close to what we measure to be their own state-specific TELRIC levels. Indeed, the average state-specific actual UNE-P rate and the average state-specific TELRIC UNE-P rate differ by 27.9 percent. Indeed, across all counties, the average broadband price under TELRIC pricing of

will increase business-fiber penetration in Charlotte from 10 to 14 percent (compared to 20 percent in the Baseline Case), an increase of only 265 lit buildings, 10.8 metro fiber route miles, and $21.4 million in investment. Thus, the special access obligations under this scenario result in a 55 percent reduction in an ILEC's CapEx relative to the baseline case without special access regulation.

It is reasonable to expect a scaling back of future CLEC fiber investment in the last mile as well. Not only would expected Ethernet revenue for CLECs decline, but CLECs could avail themselves of wholesale Ethernet options that would not otherwise exist; both forces would push CLECs away from facilities-based entry and towards resale. To make matters worse, the FCC extended the regulations to cable operators. By performing a similar analysis of lit building profitability and assuming similar cost structure for CLECs to that of the ILECs, price regulation should have a similar depressing investment effect on CLECs in last-mile facilities. The theoretical underpinnings of the ILEC model discussed earlier—that is, price regulations eroding the business case for ILEC fiber deployment—apply equally to cable business service providers and CLECs. That means the actions envisaged by the FCC will lead to less investment, deployment and competition.

CLECs' claims of higher costs of deployment (relative to ILECs) or insurmountable entry barriers (such as building access and rights of way) are not convincing. A recent financial assessment revealed that CLEC investment was rapid and profitable in high density markets, but lagged in areas that had low expected penetration.[295] Because ILECs account for less than half (roughly 40 percent) of lit buildings nationwide,[296] there are at least two or more effective players in the market with scale and cost structures on par with the ILECs. Moreover, due to towers, data centers, and long-haul facilities, several operators have comparable metro footprints in other geographic areas. Many CLECs have newer core fiber networks with greater fiber density and more availability for laterals; they also have flexibility to use contractors and lower cost resources for deployment in many cases.

CLECs' additional claim that expansion of special access rules for last-mile deployment would bolster their investments in metro rings is equally dubious; there has been a surge in investment in that segment of the industry over the past five years.[297] The artificial savings induced by regulatory advantages could just as likely be pocketed by the CLECs as they would be invested in other segments of their networks.

Finally, cable operators have indicated in filings with the Commission that mispriced resale opportunities for CLECs will undermine cable's incentive to invest their own facilities, further

---

UNE-P ends up almost 22.9 percent lower than the regulated monopoly price.").

295. Anna-Maria Kovacs, Business Broadband: Assessing the Case for Reregulation, March 2016 ("In other words, where costs are low, CLECs build their own networks. Where costs are high, they lease from ILECs at prices that do not reflect those high costs."), *available at* http://innovatewithus.org/wp-content/uploads/2016/03/Business-Broadband-Assessing-the-Case-for-Reregulation-Kovacs-3.14.16.pdf

296. Singer (2006), at 26, 32.

297. *See, e.g.*, Telecom Ramblings, Metro Fiber Miles and Lit Buildings by Select Providers (showing that Level 3, Lightower, and tw telecom increased their metro route miles by 29,600, 24,500, and 4,000 miles, respectively), *available at* http://www.telecomramblings.com/metro-fiber-provider-list.

undermining deployment.[298] Accordingly, the market-wide investment effect of Ethernet price regulation would be considerably higher than what Singer (2016) estimated for ILEC providers.

C. Un-Leveling the Playing Field: The FCC's Privacy Proposal

In April 2016, the FCC proposed to subject ISPs to a different and heightened level of privacy scrutiny relative to what the FTC previously asserted over ISPs.[299] The FCC's Privacy NPRM requires ISPs to seek affirmative opt-in consent from each customer for use of data for any purpose other than uses of information related to the provisioning of broadband service or marketing of "communications-related services."[300] The universe of data subject to the opt-in requirements include any and all consumer data—everything from passport numbers, to cookies, to network traffic statistics.[301] The FCC's opt-in model would require an ISP to inform consumers as to how it intends to use their data and then to obtain consent from users, even if the ISP never discloses the data to third-party advertisers and even though that exact data is being (or has been) used by other Internet businesses for marketing and advertising purposes. In contrast, for decades, the FTC has been able to reserve its opt-in requirements to limited situations involving "specific uses like making material retroactive changes to privacy representations, or collecting sensitive information, such as information about children, financial and health information, Social Security numbers, and precise geolocation data."[302] According to former FTC commissioner Josh Wright, the FCC has proposed "a rigid, one-size-fits-all regulatory approach, forgoing the individualized analyses that leave space for innovative, welfare-enhancing uses of customer information."[303] FTC Commissioner Maureen Ohlhausen also remarked that "opt in mandates unavoidably *reduce* consumer choice" by setting both a privacy baseline too high as well as preventing unanticipated beneficial uses of customer data.[304] And in comments filed in response to the NPRM, the FTC was quite critical of the FCC's proposal, warning that the asymmetric treatment of ISPs relative to other organizations that utilize consumer data was "not optimal" and providing a number of suggested improvements to the rules.[305]

The competitive implication is that edge providers, which already have developed highly

---

298. Reply Comments of NCTA, In the Matter of Special Access for Price Cap Local Exchange Carriers, WC Dkt. No. 05-25, RM-10593, Feb. 19, 2016, at 4 ("Given the substantial consumer benefits that have resulted from this facilities-based competition, the most important task for the Commission in this proceeding is to ensure that it preserves incentives for continuing and expanding facilities-based competitive entry and investment.").

299. *See* Notice of Proposed Rulemaking, WC Dkt. No. 16-106 (April 1, 2016).

300. *Id.* ¶¶ 127-133.

301. *Id.* ¶ 62.

302. See Dissenting Statement of Commissioner Michael O'Rielly.

303. Josh Wright, An Economic Analysis of the FCC's Proposed Regulation of Broadband Privacy, May, 27, 2016, at 6.

304. Maureen K. Ohlhausen, *Privacy Regulation in the Internet Ecosystem*, Remarks at the Free State Foundation's Eighth Annual Telecom Policy Conference (Mar 23, 2016), *available at* https://www.ftc.gov/system/files/documents/public_statements/941643/160323fsf1.pdf

305. Comment of the 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, WC Docket No. 16-106, FCC 16-39, May 27, 2016, *available at* https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection-federal-trade-commission-federal-communications-commission/160527fcccomment.pdf

successful businesses entirely in the model of tracking and monetizing user behavior pursuant to the FTC's consumer-welfare-oriented privacy rules, will be effectively immunized from competitive inroads by ISPs in online advertising markets. It follows that an incumbent provider of online ads, particularly one with market power such as Google,[306] that is shielded by government regulation will be less inclined to innovate, relative to a world in which ISPs were nipping at its heels. It also follows that ISPs will be reluctant to innovate, if not outright or severely restrained from innovating, in the highly concentrated online advertising marketplace, as doing so could run afoul of the FCC's new privacy rules. The NPRM restricts an ISP's ability to market to its own customers ("first-party advertising"), and forecloses an ISP's ability to engage with third parties for advertising opportunities ("third-party advertising") without first obtaining affirmative and expressed consumer opt-in. If the FCC's privacy NPRM is adopted in its current form, advertisers will never experience these competitive alternatives.

Moreover, former FTC chair Jon Leibovitz noted that the FCC's proposal prohibits the potential offering of discounted ISP services in exchange for greater access to consumer data.[307] In other words, the NPRM in its current form precludes the potential for cheaper broadband access to willing customers. As further explained by Professor Wright, an ISP's inability to monetize these data will place upward pressure on broadband access prices, as advertising revenue earned from the other side of the two-sided broadband platform would be perceived as a reduction in the marginal cost of serving broadband users.[308]

In summary, the FCC failed to consider (1) the transactions costs associated with an opt-in policy, (2) the potential revenue reductions that impact an ISP's ability to build broadband networks, and (3) the competitive impact of keeping ISPs from competing with edge providers for advertising dollars. The FCC offered no cost-benefit analysis of its proposed privacy rules. Lacking a statutory requirement to conduct a cost-benefit analysis like the FTC (for its general rulemaking), the FCC is evidently unaware of these legitimate economic issues until they are brought to light by an understandably concerned public.

D. Why Has the FCC Abandoned Economics Now, After Its Record of Great Success?

The record of economics at the FCC since 1980 is of great success; what possible reason might the FCC have for ignoring it for the last few years? The FCC has been silent on this issue, so we have no direct evidence. We can, however, hypothesize based on facts as to why this sudden turnabout.

---

306. Statista, Share of search queries handled by leading U.S. search engine providers as of April 2016 (showing Google's share consistently above 60 percent since April 2008), *available at* http://www.statista.com/statistics/267161/market-share-of-search-engines-in-the-united-states.

307. *FCC Overreach: Examining the Proposed Privacy Rules: Hearing Before the House Energy & Commerce Subcommittee on Communications and Technology*, 114th Cong. (2016) (statement of Jon Leibowitz, Co-Chairman, 21st Century Privacy Coalition), available at http://docs.house.gov/meetings/IF/IF16/20160614/105057/HHRG-114-IF16-Wstate-LeibowitzJ-20160614.pdf

308. Josh Wright, An Economic Analysis of the FCC's Proposed Regulation of Broadband Privacy, May, 27, 2016, at 6.

A consequence of the regulatory forbearance of the last decades is that the FCC's scope of authority has gradually lessened. The FCC simply has less to do than it did even a decade ago. Local wireline access to the telephone network was the last real area of regulatory activity. Everyone had a wireline telephone in their home, there was virtually no competition to the incumbent local exchange carrier, and none on the horizon. A major thrust of the 1996 Act was to press the FCC to remedy this problem, and the Commission spent a decade trying to introduce competition into local access, primarily by mandated local loop unbundling.

But a funny thing happened on the way to local access line competition—the market evolved. Americans began using cell phones as a substitute for wirelines, and the number of wireless-only homes began to rise quickly. Additionally, customers opted for VoIP phones rather than traditional wireline. The policy-driven option of providing wireline telephone service via competitive local exchange carriers simply died out, and customers opted to avoid wireline altogether using VoIP or wireless. Today, less than half of U.S. households have a copper wireline phone in their home, down from a high of 94 percent penetration ten years ago. The traditional wireline telephone is literally a dying business. The telephone companies realize this, and are desperately seeking strategies for exiting this business.

A problem confronts the FCC: Now that traditional regulated wireline access service is rapidly dying, what is left for the FCC to regulate? Its traditional role of regulating telephone is disappearing; aside for allocating spectrum, what is left for the FCC to regulate?

When the Civil Aeronautics Board (CAB) deregulated the airlines in the late 1970s, it did not take too long for the CAB to actually go out of business. When the Staggers Act deregulated railroads in 1980, it was not too long before the Interstate Commerce Commission likewise went out of business.

We thus hypothesize that the FCC, apparently concerned for its own survival, does not wish for the same fate to befall it. Searching for relevancy, the FCC has found the perfect foil. Net neutrality has given it a mandate to extend its regulation to the Internet, where it will no doubt have a full and busy life.

How does this hypothesis explain the FCC abandonment of economics? Now that the Commission has found a new mandate to regulate the Internet, it certainly does not want to minimize that mandate by re-adopting economic analysis, which would argue that virtually no regulation is needed for the Internet, which has progressed amazingly well without regulatory intervention. As more advocates and interest groups ask for more regulation to meet their organizational objectives, however, the FCC appears happy to oblige, in effect keeping itself in the regulatory business into the far indefinite future.

In light of the FCC's need to establish a new mandate, the imposition of Title II on the Internet makes much sense. Regulating the Internet will be a much larger job than regulating the telephone system, and unlikely to go away in the near future. It also makes sense for the FCC to forswear economic analysis, which would tell them they need not regulate the Internet given its stellar performance without any regulation at all. For the FCC, this is about survival. Acting in

rational self-interest, it will fight tooth and nail to preserve itself. It will surely be willing to listen to naïve, ill-informed advocate groups if their ideas align with its own survival. Of course, abandoning economics and welcoming advocates and pundits will have a high cost that the public will end up paying.

How can we test this hypothesis? If the hypothesis is false, we would expect that the FCC would apply economic analysis in determining whether or not to expand its regulatory writ, cutting back on regulation where empirical analysis failed to find market failure or benefits of regulation less than its empirically determined costs. If the FCC is truly not taking actions solely to expand its regulatory mandate, we would expect it to be quite cautious about its regulatory actions, cutting back where economic analysis suggests that regulation is not needed. On the other hand, if the FCC, having taken the aggressive regulatory step of imposing Title II regulation on a significant portion of the Internet, proceeds to expand its regulations to other transactions and players in the Internet industry, this would tend to confirm the hypothesis. Is this hypothesis correct? The authors certainly hope not. The data, however, suggests that this hypothesis needs to be seriously considered. Over the next few years, FCC actions will tell the tale.

V. Policy Implications

The past decade has seen a reversion back to the original regulatory paradigm at the FCC. The FCC has largely abandoned economics in policymaking. And old-fashioned Title II regulation, by which the monopoly Bell System was regulated, is once again being used to regulate both wireline and wireless Internet access. Never mind that Internet and wireless industries flourished beyond imagination without any regulation at all. This stunning and disturbing policy reversal gives rise to three important questions: (1) What are the implications for future policymaking?; (2) What are the implications for innovation in the sectors regulated by the FCC?; and (3) What can be done to avoid these outcomes and reinsert economics into the decision-making?

A. The Implications for Future Policymaking

It should be no surprise that when serious economic analysis is shown the backdoor, special interests and advocacy groups gain power. Without the economic requirement to examine the evidence, perform benefit-cost analysis, and justify regulation on the basis of market failure, political actors will seize control of the agenda. Even the White House intervened in the deliberations of a supposedly independent agency. The absence of dispassionate economic analysis in policymaking inevitably leads to politicization of the agency.

As explained in Part III, how the FCC reached this state is no great mystery. The scope of the FCC's regulatory writ in telecom threatens to shrink to zero, as the number of wired telephone access lines drops precipitously. In light of its shrinking mandate, the FCC needs to create a job for itself. It has reached for the biggest things it can find—the Internet access and wireless industries—and defines a new mandate of regulating these previously unregulated entities, with virtually no support from economics but lots of support from interest groups that stand to gain (or so they think) from FCC regulation, particularly of the ISPs.

Apparently, the firms that pressed for more regulation of the ISPs have not learned the basic lesson of regulation: Regulators will inexorably expand their control from their initial target (ISPs) to the next target (Netflix, mobile service providers), and eventually to the whole of the Internet. History provides the baleful evidence of this dynamic, including at FERC,[309] the FDA,[310] or even the FCC where regulation has expanded through merger review. Eventually, Google, a proponent of regulation, will find itself in the FCC's cross-hairs. Those who cannot remember the past are condemned to repeat it.[311]

B. The Implications for Innovation in Sectors Regulated by the FCC

Because the D.C. Circuit upheld the *2015 OIO*, we expect to see FCC regulation of the Internet/wireless just like the old Bell System. Early evidence suggests that this will suppress investment[312] and likely undermine innovation,[313] which is the lifeblood to both the Internet and the wireless industries. Imagining these industries being transformed by regulation into the old Bell System, with its plethora of orders, regulations, prohibitions and restrictions should strike fear into the hearts of those of us dependent upon either or both (likely everyone).

To see the threat concretely, consider the 2015 *Open Internet Order*, which threatens innovation in three distinct ways. *First*, by barring paid prioritization arrangements, the *2015 OIO* undermines innovation in the nascent market for real-time applications like telemedicine and HD voice. These markets are expected to develop into billion dollar industries in the coming years.[314] Although no application needs priority to function *per se*, there is a class of applications that need a certain level of quality of service that is not always consistently available on networks, especially across wireless networks that are subject to congestion. The ban on payments for priority arrangements could undermine certain collaborations among ISPs and websites/application providers, and thereby thwart a non-trivial portion of these applications from taking root, potentially costing the U.S. economy hundreds of millions of dollars annually.

Second, because sponsored-data plans by wireless carriers (including zero-rating plans) may run afoul of its "general conduct" standard, the *2015 OIO* could discourage innovative offerings that would subsidize Internet access for low income Americans. By discouraging ISPs and content providers from pursuing different ways to subsidize Internet access for consumers—another form of collaboration—the *2015 OIO* could deny the poorest Americans hundreds of

---

309. *See, e.g.*, Institute for Energy Research, FERC's Regulatory Mission Creep, Sept. 12, 2013, *available at* http://instituteforenergyresearch.org/analysis/fercs-regulatory-mission-creep/.

310. *See, e.g.*, Medical Device and Diagnostic Industry, FDA Mission Creep, Apr. 2, 2015, *available at* http://www.mddionline.com/blog/devicetalk/fda-mission-creep-don't-lease-your-510k-04-02-15 ("where 'just and reasonable' pricing was extended from interstate transmission to wellhead production in interstate commerce").

311. GEORGE SANTAYANA, I THE LIFE OF REASON (Charles Scribner's Sons 1905).

312. Hal Singer, ISP Capital Expenditures in the Title II Era (4Q Edition), Feb. 24, 2016, available at https://haljsinger.wordpress.com/2016/02/24/isp-capital-expenditures-in-the-title-ii-era-4q-edition/ (showing a decline in ISP capex of 0.4 percent in 2015, compared to an increase of 4.0 percent in 2014).

313. *Three Ways*, *supra*.

314. *See, e.g.*, The Virtual Reality Report: Forecast, market size, and the trends driving adoption, Business Insider, Apr. 29, 2015; IBIS, Telehealth Services in the U.S., Market Research Report.

millions in benefits annually. There are millions of Americans for whom (wireless) broadband is just out of reach and who would otherwise be eligible for a subsidy in the form of a sponsored-data plan.

Third, by reclassifying ISPs as telecommunications providers under Title II of the 1934 Communications Act, the order will likely slow the flow of investment dollars by ISPs, which will adversely affect innovation. Subjecting telecommunications companies to Title II in the early 2000s caused their capital expenditures to decline by between five and thirteen percent under conservative assumptions. Exposing ISPs to the same regulatory risk could undermine core investment to the same degree. Based on U.S. Telecom's estimated $76 billion in aggregate capex among U.S. ISPs in 2014, such a reduction would amount to between a $4 and $10 billion decline in investment at the core of the network.[315]

Unfortunately, the *2015 OIO* is not the only threat to innovation from economics-free policymaking. The FCC's Privacy NPRM also poses a threat to innovation, this time in online advertising markets and ad-supported services. This is a classic example of asymmetric regulation on only one set of market participants (ISPs), while specifically exempting or ignoring direct competitors (edge providers) in the market for online ads. As explained above, if adopted in its current form, the Privacy NPRM will put upward pressure on broadband access prices and immunize edge providers from competition in online advertising markets, while reducing consumer welfare in various ways, including preventing consumers from receiving promotional information about service bundles and price discounts for home security or energy efficiency services. This reduction in competition will likely lead to less innovation by incumbent content providers that dominate online advertising, and by discouraging ISPs to innovate, as doing so could run afoul of the FCC's new privacy rules.

C. Reinserting Economics into the Debate

Despite the gloomy prospects of a sustained run of populism portrayed here, we believe there are constructive ways to reinsert economic analysis into FCC decision-making. The waning influence of economic analysis seems to be connected to the politicization of the agency and its search for a new mandate. Based on that diagnosis, policymakers should shield the technocrats at the FCC from political pressure of the kind we observed in net neutrality and set-top-box proceedings. Assuming the D.C. Circuit does not vacate the *2015 OIO*, action to end the FCC's re-application of Title II regulation can only come from Congress. We offer three concrete suggestions for lawmakers.

First, Congress should clarify its intent in the 1996 Telecom Act to keep the Internet, including fixed and mobile broadband access, free from common-carrier regulation. Although the Act shields private mobile services from such rules through Section 332, there is sufficient ambiguity when it comes to Internet access services such that further clarity is needed. Would such explicit language barring application of Title II to fixed and mobile broadband access give ISPs an opportunity to hurt customers? The historical evidence supports the view than when unfettered,

315. *Three Ways*, *supra*.

ISPs generated little in the way of customer welfare loss, and certainly nothing that could not be handled by antitrust action by the Federal Trade Commission or the Justice Department.[316]

Second, Congress should give the FCC authority to regulate ISPs precisely along the lines dictated by the FCC's *2010 OIO*. This could be achieved by either expanding the agency's authority under section 706, or by issuing a new grant of authority. Recall the D.C. Circuit ruled that case-by-case adjudication of discrimination complaints against an ISP was tantamount to common carriage so long as paid prioritization was presumptively in violation of the FCC's rules. If the FCC had newfound authority to return to this presumption against paid prioritization without recourse to Title II, then this objection would be moot. Congress should further clarify that all forms of preferential treatment, including paid prioritization and zero-rating, should be subjected to case-by-case review (as opposed to a blanket ban), with challenges initially adjudicated by an FCC-appointed administrative law judge. While this presumption against preferential treatment is certainly not a perfect solution from an economic perspective—efficiency dictates the presumption be reversed, with the burden placed on disadvantaged rivals—it avoids the dangers of Title II regulation and appears to be a reasonable political compromise.

Third, Congress should require that the FCC perform rigorous cost-benefit analysis before promulgating any new rules. Executive Order 12866, which requires cost-benefit analysis for certain regulatory actions, does not apply to "independent *regulatory* agencies" (as opposed to independent agencies) such as the FCC.[317] For example, in the case of its set-top-box proposal, the FCC should be required to quantify, to the best degree possible, the costs associated with higher basic cable prices (caused by a loss in ancillary revenues), less content innovation (caused by removal and insertion of ads by independent STB makers), and threats to privacy (caused by the presentation of pirated content alongside legitimate content in search results), and to weigh those costs against the benefits of any purported reduction in STB rental fees. Recall that when the FCC issued its *2015 OIO*, it issued a separate statement noting that it had no obligation to perform a cost-benefit analysis. Imposing such a constraint on the FCC would ensure that economics plays a vital role in future FCC decision-making. There is no reason why the Department of Labor (an executive agency), the Environmental Protection Agency (an independent agency), or the Consumer Financial Protection Bureau (an independent regulatory agency) should be held to a rigorous cost-benefit analysis, while the FCC is free to embrace populism as its guiding principle. The tech industries under the FCC's domain are equally if not more important to the U.S. economy.

VI. Conclusions

The history of economics at the FCC is a long, gradual adoption of economics' basic tenets into FCC policymaking. In brief, economics teaches us that markets, absent failures, work well for consumers and the industry generally. Do not regulate unless a market failure forces the issue, and even with a market failure, only regulate when the facts dictate that the benefits to regulation exceed its costs. The adoption of economics at the FCC has been an unalloyed benefit for U.S.

316. *Id.* at 21.

317. Curtis Copeland, Economic Analysis and Independent Regulatory Agencies, Apr. 30, 2013, *available at* https://www.acus.gov/sites/default/files/documents/Copeland%20Final%20BCA%20Report%204-30-13.pdf.

consumers and the economy, both for the intended (short-run) impacts and the unintended and unanticipated (long-run) impacts.

Until the 1960s, the assumption had been that the FCC (and State commissions) needed to regulate every blessed service and product of the monopoly Bell System. Economists explained that terminal equipment (for example, telephones or private branch exchanges) exhibited no market failure and hence did not need to be regulated. The 1968 *Carterfone* decision permitted "any lawful device" to be connected to the telephone system, and ushered in an era of competitive supply of new and innovative terminal gear, just as the architects of *Carterfone* had intended. Similarly, MCI wished to offer long-distance telephone service, which had to interconnect with the Bell System's local network, and was approved by the FCC. The D.C. Circuit ruled in 1978 that indeed the Bell System had to interconnect, thereby bringing competition to long-distance service, along with lower prices for customers, just as the architects of the MCI case had intended.

More impactful were the *Computer Inquiry* decisions, in which the FCC established that "enhanced" services (primarily data) were not to be regulated, and the monopoly Bell System was permitted to enter these markets only under limited conditions, to ensure that it did not extend its monopoly power into the emerging computer and data communications markets. As the architects intended, these markets were insulated from potential entry by the Bell System, and remained completely unregulated. But what was not anticipated was the birth and development of the Internet in the 1980s and 1990s, possible because of the complete absence of any form of regulation. Clearly, the technology of the Internet was well within the capabilities of the Bell System, which owned probably the greatest industrial laboratory ever, in the form of Bell Laboratories. And yet, it was software entrepreneurs in garages in California who gave us the consumer and business Internet as we know it today, free of any FCC regulation. The forbearance of the FCC in this market made the Internet possible; with no FCC regulation, entrepreneurial talent and energy brought one of the greatest innovations of the last fifty years into full bloom without regulation, a deliberate strategy of the FCC.[318]

Equally important is the story of wireless telephony. The FCC had a long history of regulating wireless telephony, which they carried forward into the 1980s with the invention of cellular technology. Only two carriers were permitted in any city, the incumbent telephone firm and a competitor chosen by the FCC. The FCC discussion paper by Kwerel and Felker (1985) offered an economics perspective; auction off the spectrum and allow competition to rule the market. After Congressional approval, the first spectrum auction was held in 1994. Since then, the wireless industry has exploded, not only in the United States but around the world. In most OECD countries, there are more wireless phones than people, and the number of smartphones is fast approaching that number. Again, the explosive development of one of the greatest innovations of the past fifty years was enabled by the FCC's judicious use of minimal regulation, a major change from its previous tradition of regulation, brought about by economic thinking.
The engineers, entrepreneurs, and savvy business people who took risks to develop the Internet and wireless telephony deserve full credit for bringing these great economic innovations to the world today. But this could not have happened had the FCC not stepped back from its traditional

318. See Kennard, *supra.*

regulatory role and let these same people bring their revolution to fruition, and that would not have happened if economic thinking had not overcome the traditional regulatory thinking at the FCC. The FCC threatens this innovative arc as it lashes about for a new mandate. It is time for a rebirth of economics at the FCC. Based on our diagnosis of what ails the agency, Congress will have to right this ship.

The CHAIRMAN. As I mentioned in my opening statement, 94 percent of Americans prefer that all companies collecting data online follow the same consumer privacy rules, and so the question for any of you really is the FCC is, as I've said, nonetheless proposing to create a privacy regime for ISPs that's wholly distinct from the privacy rules governing all other companies on the Internet. So do any of you believe that consumers expect or want to have their online activity subjected to privacy rules that differ depending on the type of company collecting their information?

Mr. Ohm.

Mr. OHM. Absolutely. I think companies—consumers do expect that health care companies, for example, when interacting with a consumer on the Internet, are obligated to follow different rules. I think parents, and I'm a parent of young children, hope that websites are obligated to follow different rules when it comes to the sensitivity of information collected from children. I think the same is said when our children go to school and use Google Docs: we hope that the companies that are engaging in contracts with our school districts are obligated to follow special privacy rules. And as I said in my opening statement, I think ISPs belong in this group as well for the reasons that I've already laid out.

This speaks to something that we've heard in this debate, that the FCC rule will somehow confuse consumers. I think I give the American consumer a lot of credit, right? The notice and choice regime that the FTC use, which is exalted by almost everybody in this debate, is frankly a pretty complex system of reading privacy policy after privacy policy after privacy policy, trying to manipulate privacy settings. It's a really, really straightforward thing. In contrast to that, what the FCC proposes is a bright line opt-in consent for certain uses of information that are unexpected. Thanks.

The CHAIRMAN. Mr. Leibowitz.

Mr. LEIBOWITZ. Yes. Can I just respond to the last point? And I have the greatest respect for Professor Ohm. He worked for the FTC when I was there, he helped out with the Children's Online Privacy Protection Act, and he did a great job. But first of all, the FTC approach is not complicated, it is simple. It prohibits unfair or deceptive acts or practices, and if you—which means if you're a company and you don't honor your privacy commitment, the FTC will go after you. And the FTC has brought cases against Google, against Facebook, against Dish Network for not honoring its privacy commitments.

The second point I'd make—I just want to come back to the consumer confusion issue—90 percent of consumers, according to a study—this might have been what you cited, Mr. Chairman—by the Progressive Policy Institute, and I'll put this in the record after the hearing, believe that consumers should be under the same rules, and those same—and those same rules—and the reason isn't just because of consumer confusion, although that's a reason, the reason is because consumers benefit when there is competition between ISPs and other technology companies, and the FCC has an ability to take the FTC approach and turn it into rules. And that's why I think Mr. Garfield's idea of having them put out a second draft, because the draft that they've put out is full of—it makes—I believe they have policy choices or the Coalition believes, and it

is riddled with just mistakes, would be a good idea. You don't write a bill—you don't write a bill, introduce it one day and go to the floor the next day. It gets beveled by this committee, it gets tested and stress-tested, and that's what the FCC should do. This is a big part of industry. You want to get this right. They're not very close yet. They need to do a better job.

Mr. GARFIELD. Yes, I would add that the problem is not simply that it's distinct, and there's a problem there, as Mr. Leibowitz has pointed it, it's also that it ignores what is proven to be effective and workable over decades. And so replacing something with something that's likely to not be workable is making change for change's sake without any evidence that will improve the nature of things for consumers.

The CHAIRMAN. Mr. Leibowitz, has the FCC identified any specific harm or particular problems posed by ISPs that require a different privacy framework from what the FTC has applied to ISPs for years?

Mr. LEIBOWITZ. No, I don't believe it has, Mr. Chairman, and, indeed, you know, it would be easy for the FCC to take the FTC's approach embodied in the 2012 report, which, by the way, was criticized by some businesses and supported by a lot of consumer groups, and just focus on the really important thing, where consumers need protection, which is sensitive data.

The CHAIRMAN. Mr. Polka, while the FCC's proposals would place significant additional burdens on all broadband providers, as you pointed out, there are burdens that I think probably disproportionately affect smaller providers, like those serving much of South Dakota and rural America, who may have only hundreds or perhaps a few thousand broadband consumers.

Would you think the FCC's proposed regulations lead to more and better broadband service options for rural American households, or might they lead to less? And maybe you could elaborate a little bit, too, some of the burdens and how they do disproportionately affect providers in our part of the world.

Mr. POLKA. We believe it would lead to less with a chilling effect on investment and deployment, which is something none of us want. I mean, we're all here in Washington where we're encouraging greater deployment of broadband in smaller markets, rural areas. And the fact of the matter is you can look at our members and say that they're good actors. They've been member companies that have supported privacy and protected the privacy of their customers for decades.

And, in fact, our member companies have been part of the solution. We're the ones that have delivered broadband out to the smaller markets in rural areas where the large companies simply won't come. So we are part of that solution in reaching those hard-to-reach communities.

But what we're talking about here is really the challenge of balancing the need for privacy and privacy regulations with the ability to deliver important broadband services in rural markets in rural areas, in smaller markets, and in competitive areas, and that's where I think the balance is necessary with the FCC's rules.

When we look at changing the nature of what has been a consistent longstanding policy that is applied to consumers in the

broadband—Internet ecosystem for years and now changing that and changing their expectations, I think we're asking for trouble.

As your previous question alluded to, consumers expect privacy to apply across the board. If you create two different systems of privacy regulation, the consumer is going to think there is just one standard. They might be surprised on the other end, where there's a lesser standard, to realize that maybe their privacy isn't protected as maybe they assumed it would be when they're dealing with their ISP.

The CHAIRMAN. Thank you. My time has expired.

Senator Nelson.

Senator NELSON. Thank you, Mr. Chairman.

I have been struck listening to your testimony, and I thank you for it, I think it's very reasoned. What we have been going through over the past several years in trying to protect the privacy of American citizens and American persons from intrusion by the government, and, thus, we have set up this long case history that if you want to get something in somebody's house, you have to go to a judge, if you're the government, to get that. So, too, then in this new world of the Internet and telephone calls, we have said that if the government wants to get content of those communications, it has to go to a specially set-up court to handle intelligence matters, the FISA court.

Now, if that is true and now we move from government wanting to get your content over to corporations wanting to get your content, Professor Swire, is that the reason that half the people are now encrypting their communications?

Mr. SWIRE. Well, a big reason for the shift in encryption—and I was on the President's NSA Review Group and we worked a lot on those FISA kinds of things—a big reason is that American-based companies that operate overseas were facing a lot of loss of confidence overseas, folks didn't want to use U.S.-based services, and one of the ways that American-based tech companies have responded is by upping the level of encryption in a lot of different places.

Senator NELSON. But you said in your testimony, as I understood it——

Mr. SWIRE. Yes.

Senator NELSON.—that it is the consumers that are choosing to encrypt their communications.

Mr. SWIRE. It happens at the service level. So Gmail a few years ago wasn't encrypted, and now it is. Facebook a few years ago wasn't encrypted, and now it is. It's complicated for us, as individuals, to set up an encryption system, but it's by default, then it works, and what's happened for consumers is in the last few years the defaults have shifted a lot more toward encryption.

Senator NELSON. OK. Professor Ohm.

Mr. OHM. Yes, no, it's a great question and it's a really interesting one. I spent four years at the Justice Department as a computer crime prosecutor——

Senator NELSON. In essence, my question to you is——

Mr. OHM. Yes, yes.

Senator NELSON.—do we not have an obligation since we're protecting American citizens and American persons from the govern-

ment intrusion of their content, do we not have an obligation to protect from the commercial intrusion of their content?

Mr. OHM. Yes, it speaks to the Chairman's question about consumer expectations, right? Privacy is in shambles everywhere. The consumers and the citizens feel a lot of anxiety about this, and again I'm guessing that you hear this from your constituents. One measure of this is kind of clamor for encryption. And, by the way, some of that encryption may be, "Please encrypt your service so my ISP can't look over shoulder," which feeds the FCC's impetus, not cuts against it, right? And for these reasons—and, in fact, in some of my work, I've even documented how the line between these two systems of surveillance is actually quite blurry, and that a lot of government surveillance is sometimes abetted by massive data bases that are held by corporations.

But to get to your basic point, I couldn't agree more. Like if we want parity, we should have parity in all ways, including parity in the understanding that information, when it's sent through an intermediary that you have to use, you have no option not to use an ISP, will have a modicum of measured level of modest privacy support on top of that.

Mr. GARFIELD. What we're talking about is not a choice between protection or no protection. What we're talking about is the framework for that protection, and should it be grounded in well-established principles or reinvented whole cloth by the FCC?

Senator NELSON. Well, what we're talking about, when you look at it from the consumer's standpoint, is, should the consumer have the authority, by giving their consent or not, to control the invasion of their content? That's what we're talking about.

Mr. GARFIELD. Right. But opt-in and opt-out are both giving consumers choice and consent. What we're talking about is whether the agency gets to define which is——

Senator NELSON. But as a practical matter, that doesn't work that way.

Mr. OHM. Right. And if I may, Senator Nelson, it goes directly to your question, the Wiretap Act and FISA, which you referenced, they do have consent exceptions, but they're prior consent exception just like the FCC's opt-in rule. Imagine if it weren't so. Imagine if the baseline rule was all of our communications could be wiretapped unless we found some obscure government website and opted out. Right? So this goes exactly to the question that you were asking.

Mr. LEIBOWITZ. But the other thing I just wanted to mention is you are talking about sensitive data, and I think we all agree there should be protections for sensitive data. That was the FTC's approach, and we believe that could be the FCC's approach, but that is not the approach they have now, it's for all data. And keep in mind that right now over the top 10 ad sites and 70 percent ad-selling companies and 70 percent of online advertising revenue, much of it driven by rich data collection. It's not ISPs, it's everybody else in the Internet ecosystem. And so everyone should be under the same—every company should be under the same rules to protect the kind of data you want protected.

Senator NELSON. Well, I'll get into it later on. But thank you, Mr. Chairman.

But let me just tell you some country boy logic. One person's sensitive data is not another person's sensitive data. And so the question here to me is, Should the consumer have the choice of whether they want that data shared with the commercial sector?

The CHAIRMAN. Thank you, Senator Nelson.

Senator Blunt.

STATEMENT OF HON. ROY BLUNT,
U.S. SENATOR FROM MISSOURI

Senator BLUNT. And following up on that thought, Mr. Leibowitz, why would you have two different standards?

Mr. LEIBOWITZ. Well——

Senator BLUNT. Even if you do establish this data, sensitive data standard, why would you have one standard for one group of data providers and another standard for another group of data providers?

Mr. LEIBOWITZ. Well, I think you're absolutely right, and in the FTC's 2012 report, which was widely praised by consumer groups and had some praise and some criticism by businesses, we called for the same standards to be imposed on all large-platform providers, large-platform providers meaning both ISPs and other collectors of data, if those standards were to be applied at all, because we think that's what's critical, and technology neutrality, which I think is the point that you're going to.

Senator BLUNT. It seems to me, Mr. Garfield, that that's the fundamental debate we ought to be having here, is if we determine the issue of sensitive data, why would it only apply in one sector of the way we transmit this information? I mean, everything from my flashlight on my iPhone, I believe if there is a way to disconnect that from the location finder, I don't know what it is, so if I turn on that flashlight, somebody knows where I am, or at least it's been registered in a way that somebody could find out where I was, and that kind of data isn't even considered in this FCC discussion. Is that right?

Mr. GARFIELD. Correct. The FCC's proposed rules would only apply to companies that provide broadband internet access services and that are otherwise covered by the Open Internet Order and so would not apply to many of the companies that I represent.

Our advocacy—there are important differences between network operators and our companies, but our advocacy today is not suggesting that there shouldn't be protection, it is actually making the point that you're making, which is we have rules that have been working for the last—at least the last 3 decades, and rather than rewrite those rules with no foundation, no data to suggest that they would help consumers more, less rely on the rules that are well established that have been working that have been developed by the FTC.

Senator BLUNT. Mr. Polka, I believe your group of companies, the American Cable Association, is largely small and rural cable providers.

Mr. POLKA. Right.

Senator BLUNT. What would be discussed here? Does that impact the ability of your companies to provide the higher levels of Internet and communication that we think everybody needs to have?

Mr. POLKA. It would because it adds layers of complexity regarding privacy compliance. And in saying that, I'm not saying at all that our members are not strictly committed to protecting the privacy of their customers, it's just that these rules have a tradeoff effect in terms of providing broadband service in smaller markets.

When you're talking about small companies in southeast Missouri that I know of, such as BOYCOM Communications or Fidelity Communications or SEMO Communications, that have less than a couple of thousand subscribers, the FCC would be asking them to maintain a strict liability of ensuring privacy protection, which even the FTC has said is undoable. It's impossible to meet that standard, not to mention the revision of policies, the revision of consents that are asked of consumers who opted out to provide consent for commercial reasons, which they enjoy, now to an opt-in over non-sensitive data that would necessitate the addition of legal time, consultant time, man-hours. The FCC itself hasn't even determined the cost-benefit analysis of these rules on smaller operators, let alone larger ISPs, and I think it's a big issue in terms of——

Senator BLUNT. And in rural areas, it costs more to add customers——

Mr. POLKA. Absolutely.

Senator BLUNT.—that are further spaced apart, and you're saying this is just another reason not to make that additional investment to further expand your liability for very little impact on your company in a positive way? Is that——

Mr. POLKA. What this would cause is a shift of resources from investment and deployment into regulatory compliance for smaller businesses, and that means less deployment of broadband in smaller markets, rural areas, slower speeds, maybe less capacity. And in addition, because of the customer confusion, maybe customer anger over consents that they now have to give that they didn't have to give before, more consents, and in such a way, creating, you know, fatigue on the part of a consumer to say, "Well, I just give up. I don't even want the service any longer." We don't want to see that happening in our markets.

Senator BLUNT. Thank you.

The CHAIRMAN. Thank you, Senator Blunt.

Senator Schatz.

STATEMENT OF HON. BRIAN SCHATZ,
U.S. SENATOR FROM HAWAII

Senator SCHATZ. Thank you, Mr. Chairman.

Professor Ohm, it seems to me that one of the basic questions is, what is it that makes an ISP different from another Internet company? And the Title II part is easy, that was sort of pursuant to a legal strategy, the Open Internet Order. Set that aside for a moment. Your assertion, and I find it persuasive, is that ISPs occupy a unique place in the Internet ecosystem, and especially for people in rural areas and actually people in D.C. who have very few choices in terms of how they get on the Internet.

So I want you to talk a little bit about that, and then I want to give a chance for Mr. Leibowitz to respond, and then, additionally, I want you to respond to Professor Swire's data point regarding

encryption because it seems to me that this unique place in the ecosystem becomes somewhat less critically essential if you're talking about 70 percent encryption eventually and going up and up and up, which is to say, intuitively, I don't want to necessarily let an ISP have all of my data, and yet if all they know is that I went to Facebook, I went to the *Star-Advertiser* back home, I went to Gmail, that I do not find to be, to repeat Mr. Leibowitz's term, particularly personally sensitive.

So I want you to address, first of all, what is it that makes an ISP special? And how do you respond to the contention that increasing encryption may diminish that argument?

Mr. OHM. Absolutely, and thank you for the question. There are actually two ways to take on the first question. I think they're both consistent with one another. The first is simply the choice point again, that if you have an operating system, as Professor Swire suggested in his testimony, that is bucking, frankly, their industry norms and beginning to build a dossier on you as well. Well, first of all, it will have a press outcry when this is revealed; second, you have a choice to switch operating systems. It's even an easier choice if it's your browser that is doing the untoward spying, but when it's your Internet service provider, as you say, for rural Americans, for people who live on tribal lands, and for urban dwellers, that's not really a meaningful choice.

Second, it goes directly to Senator Blunt's——

Senator SCHATZ. So you're not necessarily talking about current bad behavior, but potential future bad behavior.

Mr. OHM. Potential future, yes.

Senator SCHATZ. Fairly.

Mr. OHM. I strongly believe that we don't need to wait for Pearl Harbors and data out—you know, dead bodies before we decide in anticipation to regulate something, right? And I think that's the decision that was made by this body in 1996.

Second, it goes to Senator Blunt's question about, Why have two standards? Right? As I said earlier, we have numerous privacy standards about online space itself. One reason why not to have two standards is because Congress hasn't gotten around to regulating——

Senator SCHATZ. Well, I'll just interject there and point out that if you ask a person whether they think that there should be one standard, the assumption of the respondent in the poll is that it would be one high standard——

Mr. OHM. Right.

Senator SCHATZ.—not one high standard and one low standard. So I don't find that particularly persuasive at all.

Mr. OHM. Yes, no, no. And if I can say one more thing agreeing with you on that, I have all the respect in the world for Professor Swire's work. You can read his report to say everybody is collecting information in ways that consumers don't know, don't expect, don't appreciate. Right? And so you could read it, and I think he's even said this, you can even read it as a full-throated defense for more privacy law in different sectors. Right?

Senator SCHATZ. Can I get you to respond to the encryption question and then kick it over to Mr. Leibowitz?

Mr. OHM. Absolutely, absolutely. So encryption is spreading, but as the report from Upturn, which has been widely cited, has said, 85 percent of the most widely used websites still don't encrypt. It's a sad fact in 2016.

The second thing is you were talking about a rather anodyne list of websites that you may not care if people know about, but it doesn't require much imagination to come up with the websites we might care more about. This person is visiting the NRA website reliably, this person is visiting Planned Parenthood, this person is visiting Black Lives Matter related websites. Right? There's a long tail of sensitivity, and sensitivity is often in the eye of the beholder.

Senator SCHATZ. OK. Go ahead.

Mr. LEIBOWITZ. So I will yield 30 seconds of my time to Professor Swire at the end so that he can talk about why——

Senator SCHATZ. That gives you 10 seconds.

[Laughter.]

Mr. LEIBOWITZ.—why ISPs are not unique. Then I will only yield 15 seconds of my time.

[Laughter.]

Mr. LEIBOWITZ. But I think the important answer—and I can see you're struggling with this, and I think all of us are struggling with this, is you can have similar—rules ought to be technology-neutral to the extent that they can, and if you're going to have a higher level of scrutiny—right?—for the things that consumers are concerned about and that they need to be protected about, then it should be the kind of sensitive data like health, like financial information, and like information that involves children—right?—which is what the FTC did in its role, which Senator Markey was very involved in, on the Children's Online Privacy and Protection Act.

And so all we are saying from a 21st Century Privacy Coalition approach, Privacy Coalition approach, is have the FCC's rules reflect more of the FTC's policies, which is enforcement plus restrictions on sensitive data and technology neutrality to the extent that you can do it, and then I'll turn it——

Senator SCHATZ. With the Chair's permission, we'll go to Professor Swire for just a couple of seconds.

Mr. SWIRE. I don't think I have really much to add.

Senator SCHATZ. OK. Thank you.

[Laughter.]

The CHAIRMAN. That is a first in front of this committee.

[Laughter.]

The CHAIRMAN. I have Senator Markey up next.

STATEMENT OF HON. EDWARD MARKEY,
U.S. SENATOR FROM MASSACHUSETTS

Senator MARKEY. Thank you, Mr. Chairman, very much. And I guess I would argue that where you go online all day long, and we've learned from recent surveys that adults and children are pretty much online all day long, but where you go online all day long is as sensitive as your health information. It is as sensitive. I mean, that's the profile of who you are as a human being in the United States in 2016. OK? If that information is not considered to be sensitive, then all of us have every bit of information being gathered about us, about what we're doing all day long, every sin-

gle day, as being out there and kind of being determined to be not sensitive, not sensitive, just kind of a product, just information that can be sold to people. And I think that's what the heart of this whole matter is all about.

So historically, the telephone company was viewed as a company that if you got on the phone and you called that department store or you called this or you called that place, we had laws that said the telephone company can't sell that information, where you went, who you are. Right? And beginning now, with this new FCC regulation that's been upheld, well, this broadband access is now considered to be a common carrier like a telephone company was, so now the FCC has the ability to regulate it.

And so as you're looking at the issue again and you're saying, OK, so what should the protections be? What should this common carrier be allowed to do with all of this information, which is essentially who we are as people? Now, what that company did that you called with your information, that's one issue, and we have to deal with that, but this is a separate issue. What does the telephone company do? Because essentially there's just a telephone company and a cable company. You don't have a choice. If you're going to be online, you have to pick one or the other, and in many places, you can just pick one.

So, Professor Ohm, can you talk a little bit about that transferring over of what the expectations are of ordinary Americans and the protection of this profile of who they are as a human being?

Mr. OHM. There are so many studies, including a particularly distressing one about a survey of American authors, that show that people hesitate to surf the Web in the way they would like to because they're worried about where that information may end up. Now, it may be that for some of the people, they're worried about the government, and for others, they're worried about corporations, but that chilling effect has been documented and it has a sort of deleterious effect and influence on expectations that you've been describing.

And the other thing I can tell you is I couldn't agree more with your assessment of all of this information being sensitive. I would be so bold as to say it probably could justify a ban on the sort of behavior we're talking about, but that's not what Congress did in 1996, and it's not what the FCC has done in its rule. It's a very measured rule, and I would love to say more about that, but it doesn't go to the extreme——

Senator MARKEY. Then say a little bit about that because what they're talking about is giving consumers more power to choose if their sensitive information can be used or shared by the ISPs, require the ISPs to adopt ADA security protections and notify consumers if a breach occurs, and promote transparency by mandating that the ISPs disclose what they collect about consumers. So what's wrong with that?

Mr. OHM. Absolutely. It's a modest set of requirements. It overlaps in significant part with the FTC report of 2012 that Mr. Leibowitz has talked about several times. As I hear Mr. Polka's testimony, and I'm very sympathetic to the idea that small businesses need to be accommodated by regulations, I heard him say repeatedly this his companies are responsibly already doing right by their

consumers when it comes to privacy and security. I'm guessing most of them are not selling data en masse to advertisers. This rule will have modest effect on them, and if there is something that's disproportionate, then the FCC ought to accommodate that.

Senator MARKEY. Yes. So this essentially says there's a bill of rights, that is, that each American knows what the rules are going in——

Mr. OHM. Yes.

Senator MARKEY.—rather than hoping that the FCC brings a case later on saying, "You know, that was really an unfair and deceptive practice."

Mr. OHM. Well, and I'm sorry to disagree just a little bit. I wish it were more of a bill of rights. This is merely an opportunity for a contractual, meaningful contractual, conversation with your ISP, but you're not afforded any rights, right? They can say in some meaningful ways, "The deal we're offering you is not a very good deal, but here's the deal we're offering."

Senator MARKEY. "Here's the deal."

Mr. OHM. Yes. But, again, I totally agree. It's a modest measured approach to privacy on this——

Senator MARKEY. There's kind of an argument here, well, this is kind of like a radical departure from what's been going on for the last 20 years, and what you're saying is it's not at all.

Mr. OHM. Yes.

Senator MARKEY. It's modest.

Mr. OHM. Absolutely.

Senator MARKEY. It's reasonable. It gives the consumer some rights, some sense of expectations about what they can expect, but it's in their relationship with the ISP, with the telephone company and cable company, and then they can decide what they want to do.

Mr. OHM. And, quite importantly, they're having a public NPRM. Congress is watching them very closely. They have strong incentives, the agency does, not to do something that's terribly radical, hence the modest approach.

Senator MARKEY. OK, great. Thank you.

Thank you, Mr. Chairman.

The CHAIRMAN. Mr. Leibowitz, did you want in on that?

Mr. Garfield?

Mr. GARFIELD. It is far from modest, and that's—moreover, if you are, as Professor Ohm said, going to regulate prospectively, I think it's incumbent upon you to bring forward evidence to suggest that the alternative approach that you are going to move forward with is one that will actually benefit consumers.

Mr. LEIBOWITZ. Yes.

Mr. GARFIELD. And in this NPRM, there is no zero data suggestive of that, and that's why we think it's critically important that there's a second NPRM that cabins—reacts to the responses that have been given thus far to date, and that gives consumers, as well as the public broadly, the opportunity to react to what's being proposed.

Mr. LEIBOWITZ. Yes, and I just want to say I do agree that they should put out a second draft of this proposal. But having said that, going back to your point about the constitutionality, Senator

Markey, when we were dealing with phones, it was a closed universe of information, as you know. Now we're dealing with data, and when you're dealing with data and so little of it is collected by ISPs and so much of it is collected by others, you have a problem under the Central Hudson Test because you are treating different entities that do the same thing differently. So that's the constitutional infirmity.

I won't dwell on it much longer, but it's something that I'm sure the FCC is thinking about, and the more that they make their rules technology-neutral, I think the higher the decibel level goes down, the more—and I think the less they have constitutional infirmities.

Senator MARKEY. Well, again, I would leave it up to the same lawyers at the FCC that were just upheld at the Circuit Court to determine what is, in fact, constitutional or not, and so far their record has been very good in terms of drawing those lines right where they can be upheld.

The CHAIRMAN. Thank you, Senator Markey.

Senator Moran.

STATEMENT OF HON. JERRY MORAN,
U.S. SENATOR FROM KANSAS

Senator MORAN. Thank you, Mr. Chairman.

Mr. Polka, I want to talk again about small business. In fact, I was reading the question as written in front of me, and it said we want to shield small business from the effects of harmful government regulations. The reality is, as I think about that statement, it's not the business we want to shield from harmful government regulation, it's the consequence that that harmful government regulation has to the consumer——

Mr. POLKA. Certainly.

Senator MORAN.—and that's particularly true for a state like Kansas. You visited with the Senator from Missouri, knew there are small companies. That is what dominates in our state. It is also a state in which we still struggle to have broadband services, a wide array, across our state, and some places have virtually none.

So one of the things that we've thought about doing is to consider giving legislative clarification that the FCC has exemption and waiver authority to deal with those kinds of issues. And my question is, Do you believe that to be necessary and helpful? And if so, I assume you and others would work with us to try to get it right?

Mr. POLKA. Without question. Companies like Eagle Communications out of Hays, Kansas, that are phenomenal providers of broadband service, have worked because our regulatory scheme has encouraged smaller businesses working with their consumers to flourish to provide these services in their marketplace. But under today's circumstances, it's becoming increasingly more difficult to do the same things.

We're here today talking about privacy where, with all due respect to my new friend, Professor Ohm, I wouldn't say it's an easy transition from one set of rules we're under to the proposed new rules, particularly for smaller providers. But that's one set of rules where we're talking about the need to shift resources from providing more services to meeting a regulatory compliance burden.

But at the same time we're sitting here, there are at least three other major rulemakings that are moving forward at the FCC that have the same impact, implementation of the Title II Order, the FCC's rulemaking on set-top box reform, and also the FCC's rulemaking on broadband business data, otherwise known as special access. Each of these in their own could have the kind of negative effects that we fear that our members would have to suffer by shifting resources from deployment to compliance and regulation.

Now, again, it's not a situation where our members are at all saying, "We're not up to doing our duty," but there is a balance that you have to reach when you talk about providing the service from a commercial perspective as well as protecting the consumers, and we're here to hopefully be part of the answer to that. But certainly any greater understanding by the FCC or requirement for the FCC to even look at the impact on smaller businesses would be enormously helpful to achieving everything we want to achieve, which is more deployment in smaller markets.

Senator MORAN. Sir, you make a good point. It never seems to me that it's one regulation or one event that causes small business to struggle and/or fail, it's the series of things, it's death by 1,000 cuts——

Mr. POLKA. That's correct.

Senator MORAN.—one more additional burden, and at some point in time the proverbial straw broke the camel's back.

Let me talk to Mr. Garfield about the cross-border data transfers, the EU Privacy Shield negotiations. I'm told it has just been announced that there is an agreement. This agreement is necessary, I suppose, because the EU and the U.S. have fundamental differences in the way we look at privacy, ours based upon our Constitution. It's my understanding that Americans officials advocated standards based upon the longstanding FTC guideline for privacy. What effect would occur in those negotiations, the resulting agreement, if we now have the FCC regulations, the new standard?

Mr. GARFIELD. Let me begin by thanking Congress for their role in getting the Privacy Shield passed. The passage of the Judicial Redress Act was critically important in getting that done. To answer your question, I think it would add a layer of confusion that would be unhelpful, and so the Privacy Shield recognizes that there is some distinction between the privacy regime in the U.S. and the security regime in the U.S. and Europe, but that they're essentially equivalent, and that's a recognition that the FTC's framework and principles are well established. It would be highly ironic and certainly unhelpful if, because of another regulatory agency, that agreement that has just been put in place would be called in question because we're now questioning whether the privacy regime in the U.S. is one that's workable.

Senator MORAN. Mr. Leibowitz, anything you want to add to that?

Mr. LEIBOWITZ. No. I absolutely agree that the Commerce Department and others are relying on the FTC approach, and if it's being questioned it's not strong enough, I think that it does not potentially bode well as the Privacy Shield goes through the European Union vote.

Mr. GARFIELD. If I may just add one other thing that makes it particularly relevant, is that though the Privacy Shield has been passed, our expectation is that it will continue to get challenged in Europe, including in the courts, and so the actions that are taken here will certainly have impact, not only in Europe, but in other markets around the world.

Senator MORAN. Thank you.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Moran.

Senator Klobuchar.

STATEMENT OF HON. AMY KLOBUCHAR,
U.S. SENATOR FROM MINNESOTA

Senator KLOBUCHAR. Thank you very much, Mr. Chairman. Thank you. I've been going back and forth to a FOIA hearing in Judiciary in the same area of information and issues, so I want to thank you for this important hearing and all of you for coming today.

I've been very involved in the broadband issue and, as has the Chairman especially in the rural areas, trying to get broadband out. We have many problems with a lot of our businesses, small businesses, farmers having to go to McDonald's parking lots to get any kind of access. So this privacy concern with broadband is incredibly important, but to some of them may be a luxury because they can't even get the access yet. But for most people who have access, this is an issue.

Senator Hoeven and I actually have worked hard to include the Driver Privacy Act, it's part of the FAST Act that was passed, to put in some privacy protections for data collected in cars. I'm not going to focus on that as much today.

I guess I would start with you, Mr. Leibowitz, about data breaches continuing to jeopardize the security of consumers' personal information. Data breaches can have, as we know, long-term financial consequences for consumers. How should we determine, Mr. Leibowitz, what kind of threat should lead to a consumer being notified of a data breach? We certainly had this issue with Target, my hometown company, and others. How do we ensure that consumers receive data breach information that's useful to them?

Mr. LEIBOWITZ. Well, I think that you have to have a harm trigger because—and, of course, in the example of Target and many of the 50 data breach cases that the FTC has brought, it involved harm. But the FCC's approach for data breach doesn't have a harm trigger at all. So our concern is under the approach they have, there would be massive overnotification to consumers, and consumers would become—would see so many notifications, and this is a problem in other disciplines as well that the FTC has commented on, that they won't look at the real notification that they need to because they'll be swamped with other notifications that don't really have meaning.

The other thing, less important because it's not consumer related, but important nevertheless, is that a sort of a no harm approach for the ISPs is in some contrast with the cybersecurity framework that NIST has prepared, which is really about protecting critical information.

Senator KLOBUCHAR. I see. I get it. And you also argue about the FCC proposal to prohibit Internet service providers from allowing companies to pay for extra privacy protections, and you state that many of us may decide that the price to pay to avoid personalized marketing is worthwhile. Of course, not all consumers have the financial means to make that decision. How would you answer the criticism that allowing consumers to pay for privacy will result in weaker privacy protections for low-income consumers?

Mr. LEIBOWITZ. Well, it's not certain. I mean, it's a reasonable question to be raised, but it's not certain what ISPs would do if this—and this is an actual prohibition, as Professor Ohm knows, if this—or this would be, if they were allowed discounts. It may just be collecting data and using it with your similarly branded affiliates.

These are not—ISPs are not data brokers. No one, I think, would ever propose something like that. And so I think the approach should be give consumers real informed notice so they know what they're being offered, if they're being offered a discount, and let them make the decision. And if I'm a family of four making $35,000 a year and living in Minnesota, and I want, you know—I want home security service or I want music streaming or I want energy efficiency, I should have the right or the ability to make that determination. The FCC's approach in that area, at least, seems to me very top-down and command-and-control.

Senator KLOBUCHAR. OK. Mr. Ohm, maybe you want to respond to that? And do you think FCC regulation of broadband privacy can complement the FTC's privacy work?

Mr. OHM. Yes, thank you for both those questions. Number one, when it comes to pay for privacy, as it's colloquially called, it does really give me a lot of pause, the idea that we've already talked a lot during this hearing about the paucity of choice that you have for a broadband provider, the idea that the only broadband service you could possibly have is one where you have to pay extra if you want the privacy version of it, is distressing to me and it's something that I hope the FCC will strongly consider dealing with.

It speaks to, I think, a broader undercurrent in this debate. I don't have a lot of time, so let me say it briefly, which is, a lot of the arguments and criticism has come from the perspective of the well-paid D.C. lawyer. For example, a statistic that's used often is the average American has 6.1 devices and three ISPs. Well, that may be true for the average American, but it's not true for a lot of Americans, and, in fact, a Pew study shows that a lot of Americans who have one device and one ISP are disproportionately younger, they're poorer, and they're also representative of racial and ethnic minority groups.

So as we think about the policy questions, I want to make sure we're thinking about all Americans, not just the well-to-do.

Second, if you could repeat the same question, if I have time to answer this.

Senator KLOBUCHAR. Go ahead, yes. It looks like Mr. Leibowitz might want to respond.

Mr. LEIBOWITZ. That might be a point of privilege. But, look, I spent—as you know, I spent most of my career in public service, and, look, don't take my word for the concerns about the FCC's

rule, just look at the FTC's unanimous comment where it says some of the choices made by the FCC are not optimal, and it cites 28 different instances where they're in disagreement, in polite, diplomatic language. Don't take my word for it, don't take an academic's word for it, we're all—I think we are all articulate witnesses, I may be the one exception, but, you know, look at what the FTC thinks they have done—thank you—they have done—the FTC has been the Nation's leading privacy agency for the last 30 years, they're informed, they know what they're talking about. I would listen to them as well and perhaps more than all of us together.

Mr. OHM. I think I'm out of time, but I invite the opportunity to talk about the FTC. I would love to do that.

Senator KLOBUCHAR. Well, I guess that's open for my colleagues to ask you, and maybe I'll follow up with some of this in writing, including with you, Mr. Garfield.

Mr. OHM. I appreciate it.

Senator KLOBUCHAR. So thank you very much.

Mr. OHM. Thank you.

The CHAIRMAN. Thank you, Senator Klobuchar.

Senator Daines.

STATEMENT OF HON. STEVE DAINES,
U.S. SENATOR FROM MONTANA

Senator DAINES. Thank you, Mr. Chairman.

Mr. Polka, I appreciate you highlighting in your testimony the burden that these privacy rules will place on small businesses. In a state like Montana, population and geography pose tremendous challenges for small ISPs. I think about Blackfoot Communications. They're the sole provider for Elliston, Montana, population 225. Do small carriers even have the technical capability to engage in the conduct the FCC is trying to prevent? And if they do, do they have any incentive to do so?

Mr. POLKA. Not really, Senator. The situation you talked about is typical, the company you referred to is typical. I've been inside the network operation centers, if you want to call them that, a small room in a head-end for a smaller provider, and they may have a board and a diagram up there, and that diagram has either a red signal or a green signal. Green means the network is operating. Red means there's a problem they have to fix. That's about the level that our members are looking at to make sure that they're able to provide broadband service to their customers.

The fact of the matter is, is that our members, the smaller providers, as I've said before, are in the business of trying to deliver that network service to their customer for the customer to then use as the customer sees fit. And typically our members have not been engaged, even under today's rules, in the kinds of information gathering that would require opt-in consent by a consumer.

Senator DAINES. Let me—I want to continue this discussion, and I think there has been talk about some of the inconsistency perhaps. I'm just—I'm concerned about as these regulatory bodies try to move at the speed of government when the world is moving the speed of business, how we're just always playing catch-up, and as

Wayne Gretzky famously said, "Skate to where the puck is headed, not where it's at."

When I send an e-mail, I add a Snapchat perhaps to a story, there are a number of entities collecting data. Snapchat is my browser, the ISP, they all have access.

Mr. Leibowitz, the question is, Do you think consumers expect that all entities involved in sending an e-mail, snapping a photo, are held to the same privacy standards, and does it make sense to treat any one of these actors different than the other?

Mr. LEIBOWITZ. No. I think from the perspective of the 21st Century Privacy Coalition, and I think from the perspective of the consumers themselves, you want the same rules applying across the board.

Senator DAINES. So I was struck—I think, Mr. Leibowitz, you made a comment I think in the back-and-forth with regard to online ad marketing. Ten companies hold 70 percent of the market share, none of them are ISPs.

Mr. LEIBOWITZ. That's correct.

Senator DAINES. In looking at the cross-context chart in Professor Swire's report, it's astonishing how much consumer information in the ad space, the social network space, have compared to the ISPs. I mean, look at our phones. And, by the way, if you want to see the behaviors, watch members during a hearing, where are they at? They're camped out and probably oftentimes on apps even more so than surfing. And I think when you look at where young people are headed now, where, you know, there's now more daily Snapchat users than Twitter users here, it just crossed in the last 30 days. I mean, just profound quick shifts here, where they're not out there surfing, they're camped out on apps oftentimes. I realize the FCC does not have jurisdiction over the entire Internet ecosystem, but does it make any sense to have very prescriptive rigid rules for ISPs and more flexible rules for edge providers and apps when ISPs only see a fraction of what the edge providers see?

Mr. LEIBOWITZ. No, it doesn't, and I agree with you entirely. And it goes to another point as well, which is the constitutional question, because when you are treating the same information differently, you—it raises concerns under the seminal Central Hudson Test, which is a Supreme Court case from 1980.

Senator DAINES. So, again, this is a concern where I think they're chasing the ISP issue right now, but look to where are consumers increasingly headed more so?

Mr. LEIBOWITZ. Yes, I agree with you, and the only other thing I would add is if you want to protect consumer privacy, which is critically important, and because the ISP—because the FCC invoked Title II, they took away jurisdiction from the FTC. The FTC has no jurisdiction over common carriers. ISPs are now designated common carriers and upheld under the D.C. Circuit decision, may be appealed. Because of that, they have to do a rule, but they should do an intelligent rule that is free from mistakes. We don't think their rule is balanced.

Senator DAINES. So let me get a point the FCC made, and this is my last question. In the FCC's Notice of Proposed Rulemaking, it offered a justification for its approach, and it stated, and I quote, ISPs are the most extensive conduits of consumer information and

have access to very sensitive and very personal information, end quote.

Professor Swire, does your research find this statement to be true?

Mr. SWIRE. It depends on the word "conduit." If they're the only conduits, then they'll be the most extensive conduit. So it might be a finely crafted sentence that you could technically say is true.

Senator DAINES. So are ISPs the most extensive conduits of consumer information with access to highly sensitive information?

Mr. SWIRE. They have access to location data, which is considered sensitive information, but overall, the point of our research is that there is a lot of other folks who also see it, and so—look, ISPs do see a bunch of information, so do a lot of the other companies you were talking about, and this committee and everyone has to figure out overall how we're going to handle that.

Senator DAINES. OK. Thank you.

The CHAIRMAN. Thank you, Senator Daines.

Senator Gardner.

STATEMENT OF HON. CORY GARDNER,
U.S. SENATOR FROM COLORADO

Senator GARDNER. Thank you, Mr. Chairman. And thank you to the witnesses for being here today.

Mr. Polka, why don't I start with you a little bit? This committee, if you look around at the composition of the Committee, it's a very rural committee, many members come from states that have the very, very sparse populated areas, at least in part, if not whole, of the state. I live in a little tiny town in the eastern plains, about 3,000 people. The nearest big city is a town that's 60 miles away, and it's 10,000 people, and then you have to go another 60 miles after that to get to a town that may be 100,000 people. So these areas are very, very spread out, very rural. And, if Senator Klobuchar was here, I would say that having a McDonald's is a luxury.

[Laughter.]

Senator GARDNER. That's something that many of our small towns, we don't have. But we talk about a lot of regulations here in Washington that have opt-outs and provisions, and then to say, you know what, we're going to pass this rule, but we understand there are small businesses that would be overly adversely impacted by this, and so we're going to give an opt-out for this. Look at the CFPB, I know there are conversations about whether community banks and credit unions ought to be tailored, regulations tailored, under CFPB, the regulations under Dodd-Frank, to address smaller banks and financial services. Here we are talking about, well, a new rule that would opt out for smaller providers, but it just seems like that opt-out never happens, the regulations pile on, and then you end up with higher costs and less service in many areas. So how many of these companies you're talking about have full-time regulatory compliance officers?

Mr. POLKA. Very few. As I said in my statement, most of our member companies have about 10 employees. Maybe they have one or one and a half technical people that are out actually putting service into the home or maybe climbing a pole or doing a service

call or maybe fine-tuning things in the head-end, so to speak, where all the signals come in. But it's very, very difficult. That being said, our members, over the last couple of decades, have worked to comply with Section 631, the Cable Privacy Rule, Section 222, for phone service of the CPNI rules, and they have worked to develop policies that have been open and that have been—provided disclosure to their customers. And they have worked to protect the sensitive data of their customers, whether, as Mr. Leibowitz was saying, whether it's banking information, school information, health care information, et cetera.

But to do what the FCC is requiring, would require under this rule, would go to a level of complexity that when we talk about shifting resources would be enormous in terms of legal time to revise policies, to revise notices, to send out notices that consumers aren't expecting, to comply with higher standards of data security, which, as the FTC has said, is impossible to meet.

Senator GARDNER. So take away time from expansion, investment, upgrades——

Mr. POLKA. Without question, and without even an idea yet from the FCC how much time, man-hours, paperwork, or cost it would take. And, frankly, from a small business perspective, I would have hoped that the FCC might have done a little bit of homework in that area before implementing these rules or moving forward because, in our view, there is none, and it's not my word, it's the Small Business Administration's Office of Advocacy that said these would be overly burdensome for smaller ISPs. That's a fear and a threat that our members face.

Senator GARDNER. Thanks. Mr. Garfield, you spent a good deal of your testimony arguing about the FCC's approach to privacy being both inconsistent with consumer expectations and inconsistent with existing privacy regulations at the Federal Trade Commission, FTC. I've supported numerous pro-privacy initiatives during my time in Congress, and I want to ensure my constituents that—I want to ensure their private information is protected. But do you believe the inconsistencies you mentioned could actually undermine consumer privacy protections? And if so, how might negative consumer reaction to concerns with their personal privacy impact your member companies' businesses?

Mr. GARFIELD. I made the point—thank you for the question, Senator Gardner—in my testimony that privacy and security are first principles for our companies, and so any rule or regulation that undermines our ability to advance both is highly problematic.

Connecting your second to your first, I think this proceeding of the FCC is actually an opportunity, it's an opportunity to do something that is not a framework based on exemptions for small business or exemptions generally, but to build on things that have worked in protecting consumer privacy and to call on the well-established history that has been built by the FTC. And so it's incredibly important, and I want to ensure, and I think our companies in general want to ensure, that we don't miss the opportunity to protect consumer privacy in a way that's workable.

Senator GARDNER. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Gardner.

Senator Heller.

STATEMENT OF HON. DEAN HELLER,
U.S. SENATOR FROM NEVADA

Senator HELLER. Mr. Chairman, thank you.

And I'm another rural advocate over here, so I'll probably go down the same line as the previous comments. But, frankly, anything that you really want to ask has probably been discussed here at one point or another. And I want to thank all of our witnesses for being here, for your comments, for your insight, because it has been very helpful.

You know, we do have an answer to all this, and we actually saw this in this committee. We've already passed out the FCC Reform Act. The purpose of the FCC Reform Act was to make sure that the Commission, the FCC Commission, operates in a transparent and effective manner. And this FCC Act had two important principles, and one was that there would be a conducted cost-benefit analysis, and we've discussed that, and the Commission should demonstrate a market failure. And in neither of these cases can I tell by any discussion that we've had today that either of these have been the case.

Even the Chairman, even the Chairman of the FCC, last year came in front of this committee and stated that consumers deserve a uniform expectation of privacy, in front of this committee he said that, and that the FCC will not be regulating the edge providers differently from Internet service providers. This is what the FCC Chairman said. So in March, there was a vote, a 3-to-2 vote, to switch that position. I'm wondering if there is anybody here on this committee, Mr. Leibowitz, perhaps yourself, that would tell me what has happened, what's the change of heart, for the FCC to say exactly the opposite of what they're doing today a year ago?

Now, it doesn't surprise me that the FCC changes or, for that matter, Mr. Wheeler changes his mind because he changes his mind on everything. I mean, we have seen this consistently over and over and over again, that the Chairman of this particular Commission changes his mind. Can someone tell me, what has changed in the last year when this Chairman came, the FCC Chairman, Wheeler, came in front of this committee and said that the consumers deserve a uniform expectation of privacy? Why has all this changed?

Mr. LEIBOWITZ. Well, I mean, I can't tell you why. I'm a former FTC Chairman, I'm not an FCC Commissioner——

Senator HELLER. But he was agreeing with you. He was agreeing with you a year ago.

Mr. LEIBOWITZ. And in fairness to Chairman Wheeler, you know, they could modify their rule to make it look more like the FTC approach, that would be what the 21st Century Privacy Coalition would encourage them to do. But I do hear you.

And I guess I would make one other point for those who have watched the FTC. At the FTC, we didn't always have unanimity, but we always strived to have it, and on important votes involving rulemakings, involving major cases, we would typically end up with unanimity or a supermajority, bipartisan supermajority, and I think that makes rules much more enduring.

Senator HELLER. I agree.

Mr. LEIBOWITZ. And you know this, when you have a bipartisan coalition, and all of you on this panel sitting here have put them together, it makes the rules more legitimate, it makes your bills more legitimate, your legislation, and it helps them last longer.

Senator HELLER. Well, I would just argue that transparency is the difference between the FTC and the FCC. That is the difference, is the transparency, and I think that's the reason, the most important reason, why we pushed this FCC Reform Act, Process Reform Act, is to make sure that we get this transparency into the FCC.

I just want to touch on one other point before my time runs out, and that is the Small Business Administration, their advocacy office came out with concerns about this particular proposal, and, Mr. Polka, I would like you to respond, but they were knowing that the costs would include consulting fees, attorneys fees, hiring and training in-house privacy personnel, consumer notification costs, and probably opportunity costs, if you want to do the economics behind that also. These are the costs. So the question is, one, there hasn't been a cost-benefits analysis because the FCC does not believe in a cost-benefits analysis. But, two, do you believe that the FCC has considered the economic harm to small providers like those in my state of Nevada?

Mr. POLKA. And not to mention what you said, but also risk management assessments, which smaller providers don't do today, which would take significant legal and consultant times as well as other items.

I do not believe that the specific concerns of smaller companies and the economic impact has been considered. And we were very pleased to see that the SBA noted that from the Office of Advocacy. Frankly, the rules relating to the FCC and implementation of a rulemaking does require it, to do at least some sort of analysis about the impact on smaller businesses. The FCC in its rulemaking has asked questions about the impact on smaller business, but to our knowledge, no type of cost-benefit analysis, and as I said before, no estimation of man-hours, paperwork hours, et cetera. And when we look at other opportunity costs that would be shifted, one of the things that the FCC would require us to a point would be a senior privacy officer, senior data security officer, someone who has that title within our company. As I said before, when you have 10 or fewer employees, I think we're going to be looking around the office to say, "Do you want it?" because it's going to be hard to fill.

Mr. SWIRE. Can I just very briefly, as a point of information, under HIPAA, there's a whole part of the HIPAA rule called "scalability," which is the Mayo Clinic has to be super strict and big, but two doctors in a little office have a different level of privacy and cybersecurity, and it may be, and I don't think this was fully fleshed out in the FCC's proposed rule, that there could be some learning done from 15 years of experience there and how to handle small versus large organizations.

Mr. POLKA. And that's consistent with what the FTC has done over the years as well, to take size into account.

Senator HELLER. Thank you. I want to thank all of the witnesses.

Mr. Chairman, thank you.

The CHAIRMAN. Thank you, Senator Heller.
Senator Blumenthal.

STATEMENT OF HON. RICHARD BLUMENTHAL,
U.S. SENATOR FROM CONNECTICUT

Senator BLUMENTHAL. Thanks, Mr. Chairman.

Mr. Leibowitz, you mentioned in your testimony how ISPs want to enter the online advertising market, not really a new phenomenon. You and I probably both recall, although you may not because it may have been just a minor blip on your radar, but in 2008, Charter Communications announced plans to launch a pilot program in Newtown, Connecticut, that would target advertising to subscribers based on their Internet traffic through an invasive technique called deep-packet inspection.

I was Attorney General at the time. I sent a letter to Charter with serious concerns about the legal and privacy implications, and fortunately in this case, Charter reversed course, abandoned the plan, and there was also, parenthetically I should mention, a public outcry from consumers, consumer advocates, and lawmakers, including none other than Congressman Edward Markey, of the great state of Massachusetts, although he may not remember it either because it was probably a minor blip on his radar of many accomplishments in the area of consumer protection.

So what I guess I'm asking you and Mr. Ohm is, is what the ISPs are trying to do today different from what they were trying to do in 2008? In what ways has the technology for tracking a subscriber's browsing history and deep-packet inspection, DPI, grown more sophisticated and potentially more intrusive on consumer privacy since 2008 when Charter tried to do it in Connecticut?

Mr. OHM. So I welcome the question. It actually wasn't a blip on my radar. I wrote I think the only extended *Law Review* article analyzing the work of your office and others, in which I came down pretty hard on ISPs for the moves that they were making.

The Swire report does establish that deep-packet inspection will not work to the same level of efficacy as it has in the past with encrypted communications, but it's again important to underscore that there are a lot of communications that remain unencrypted, and deep-packet inspection remains a problem that looms large on the horizon, and, in fact, today there is a rich ecosystem of vendors just chomping at the bit to sell deep-packet inspection systems to ISPs.

The second thing I would say is there was a time in the not so distant past, in fact, 2008, 2009, where because of the relative processing speeds of computers versus the speeds of these fiber optic cables, it was really hard to do surveillance on everybody all at once. That curve has completely flipped, and today a company that really does want to compile a dossier about every single one of their customers, even one with relatively constrained resources, like a small ISP, can absolutely off the shelf buy the technology to do something like that.

Senator BLUMENTHAL. Mr. Leibowitz, I would ask you the same question also about perhaps the ISPs you represent voluntarily committing to refrain from using deep-packet inspection.

Mr. LEIBOWITZ. So I think that's a great question, and we had discussions, and you were involved, and very successful, I think, enforcement advocacy and jawboning, and the DPI never got off the ground.

We addressed this issue in our 2012 FTC Privacy Report because we thought that all large-platform providers, that is, companies that collect data, including ISPs, shouldn't collect sensitive information, so health information, financial information, kids' information, and we talked about deep-packet inspection. And, in fact, in 2012, ISPs—two ISPs committed, and I'll get you this, and it is in our Privacy Report, two ISPs committed to not using deep-packet inspection without advanced opt-in consent. So we thought that was really important to follow up on your work, and because we had concerns about it at the FTC, as a commission.

So I think I would have to go back to our companies, but I think if what's on the table is a prohibition on deep-packet inspection, that would be great to know from the FCC, and a second iteration of their draft, if they went in that direction, I think would be tremendously meaningful.

Senator BLUMENTHAL. Thank you. Well, I would very much like to work with you on this issue, and as the FTC Chairman, you certainly helped to make the FTC the primary champion of privacy in the Federal Government, so I think your leadership then and now is profoundly important. Thank you.

Mr. GARFIELD. If I may just add, your question speaks to the importance of having an approach and a paradigm that has some flexibility to it, which is part of the problem with the FCC's approach, is that it's very much based on rigid, mandatory, mechanical approach, unlike the approach the FTC has taken and that NIST is taking when it relates to privacy and cybersecurity.

Mr. SWIRE. Very briefly on deep-packet inspection. So three points. This first is, as Professor Ohm said, there is some good news here, which is where there is encryption, DPI doesn't work. So some things have gotten better in life, even though we don't usually notice that.

The second point is that deep-packet inspection has been used by ISPs for cybersecurity purposes to look for signatures in malware, and so whatever your views are on marketing, there are some cybersecurity things to take into consideration about that.

And the third and related point is there's comments by a group of network researchers trying to improve overall network performance who have said that having a research exception so that it can really analyze the data has some public benefits. So an across-the-board ban might run into cybersecurity and research problems, so there should be some nuance as people consider that.

Senator BLUMENTHAL. Thank you.

The CHAIRMAN. Thank you, Senator Blumenthal.

Senator Markey, do you have other questions?

Senator MARKEY. May I, Mr. Chairman?

The CHAIRMAN. Yes.

Senator MARKEY. Thank you. Tell me, Professor Ohm, if you could, how you view this issue of what information can ISPs collect about consumers, and how can that information be used to paint a detailed picture of their lives?

Mr. OHM. I like when I talk to my students about this, I like to ask them to imagine, if they will, a stream of information just streaming behind you, always connected to you, that in a very detailed way really does kind of amount to the sum and substance of who you are. I think you actually said this earlier in the hearing, right? This is detailed, this is persistent, and it's very, very, very difficult to escape this, right?

Senator MARKEY. So if a mother is searching for information about her 13-year-old daughter's anorexia——

Mr. OHM. Yes.

Senator MARKEY.—the ISP has that information.

Mr. OHM. Absolutely, and——

Senator MARKEY. And so does the website that she went to——

Mr. OHM. Of course.

Senator MARKEY.—but the ISP has the information as well.

Mr. OHM. That's right, and it speaks to proposals that some have suggested that the FCC just make this about what is sensitive or not, right? But that is getting at this problem the wrong way. I mean, it's better to categorically say that this is intrinsically who you are, and, in fact, whether something is sensitive or not really might vary minute to minute, second to second.

Senator MARKEY. So if the mother or the daughter, the 13-year-old, went to a religious website, the ISP has that information.

Mr. OHM. Right.

Senator MARKEY. Now, the daughter or the mother, they know that they went to the religious website, so they know what they're doing.

Mr. OHM. Right.

Senator MARKEY. Now, the ISP has it as well.

Mr. OHM. That's right. That's right.

Senator MARKEY. Is that sensitive?

Mr. OHM. Absolutely. Not just that they visited it once, but precisely to the second when they visited it, how much information they downloaded from it, perhaps if it's not encrypted, exactly what sub-page they were looking at, what specific affliction or what specific religious question they were interrogating the website about, and I think, as importantly, how many times they revisit it, when they revisit it, and the name of the game here in a big data world is to correlate that with everything else in your life.

Senator MARKEY. So how about if I need a loan and I've gone to one of those websites?

Mr. OHM. Absolutely.

Senator MARKEY. I know I'm going to that website, I need a loan, but the ISP knows it as well.

Mr. OHM. And contrast this with 1996, when we were focused a little bit more on telephone numbers, right? There was a tiny bit of comfort from a privacy point of view in not knowing exactly what you did when you called a particular number, and, in fact, examples have been made, people call weather lines and they call for the lottery numbers. On the Web, often the domain name will reveal exactly what you are doing. In fact, I've sometimes described it as a machine that preserves the very last thought that you had in your head. So that's what's being logged.

Senator MARKEY. So how can ISPs use the information in a way that could harm the consumer?

Mr. OHM. Yes, I mean, you know, the FTC itself has documented in their Big Data report that they would like to sell this information to data brokers, and just to be clear, that's not what the FTC said about ISPs, but I'm talking about the advertising ecosystem more generally, and they would like to categorize you, and, you know, it might just be for marketing purposes. It might be that you're the kind of person who is more likely to be interested in this product because of the things that you've been reading lately.

Senator MARKEY. And so how would the FCC's rules protect that personal information that I just outlined amongst thousands of other potential examples?

Mr. OHM. Yes. In my mind, the most important, I would say, feature of the rule is the fact that in an opt-in world, you have the comfort of not having to think about this, that if you're someone who is worried about this in any way, your choice by default is not to be tracked or for the information not to be used in this way. On the other hand, if you're someone looking for a deal with your ISP, your ISP has ample opportunity to sell that service to you, and you can opt in to the tracking——

Senator MARKEY. In other words, the ISP says, "Please give us the right to sell all of your private information."

Mr. OHM. Yes.

Senator MARKEY. You have the right to give them the permission.

Mr. OHM. Absolutely. Like I said, there's no ban here. And, in fact, I think ISPs are probably going to be successful convincing some consumers to undergo programs like this, but for the rest of the people, again, it's the comfort of the bright line, it's the ability to live under the default rule, which protects the expectation that a lot of consumers have and to address the fears that a lot of——

Senator MARKEY. And I find that in general as kind of a rule, there are some people, they have some disease, you know, they're telling everyone about it.

Mr. OHM. Right.

Senator MARKEY. OK?

Mr. OHM. Yes.

Senator MARKEY. And there's an equal number of people going, "I'm not telling anybody about this. If you tell anyone I have this disease, I'm going to kill you." Right?

Mr. OHM. Right.

Senator MARKEY. So you should have that right, you know, just to say, you know, if you want to brag about it, you know, then you go and do it, but if you want to keep it a complete secret, you should be able to do so as well, and this is the option that the FCC is giving to people.

Mr. OHM. I think it's not inaccurate at the end of the day to boil down this rulemaking as, how can we best give the opportunity for consumer choice, respect that consumer choice, and at the same time allow ISPs to engage in innovative and competitive economics?

Mr. GARFIELD. Professor Ohm, what you've eloquently argued for in your writing and today is a reworking of the privacy framework

in the United States, and what I would humbly suggest is that the appropriate place for that discussion to occur is in Congress and not in an agency.

Mr. OHM. And I would just submit that I think that debate was had at least in part in 1996, when this Section 222 was enacted, and, frankly, I think it's continuing to happen. The House had a hearing on this last month. The Senate has a hearing today. There is ample opportunity to amend the statute if that's the will of this body, but the law on the books is clear and unambiguous.

Senator MARKEY. I guess the way I would view it is you put HIPAA on the books, you put FERPA on the books——

Mr. OHM. So there, well, the law is there for the FCC to act under.

Senator MARKEY. They're there as a section of the law, and they're acting under that section of law, so it's not a rewriting of the laws, it's an interpretation of the law reflecting the change in technology, but not a change in the authority under which they are operating.

Mr. OHM. And Mr. Garfield is right, it's a distinctly American phenomenon that we do not have a lot of privacy laws. This body has been very deliberate about identifying those opportunities, those moments, those industries, those contexts where specific law is needed, and it did so when it comes to telecommunications providers.

Senator MARKEY. And common carriers have always been.

Mr. OHM. Absolutely.

Senator MARKEY. Since 1934 in this special category.

Mr. OHM. That's right.

Mr. GARFIELD. It is true that the U.S. approach is distinct, but the U.S. approach is not deficient, and so we shouldn't confuse those two things. Even in Europe, which is viewed as heightened privacy protection, is based on the same FIPs framework that the United States is, and the Privacy Shield that was just advanced is a reflection of the rough equivalence of the approaches that are taken here in the United States and Europe. So to suggest that just because the U.S. is different in fact means it's distinct is counterfactual.

Senator MARKEY. Thank you.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you.

Mr. Leibowitz, do you have anything to add on that?

Mr. LEIBOWITZ. No. I mean, I think yours is a principal position, Senator Markey, as it always is, but, you know, the vast majority of data collection online is by non-ISPs, and we had a term for them at the FTC, for all collectors of data, we called them "cyberazzi." And the better approach to take, from my perspective, and again we can disagree, and from the 21st Century Privacy Coalition's perspective, is try to keep your approach technology-neutral, and when you can't, try as much as possible to adopt the FTC approach, which you've been supportive of and which has been tested for many years and deemed reasonably successful.

Senator MARKEY. And again, I think that, while I agree with you on all these social media sites in terms of the protections which should be there, the ISP has a special relationship, it's the only

way you can get online. You don't have a choice. You know? If you want to reach 1 million websites, you've got to go through one company, and so that's a special relationship. They're gathering everything. And so that's separate from an individual decision which a consumer is making to go to that social website or that one or that one. And so I just think there is a distinction that exists because they control the conduit. The content-conduit divide is quite profound, and that's why this industry, this conduit industry, which is the ISPs, but it was the telephone company as we were growing up, was always under this special regime because everyone had to go through the same company.

The CHAIRMAN. So, Mr. Leibowitz, is there any reason to think that consumers under the FCC proposal, having been given some greater control about how broadband providers use their information, may feel a false sense of security that other online entities are also going to be respecting those ISP-related control decisions?

Mr. LEIBOWITZ. Well, I mean, they may feel a false sense of security, there may be consumer confusion. They may not understand why they can't get discounted products from their ISPs online without either an opt-in, or if it's for the broadband itself, why they can't get it at all while they can get it from everyone else in the Internet ecosystem. So, yes, I think that's a possibility.

The CHAIRMAN. All right. Senator Blumenthal, do you have any more questions?

Senator BLUMENTHAL. I have just a couple of quick questions, Mr. Chairman.

To ask a somewhat mundane question, I'm impressed—maybe I should direct this to both you, Mr. Leibowitz, and any other members of the panel who want to respond—that there is often overlapping and disparate responsibility for enforcement of privacy protections. The example that comes to mind is HIPAA. The Department of Health and Human Services enforces the Health Insurance Portability and Accountability Act, I'm saying it just so I can remember what it stands for, HIPAA——

[Laughter.]

Senator BLUMENTHAL.—the privacy rules that operate under that statute and regulate the use and disclosure of protected health information. The FTC exercises a complementary jurisdiction over all the entities or individuals with access to the personal medical information not covered by HIPAA, and for many people, their introduction to HIPAA and to privacy concerns is when they want information about a loved one and find obstacles to obtaining it.

So my question is whether this system can be rationalized. I know it sounds like mundane and somewhat nuts and bolts. Would you say that the broadband privacy rule is analogous to this issue?

Mr. LEIBOWITZ. Well, yes, Senator, I do think it is, or at least it was. So in the first Obama term, they came up with a Consumer Privacy Bill of Rights, and they wanted the FTC to be responsible for all privacy enforcement across the board, and they wanted it to focus on sensitive information. It's now—the answer is, yes, of course, it could be, but now with the FTC having invoked Title II, it has created, it has designated ISPs as common carriers, and so as common carriers, it can't forebear back to the FTC in this area.

What it can do—and as you know, we need a cop on the beat because when the FTC's jurisdiction was taken away, there was no one left but the FCC. But what they can do, and it goes to your point about DPI and sensitive information, is they can make their rule sort of more rational and more reflective of the FTC's approach. And, by the way, they have authority over practices that are unjust and unreasonable, and that's not too far from the unfair and deceptive statute that you worked with when you were the Connecticut AG and that the FTC works with all the time.

Mr. OHM. So if I may, Chairman Leibowitz receives a lot of well-deserved praise for the work that the agency did in privacy. He made one horrible misstep while he was there, he hired me——

Mr. LEIBOWITZ. Not at all.

Mr. OHM.—to be a Senior Policy Advisor for privacy issues. I witnessed an agency that is operating at the top of its game, and it's developed a well-earned reputation for being one of the savviest privacy enforcers probably globally. At the same time, there is nothing that the FCC is trying to do here which is inconsistent with the FTC rules. There is no company that is going to be told X by the FCC and Y by the FTC. In fact, some companies will actually have engagement with both of the agencies in a way that's complementary, not contradictory. There's an MOU that the staff of the two agencies entered into that kind of reflects this.

I think people have read far too much into this staff comment, which 99 percent of it was supportive and offered little tweaks, and there was one sentence in there which I totally concede was mildly critical of the FCC.

And then the last thing I'll say, because I'm so glad you brought us back to the HIPAA analogy, one way to I think, I think, fairly characterize the way this debate has unfolded is to say we have this law, it protects health information, it obligates doctors and hospitals to respect it because we think they ought to respect it, but in today's online ecosystem, it turns out Fitbit knows a lot of health information about you. Is the argument, is the result, really that we should now say, you know what, there is no use regulating privacy of hospitals and doctors any longer, that we ought to lower the standard of privacy just because there are online actors who now have comparable sets of information? I don't think so. I think that would be an odd argument to try and make in the health context, and I think it's equally odd in the online context.

Mr. GARFIELD. And the argument is not to lower, the argument is to respect and recognize the work that's been done from the agency that's well versed in this area.

Mr. LEIBOWITZ. Yes, and I would just add one thing. You have both probably read the FTC comment. You cited it, Chairman Thune, at the beginning of the hearing. All I would say is go back and read the FTC comment to the FCC. It uses the phrase, and it's diplomatic, as it should be, but it uses the phrase "not optimal," and I counted 28 separated instances where they're in disagreement or where they question a potential policy of the FCC. Don't take my word for it, don't take Professor Ohm's word for it, don't take the very smart—don't——

[Laughter.]

Mr. LEIBOWITZ.—I mean, listen to us because I think collectively we have something to say, but go back and just listen to the FTC.

The CHAIRMAN. I think it would be incredibly complicated to have to answer to multiple agencies on this issue, but you pointed out, Mr. Leibowitz, that the law clearly prohibits the FTC from regulating communications common carriers. Is there any clear limitation in law that prevents the FCC from regulating the privacy practices of so-called edge providers?

Mr. LEIBOWITZ. You would have to have a very expansive view of Section 706 to try to do that and——

Mr. GARFIELD. You may get some arguments from us.

[Laughter.]

Mr. LEIBOWITZ.—we would get some arguments from Mr. Garfield about that.

Mr. SWIRE. Yes, I was going to say it may be challenged.

Mr. LEIBOWITZ. I don't want to say they couldn't do it, and I don't want to say this FCC couldn't do it. I think it would be a bad policy, and I don't—you know, and I think it would be just an extension of what we believe now is a flawed policy at the FCC, and you would extend it from a small group of collectors of information on the Internet to the vast and overwhelming majority. So I think we have agreement on that.

Mr. GARFIELD. Yes, we do.

The CHAIRMAN. All right. Well, with that, we'll wrap up. We thank you all very much for your insights and your input. And we'll keep the hearing record open for 2 weeks during which time Members are encouraged to ask or submit questions for the record, and upon receipt, we're asking witnesses if they would submit their answers to the Committee as soon as possible.

Thank you all very much. This hearing is adjourned.

[Whereupon, at 12:09 p.m., the hearing was adjourned.]

A P P E N D I X

Response to Written Question Submitted by Hon. Deb Fischer to Paul Ohm

Question. Professor Ohm, you have said that it is important to keep privacy protections in mind for rural Americans, because they may have access to only one broadband provider. Living on a ranch in Cherry County, Nebraska, I certainly understand the challenges facing rural America when it comes to broadband availability. That said, I am not clear how the number of broadband providers in a given area is related to the level of privacy protection that is needed. Are you suggesting that the providers that offer service to rural America should be subject to more stringent privacy protections than other providers? It seems like that would only hurt broadband deployment where we need it most.

Answer. I did not mean to suggest that the privacy protections for providers should vary based on the amount of choice consumers have in a given region. I am sorry if I was not clearer about this. I think the limited choice that most American consumers have for broadband service strongly supports the need for special privacy rules for broadband providers, such as those proposed by the FCC. A consumer who is unhappy with the privacy practices of his or her broadband provider can often not switch to a more privacy-respecting competitor, because there often is no viable alternative on the market. This is especially a problem for the millions of Americans with only one choice for broadband, a population that includes many rural Americans and Americans living on tribal lands.

The lack of choice in broadband service is only one justification for the FCC's privacy rules. My testimony supplies at least three others (history, visibility, and sensitivity). These reasons justify a privacy rule for all providers, large and small, urban and rural, and irrespective of whether consumers in a covered region have one provider, two providers, or more. I once again applaud the FCC for proposing a strong privacy rule, one that implements Congress's intent in Section 222 of the Communications Act.

Response to Written Questions Submitted by Hon. Deb Fischer to Dean C. Garfield

Question 1. Mr. Garfield, as you know, the number of mobile devices in this country is growing at an exponential rate. The Internet of Things has the potential to grow our economy and make our workforce more productive. As we talk about the Internet of Things, concerns are inevitably raised about how we can protect the privacy of the data that is sent from device to device. While these are important concerns, I also worry that overly restrictive privacy regulations will stifle development of the Internet of Things. Do you believe that is the case for the FCC's proposed regulations?

Answer. I would like to begin by thanking you for your leadership on the Internet of Things and the DIGIT Act. That legislation recognizes the important and transformational impact the IoT will have in our communities, our economy, and society at large when we consider safety, health, and other applications we cannot yet fathom. We would agree that overly restrictive privacy regulations could, and likely will, prevent investment, innovation, and experimentation in the IoT.

As you know given your significant work on IoT, in applications where data that identifies individuals is collected, the collection, use, sharing, and protection of such data are already subject to existing laws. For instance, IoT manufacturers fall within the jurisdiction of the Federal Trade Commission (FTC) and are thus subject to its unfair or deceptive acts or practices authority under Section 5 of the Federal Trade Commission Act. Grounded in Fair Information Practices Principles (FIPPs), the FTC's approach to privacy helped enable the Internet to thrive and, as a consequence, ITI companies have been able to offer an expanding range of services and applications (including IoT applications), often times free or at a nominal expense

to consumers. Depending on the data collected and the actors involved, other statutory authorities may also be applicable to IoT products or services. There are certain protections for health information under the Health Insurance Portability and Accountability (HIPAA) Act and the Health Information Technology for Economic and Clinical Health (HITECH) Act, while the Graham-Leach-Bliley (GLB) Act and the FTC's Safeguards Rule govern the protection of information held by financial institutions.

In addition to being overly prescriptive and not grounded in the FIPPS, which guides privacy frameworks around the globe, the FCC's proposed rule also subjects the same data to different requirements based on which sector collects the data. We believe this is a bad precedent and will limit not just IoT development but innovation by companies that may operate in multiple spaces such as broadband Internet access service providers who may also offer IoT products or applications, or online content or services.

Question 2. Mr. Garfield, in your testimony you describe how the FTC and state attorneys general work together to create a meaningful system of enforcement and consumer protection. For example, state attorneys general typically enforce laws addressing "unfair or deceptive acts or practices" at the state level, while the FTC will do the same on the Federal level. Under the new privacy regime proposed by the FCC, what will be the role of state attorneys general? Will their authority be changed in any way?

Answer. The NPRM specifically proposes to "preempt state laws only to the extent they are inconsistent with any rules adopted by the Commission." [1] If a state regulation or law conflicts with the Commission's final rule, the role of that state's Attorney General would be significantly diminished in that he or she would no longer be able to bring an enforcement action against broadband providers for violations of such existing state regulation or law until the state regulator or legislature acts to bring the rule or law into alignment with the FCC's rule. Further, states may continue to enforce or adopt new regulations or laws that are more restrictive than the FCC's rule so long as compliance with both the state regulation or law and the Federal regulation is feasible.

Response to Written Question from Hon. Deb Fischer to Matthew M. Polka

Question. Mr. Polka, in his written testimony, Professor Ohm said that it is important to keep privacy protections in mind for rural Americans, because they may have access to only one broadband provider. Living on a ranch in Cherry County, Nebraska, I certainly understand the challenges facing rural America when it comes to broadband availability. That said, I am not clear how the number of broadband providers in a given area is related to the level of privacy protection that is needed. It seems like putting more stringent requirements on rural providers would only hurt broadband deployment where we need it most. Do you have thoughts on this point?

Answer. As a threshold matter, Professor Ohm is incorrect that rural consumers may have access to only one broadband provider. In virtually every community and in all but the most remote areas, consumers can access at least two wireline broadband providers, four wireless broadband providers, and two satellite broadband providers. In addition, as I discussed at the hearing, the question is not whether or not consumers get privacy protections. Of course, they do. The question is how to develop and implement robust privacy protections for customer proprietary network information consistent with other public interest objectives, including, as you state, enhancing broadband deployment. Broadband Internet access providers have been subject to the Federal Trade Commission's privacy regime for many years, and it has successfully protected consumers and proven workable for providers. Rather than create extensive new requirements from whole-cloth, the Federal Communications Commission should use this model as the basis for its rules.

○

[1] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services,* WC Docket No. 16–106, Notice of Proposed Rulemaking, FCC 16–39, ¶¶276–77 (Apr. 1, 2016).

This page intentionally left blank.

This page intentionally left blank.

This page intentionally left blank.