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

Before the
United States Senate
Committee on Commerce, Science, and Transportation
July 12, 2016

Hearing on

How Will the FCC's Proposed Privacy Regulations Affect Consumers and Competition?

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

[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.

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 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

[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.").

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.

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

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

[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).

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

---

[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/.

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 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 under protect 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

[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.

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-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

[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.

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

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, 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 emails you no doubt receive after every significant data breach or other privacy debacle; given the survey after survey which bear witness to the breadth and depth of concern American citizens have about this state of affairs; and given the critical importance of an Internet we can trust for commerce, communications, and innovation, this is 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.

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