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

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

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

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

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

The FCC has acted appropriately and wisely. Rather than dissect the proposed rules, I will focus on how the application of section 222 to these providers represents not only a straightforward application of the law but also a laudable exercise of privacy theory and policy. I support these conclusions not only through my 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 BIAS providers to serve as important gatekeepers of privacy, a sensible choice then and now,

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

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

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

1 The Statute Treats BIAS Providers as Gatekeepers of Individual Privacy

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

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

1.1 History

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

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

1.2 CHOICE

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

1.3 VISIBILITY

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

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

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

---

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

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

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

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

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

1.4 SENSITIVITY

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

---

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

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

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

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

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

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

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

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

2 THE NEED FOR BRIGHT LINES

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

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

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

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

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

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

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

3 THE LEVEL PLAYING FIELD

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

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

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

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

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

4 THE NEED TO ENHANCE PRIVACY IN OTHER CONTEXTS

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

4.1 THE FTC CANNOT GO IT ALONE

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

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

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

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

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

4.2 THE NEED TO STRENGTHEN OUR PRIVACY LAWS

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

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

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

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

5 CONCLUSION

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