Testimony by Peter Swire
Huang Professor of Law and Ethics
Scheller College of Business
Georgia Institute of Technology

Senate Commerce Committee Hearing
"How Will the FCC's Proposed Privacy Regulations Affect Consumers and Competition?"

July 12, 2016

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, 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 mis-perceptions, 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.
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 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 email, 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 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 emails, 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 web sites.[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, 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 percent 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.

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.
- 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 particular . . .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 web site 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]

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.

Endnotes:

[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.
[3] My statement is at https://peterswire.net/wp-content/uploads/Swire_FCC-testimony_CPNI_04_27_15.pdf.
[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.
[9] "2016 Global Internet Phenomena, Latin America & North America," *Sandvine*, 1, Jun. 2016 ("Sandvine forecasts that 70% of global Internet traffic will be encrypted in 2016, with many networks expected to exceed 80%") *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.
[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.*
[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% 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.
[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.
[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.
[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.*
[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 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% of the US 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.

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.