July 6, 2016

Supplementing the Record About Limits on ISP Comprehensive and Unique Visibility

Peter Swire & Justin Hemmings[1]

Executive Summary

These reply comments to the Federal Communications Commission (FCC) provide additional facts about limits on the ability of Internet Service Providers (ISPs) to have "comprehensive" and "unique" visibility into the Internet activities of individual users.

To provide context for these comments:

1. 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).[2]
2. In February, we issued a Working Paper on "Online Privacy and ISPs: ISP Access to Information is Limited and Often Less Than That of Others."[3] 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.[4]
3. 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,"[5] (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.
4. These reply comments supplement the record by providing additional facts and insights to support our view that ISPs lack comprehensive knowledge of or unique insights into users' Internet activity, in light of comments already submitted to the FCC. As with our February Working Paper, these reply comments take no position on what rules should apply to ISPs and other players in the Internet ecosystem going forward; however, public policy should be based on an up-to-date and accurate understanding of the facts. 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.

These reply comments have two main themes:

1. **ISP visibility 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.

2. **ISPs appear to lack unique data insights into users' Internet activity.** In the reply comments, 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.

Discussion

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

Our Working Paper set forth important limits on the ability of ISPs to have "comprehensive" visibility into user behavior. The most important of these is the historic shift to encrypted traffic. Other reasons include the historic shift to mobile computing, so that the home or work ISP often does not see a user's mobile activity, as users shift among multiple hotspots.

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,[6] and encryption will become increasingly ubiquitous in the next five to ten years.[7] 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 our 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.[8] 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.[9] 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.[10] 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.[11]

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.[12] 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 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.[13] 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.[14] 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.[15] The organization hosts a support community for those seeking to implement Let's Encrypt certificates and to navigate the obstacles to encrypting a website.[16] In March, Let's Encrypt issued its one millionth certificate and reported a rate of growth of 100,000 certificates per week.[17] The success of the project, thanks in part to the support of numerous sponsors from public interest groups and technology companies,[18] is raising encryption adoption for smaller web sites.[19]

- **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.[20] 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.[21] 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,[22] 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.[23] The FTC gave notice that companies face the risk of enforcement action if they fail to encrypt their devices and communications.[24] 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 other display advertising-supported sites to follow suit.**

Our original Working Paper provided extensive additional information about the trend toward prevalent use of encryption.[25] 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 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,[26] and the market share of desktop computers is continuing to fall.[27] Today, the great majority of Internet users own mobile devices.[28]

- **Mobile traffic is offloaded to WiFi networks.** By 2014, an estimated 46 percent of all data traffic shifted to WiFi networks,[29] growing to an estimated 60 percent of all mobile data traffic by 2020.[30] 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.[31]

- **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.[32]According to the FCC, between a fifth and a third of wireless subscribers switch their carriers annually.[33] 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.[34] 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.

2. 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"[35] and their position as an Internet "bottleneck" gives them unique access to privacy sensitive insights about users.[36] 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.

Before discussing the relevant categories of data, we 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 FCC 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.[37] 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.

We next examine categories of Internet activity data identified by commenters, which are sometimes or always available to ISPs. For each category, we 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.[38] 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 our 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.[39]
  - 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.[40]

- **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."[41]
  - Insights: Many privacy experts, along with the FTC in its report on Data Brokers,[42] 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.[43]

- 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.[44] 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)[45] and NetFlow[46] are protocols for monitoring network traffic.[47] For any individual IP flow, or "sequence of packets sent from a particular source to a particular . . .destination,"[48] 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.[49]
  - 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.[50]
  - 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"[51] from the IP flow information; to do this appears to require "finger printing" each web site of interest[52] 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,"[53] Professor Nick Feamster reports that IPFIX normally samples one out of every 1,000 packets for traffic statistics.[54] 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,[55] for advertising. This data, however, is useful for purposes including network management, network security, and research.[56]

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.

For a discussion of select questions regarding our report and previous comments, please see the attached appendix labeled "Questions and Answers."

Endnotes:

[1] Peter Swire, Associate Director, The Institute for Information Security & Privacy at Georgia Tech; Huang Professor of Law, Georgia Tech Scheller College of Business; and Senior Counsel, Alston & Bird LLP. Justin Hemmings, Research Associate, Georgia Tech Scheller College of Business and Policy Analyst, Alston & Bird LLP. Research support for these reply comments comes from Broadband for America, the Institute for Information Security and Privacy at Georgia Tech, and the Georgia Tech Scheller College of Business. The views expressed here are those of the authors.

[2] 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.

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

[4] 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.

[5] *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.

[6] "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/.

[7] 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.

[8] *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.

[9] 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.

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

[11] 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.

[12] "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.

[13] 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/.

[14] 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/.

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

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

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

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

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

[20] *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/.

[21] *Id.*

[22] 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/.

[23] "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.

[24] *Id.* at 30.

[25] 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.

[26] 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.

[27] 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/.

[28] 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.

[29] "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.

[30] "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.

[31] 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.

[32]"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.

[33] "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.

[34] "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.

[35] 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.

[36] *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.

[37] 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.

[38] 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.

[39] 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.

[40] *Id.*

[41] 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.

[42] "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.

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

[44] *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.

[45] 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.

[46] 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.

[47] *See id.*

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

[49] *Id.*

[50] 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.

[51] "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.

[52] 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

[53] *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.

[54] 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.

[55] "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.

[56] 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.

July 6, 2016

Appendix 1: Questions & Answers

Q1: One comment stated that Professor Nick Feamster of Princeton University characterized your paper as full of "technical inaccuracies concerning ISP capabilities." Is this correct?[1]

A: No. Professor Feamster initially wrote that statement in a letter issued very soon after publication of our Working Paper. After reviewing our Working Paper more carefully, Professor Feamster revised his view, saying that he had "not found anything in the report that I believe is incorrect."[2]

To ensure accuracy, from the beginning we created a request for comments to alert us to any factual concerns about the paper. We carefully examined the two comments we received, and based on that we corrected one sentence in our report of 128 pages. A point-by-point discussion of those comments appears at pages 129-131 of our submission in May to the FCC. Similarly, we will receive public comments on the materials we are submitting in the reply comment phase, and respond and revise if we discover any inaccuracy.

Q2: One comment stated that the Swire Working Paper is "out of date, and intentionally lacking relevant context," specifically in failing to incorporate the importance of "predictive analytics."[3] **Do you agree?**

A: No. Public Knowledge defines predictive analytics as an "approach to targeted marketing us[ing] the numerous data points associated with an individual's online (and offline) behavior to predict with precision when, how, and on what device to deliver an advertisement so as to maximize the likelihood of success."[4] Our Working Paper provides multiple chapters that explain the modern advertising ecosystem, such as an entire chapter devoted to the growth of "interest-based advertising," a commonly-used synonym for "predictive analytics," which we stated: "includes the increasingly common practice of adding online information to cookie-based, mobile advertising ID-based, and other online information."[5]

Among other examples, we note these discussions of modern big data/predictive analytics topics in the Working Paper: (1) the different kinds of location data available to participants in the online advertising ecosystem;[6] (2) the increasing practice of appending offline data to online user profiles;[7] (3) the idea of cross-context tracking, by which companies can combine data across user contexts (such as their social network, browser, operating system, internet video, and e-commerce uses);[8] and (4) the ways that companies can engage in cross-device tracing.[9]

Q3: One comment stated that, even for encrypted data "[i]n the aggregate, this information can reveal what a customer is doing even *with* the encryption turned on" and that "network security research has definitively shown that monitoring encrypted connections is more than feasible, and can provide near plain-text results"?[10]

A: As our initial Working Paper stated,[11] when HTTPS encryption is properly deployed an ISP cannot see the content or detailed URLs. An ISP would still see the top-level domain and other sorts of IPFIX or Netflow data, such as the number of bits, length of session, and the chronological series of top-level domains visited. Our reply comments discuss how the same or similar Netflow data is often available to others; meanwhile, that information is less revealing than the information available to others in the Internet ecosystem, notably including full content and detailed URLs.

We disagree that monitoring encrypted connections "can provide near plain-text results." The ongoing public policy debates about encryption, including the FBI's efforts to read an encrypted Apple device, show that "monitoring encrypted connections" provide far less than "plain-text results."[12] Having strong encryption is so important precisely because it provides effective protection against a wide variety of attempts to learn the text of actual communications.

Q4: Comments stated that: "According to a recent report on the state of encryption, few sites provide full, modern HTTPS encryption by default, and many sites still do not support it all," and "[d]espite being major generators of behavioral and financial data, e-commerce sites are (contrary to Swire's claims) notoriously unencrypted"?[13] Do you agree with these statements?

A: The Working Paper, as well as our reply comments, document a historic and rapid rise in the use of encryption, with 13 percent of US backbone data being encrypted in early 2014, 49 percent by early 2016, and an estimated 70 percent by the end of this year. In addition, a majority of non-video traffic is now encrypted. The Working Paper also provided an appendix showing the prevalence of encryption on 42 of the 50 most visited sites.[14] One comment expressed concern that some sites only encrypt in limited circumstances, such as for credit card information.[15]

We are now updating that appendix with results from June, 2016. Of the top 50 sites, 24 encrypt by default. An additional 16 encrypt all the time when a user is logged in, so that 40 of the top 50 sites encrypt the full session when a user is logged in. An additional 7 sites encrypt at the time of purchase (such as for credit card information) or when providing account information. 3 sites do not appear to offer encryption at this time.

Although the most-visited sites have thus gone far toward adopting encryption, there is a long tail of other websites that have not to date adopted HTTPS at the same rate as the top sites, or that only use HTTPS for limited purposes, such as payment.[16] As our Working Paper and reply comments show, there are strong trends toward higher adoption by these sites, including the spread of encryption tools such as Let's Encrypt,[17] Wired.com's move to HTTPS by default,[18] and WordPress's move to provide free HTTPS for all custom hosted domains on WordPress.com.[19] In the time period where any FCC privacy rulemaking would apply, we believe these trends will mean substantial and increasing adoption of HTTPS by other websites, including for e-commerce sites.

Q5: Concerning home Internet of Things (IoT) devices, a comment has stated: "Even if these devices practice good encryption techniques – which evidence suggests they do not – [ISPs] can ascertain a home's IoT devices"?[20]

A: We share the view of the FTC and many cybersecurity experts that there are serious security flaws in the current generations of many IoT products and services, which may permit access to data by parties including ISPs, operating systems, and applications and devices that manage a user's connected devices. We believe encryption and other cybersecurity tools should be more broadly adopted in that sector in the near future, and are encouraged by the attention the topic is getting, including in the FTC's January IoT report.[21]

As part of the broader shift toward encryption adoption, Apple has announced that iOS apps (including IoT apps) must be encrypted by the end of 2016. This welcome step would block ISPs and others from seeing the details of IoT data flows.[22] Another recent development is

the announcement that the Broadband Internet Technical Advisory Group (BITAG) will produce a technical report on IoT security and privacy, to be co-edited by Professor Nick Feamster.[23]

In some ways, the ISP situation today is similar to the personal computer ecosystem in the late 90's. Industry developed many new services and features in a race for early adoption, but did not provide enough attention to security initially. Over time, industry addressed the security challenges more thoroughly, such as when Microsoft "locked down" all development except for security during the launch of its Trustworthy Computing Initiative in 2002.[24] We should learn from the mistakes of the past and try to get security built in much sooner for IoT deployment.

Q6: Comments stated, for Virtual Private Networks, that "whether the ISPs can see the domain names that users visit depends entirely on the user's VPN configuration" and "it would be quite difficult for non-experts to tell whether their configuration is properly tunneling their DNS queries, let alone to know that this is a question that needs to be asked"?[25]

A: As our Working Paper and our follow-up addendum stated, VPNs and similar services that block the visibility of domain names have the **capability** to block even the host name from the ISP. Our own research suggested that VPN use by individuals has not been especially common in the US, so we did not emphasize this technical limit on ISP visibility nearly as much as the growth of encryption. On the other hand, new services by Facebook, Google, and Opera demonstrate that this type of technology can be made user-friendly and easily adopted.

Google's Data Saver proxy service, for example, is integrated with Google's Android operating system and Chrome web browser. Google encourages new users to activate this service as part of the Android operating system registration process, and activating the process takes only a few steps whether on a mobile or traditional device.[26] Similarly, the Opera browser's new built-in free VPN requires only a few steps to activate.[27] Facebook' acquisition of the VPN service Onavo also signals the potential for a similar service for Facebook users similar to those offered by Google and Opera. [28] Onavo also already offers a VPN app for Android and iOS called Onavo Protect which can be installed and activated in a few steps.[29] While these services are often not full VPNs and are, in some cases, designed primarily to limit data usage, they are designed to block the visibility of ISPs and others about the domain names a user visits.[30]

Appendix 2: Use of Encryption on Top 50 Websites[31]
June 29, 2016

SITES THAT ARE ENCRYPTED BY DEFAULT	
WEBSITE NAME	**WEBSITE LINK**
Google	https://www.google.com/
Facebook	https://www.facebook.com/
YouTube	https://www.youtube.com/
Yahoo.com	https://www.yahoo.com/
Wikipedia.org	https://www.wikipedia.org/
Twitter.com	https://twitter.com/
Reddit.com	https://www.reddit.com/
Netflix.com	https://www.netflix.com/
Live.com	https://login.live.com/
Linkedin.com	https://www.linkedin.com/
Pinterest.com	https://www.pinterest.com/
Chase.com	https://www.chase.com/
Paypal.com	https://www.paypal.com/home
Tumblr.com	https://www.tumblr.com/
Instagram.com	https://www.instagram.com/
Bankofamerica.com	https://www.bankofamerica.com/
Weather.com	https://weather.com/
Wellsfargo.com	https://www.wellsfargo.com/
Office.com	https://www.office.com/
Wordpress.com	https://wordpress.com/
Etsy.com	https://www.etsy.com/
Microsoftonline.com	https://login.microsoftonline.com/
Microsoft.com	https://www.microsoft.com/en-us/
Washingtonpost.com	https://www.washingtonpost.com/regional/
SITES THAT ARE ENCRYPTED ALL THE TIME WHEN USER IS LOGGED IN	
WEBSITE NAME	**WEBSITE LINK**
Amazon.com	http://www.amazon.com/
Ebay.com	http://www.ebay.com/
Craigslist.org	http://washingtondc.craigslist.org/
Imgur.com	http://imgur.com/
Bing.com	http://www.bing.com/
Imdb.com	http://imgur.com/
Msn.com	http://www.msn.com/
T.co (Twitter)	http://t.co/
Blogspot.com	http://blogspot.com/
Yelp.com	http://www.yelp.com/
Walmart.com	http://www.walmart.com/
Intuit.com	http://www.intuit.com/
Buzzfeed.com	http://www.buzzfeed.com/

Aol.com	http://www.aol.com/
Comcast.net	http://my.xfinity.com/?cid=cust
Wikia.com	http://www.wikia.com/fandom
SITES THAT ARE ENCRYPTED AT TIME OF PURCHASE OR ON PERSONAL INFO PAGE	
WEBSITE NAME	**WEBSITE LINK**
Go.com	http://go.com/ *(Encrypts at the time of checkout.)*
Nytimes.com	http://www.nytimes.com/ (*Encrypts at the time of checkout.)*
Zillow.com	http://www.zillow.com/ *(Encrypts when you are viewing your personal page, not when logged in and viewing listings.)*
Apple.com	http://www.apple.com/ *(Encrypts at the time of checkout.)*
Target.com	http://www.target.com/ *(Encrypts at the time of checkout and when viewing a personal page, NOT when looking at the items to purchase.)*
Foxnews.com	http://www.foxnews.com/ (*Encrypts at the time of checkout.)*
Bestbuy.com	http://www.bestbuy.com/ *(Encrypts at the time of checkout.)*
SITES THAT ARE NEVER ENCRYPTED	
WEBSITE NAME	**WEBSITE LINK**
Cnn.com	http://www.cnn.com/
Espn.go	http://espn.go.com/
Huffingtonpost.com	http://www.huffingtonpost.com/

[1] Kate Tummarello & Alex Byers, *Tech Immigration Troubles Surface at GOP Debate*, Politico (Mar. 4, 2016, 10:00 AM) ("[P]rofessor Nick Feamster sent a letter to FCC Chairman Tom Wheeler Thursday criticizing the broadband privacy report filed Monday by longtime privacy adviser Peter Swire. He argues Swire's take makes some technical mistakes[.]") *available at* http://www.politico.com/tipsheets/morning-tech/2016/03/morning-tech-debate-headline-here-thune-eyes-quick-timeline-for-mobile-now-mccaul-courts-encryption-commission-allies-213035.

[2] Comment of Peter Swire, In the Matter of: Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106, Addendum, p.3 (May 24, 2016) ("Prof. Feamster has authorized us to say 'Upon more careful review of the paper, I have not found anything in the report that I believe is incorrect.'") *available at* https://www.fcc.gov/ecfs/filing/60001926727.

[3] 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, 11 (May 27, 2016) *available at* https://www.fcc.gov/ecfs/filing/60001974141/document/60002080037.

[4] *Id.*

[5] Peter Swire, et al., *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others*, 12 (Feb. 29, 2016) *available at* http://www.iisp.gatech.edu/working-paper-online-privacy-and-isps.

[6] *Id.* at 70-72.

[7] *Id.* at 82.

[8] *Id.* at 101-07.

[9] *Id.* at 116-121.

[10] 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, 21 (May 27, 2016) *available at* https://www.fcc.gov/ecfs/filing/60001974141/document/60002080037.

[11] Comment of Peter Swire, In the Matter of: Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106, 25-27 (May 24, 2016) *available at* https://www.fcc.gov/ecfs/filing/60001926727..

[12] Swire's own background on encryption is substantial, including 2015 testimony before the Senate Judiciary Committee, the discussion of the effects of encryption in President Obama's Review Group on Intelligence and Communications Technology, and extensive scholarship available at www.peterswire.net.
[13] 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, 19-20 (May 27, 2016) *available at* https://www.fcc.gov/ecfs/filing/60001974141/document/60002080037.
[14] Comment of Peter Swire, In the Matter of: Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106, 36-37 (May 24, 2016) *available at* https://www.fcc.gov/ecfs/filing/60001926727.
[15] 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, 19-20 (May 27, 2016) *available at* https://www.fcc.gov/ecfs/filing/60001974141/document/60002080037.
[16] Comment of Peter Swire, In the Matter of: Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106, 126 (May 24, 2016) *available at* https://www.fcc.gov/ecfs/filing/60001926727.
[17] Josh Aas, *Our Millionth Certificate*, LET'S ENCRYPT (Mar. 8, 2016) *available at* https://letsencrypt.org/2016/03/08/our-millionth-cert.html.
[18] 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/.
[19] *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/.
[20] 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, 18 (May 27, 2016) *available at* https://www.fcc.gov/ecfs/filing/60001974141/document/60002080037.
[21] FEDERAL TRADE COMMISSION, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD (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.
[22] For encrypted IoT apps, ISPs would get IPFIX data, as they do for other encrypted communications. We discuss IPFIX data in our reply comments.
[23] John Eggerton, *Broadband Stakeholders Eye Security, Privacy of Internet of Things*, BROADCASTING & CABLE (Jun. 28, 2016, 9:25 AM) *available at* http://www.broadcastingcable.com/news/washington/broadband-stakeholders-eye-security-privacy-internet-things/157645.
[24] Warwick Ashford, *Microsoft: Is Computing More Trustworthy 10 Years On?*, COMPUTERWEEKLY.COM (Jan., 2012) *available at* http://www.computerweekly.com/feature/Microsoft-Is-computing-more-trustworthy-10-years-on, Josephine Moulds, *Microsoft Never Recovered from Vista, says Steve Ballmer*, THE TELEGRAPH (Oct. 5, 2009, 8:58 PM) *available at* http://www.telegraph.co.uk/technology/microsoft/6263248/Microsoft-never-recovered-from-Vista-blow-says-Steve-Ballmer.html.
[25] "What ISPs Can See: Clarifying the Technical Landscape of the Broadband Privacy Debate," *Upturn*, 9-10 (Mar. 2016) *available at* https://www.teamupturn.com/reports/2016/what-isps-can-see.
[26] *Use Less Data with Chrome's Data Saver*, CHROME HELP (last visited Jul. 5, 2016) *available at* https://support.google.com/chrome/answer/2392284?hl=en.
[27] Krystian Kolondra, *Free VPN Integrated in Opera for Better Online Privacy*, OPERA BLOGS (Apr. 20, 2016) *available at* http://www.opera.com/blogs/desktop/2016/04/free-vpn-integrated-opera-for-windows-mac/.
[28] Ingrid Lunden, *Facebook Buys Mobile Data Analytics Company Onavo, Reportedly For Up To $200M… And (Finally?) Gets Its Office In Israel*, TechCrunch (Oct. 13, 2013) *available at* https://techcrunch.com/2013/10/13/facebook-buys-mobile-analytics-company-onavo-and-finally-gets-its-office-in-israel/.
[29] *FAQ*, Onavo (last visited Jul. 5, 2016) *available at* http://www.onavo.com/faq/.
[30] Michal Špaček, *Opera VPN Behind the Curtains is Just a Proxy, Here's How it Works*, GitHub (last visited Jul. 5, 2016) ("This Opera 'VPN' is . . . protecting just the traffic between Opera and the proxy.") *available at* https://gist.github.com/spaze/558b7c4cd81afa7c857381254ae7bd10, Simon Codrington, *Saving Bandwith with Chrome's Data Saver*, Sitepoint (May 4, 2016) (noting that Data Saver provides a proxy server for HTTP browsing only, with Google performing the DNS lookups for the user) *available at* https://www.sitepoint.com/saving-bandwidth-with-chromes-data-saver/, FAQ, Onavo (last visited Jul. 5, 2016) ("Onavo Protect uses two different VPN types - one to manage data and the other to protect your connection.") *available at* http://www.onavo.com/faq/.

[31] Alexa lists the top 50 websites. For each site, we had a researcher visit to determine the status of encryption as of June 29, 2016.