July 6, 2016

Ms. Marlene H. Dortch, Secretary
Federal Communications Commission
445 Twelfth Street, SW
Washington, DC 20054

Via Electronic Filing

Re: **WC Docket No. 16-106, Protecting the Privacy of Customers of Broadband and Other Telecommunications Services**

Dear Ms. Dortch,

I[1] offer these reply comments to aid the Commission in distinguishing factual technical claims offered in the privacy matter from false ones. Factual errors are at the root of the Commission's decision to apply Section 222 to the firms that it terms "Broadband Internet Access Providers" when it could forbear from applying these obviously telephone technology-centric regulations to Internet Service Providers.

The Commission may either press ahead with the regulations proposed in the NPRM or revise the proposed regulations so that ISPs and other parties in the Internet marketplace are governed by non-discriminatory, consistent regulations that promote higher quality advertising through increased competition. In either case, the Commission has an obligation to ensure that its rulemaking is based on a solid factual foundation.

FCC's Factual Errors

The NPRM is based on the erroneous belief that ISPs have greater access to consumer information than do other players in the Internet marketplace. This mistaken belief is copied into the Privacy NPRM from the Commission's "Open Internet Order" of February 26, 2015. The OIO declares:

> *Broadband providers serve as a necessary conduit for information passing between an Internet user and Internet sites or other Internet users, and are in a position to obtain vast amounts of personal and proprietary information about their customers [footnote].*[2]

The footnote refers to comments on deep packet inspection filed by human rights NGO *Access*: "See, e.g., Access Comments at 7 (stating that broadband providers have the technological capacity to exercise monitoring and control of their customers' use of the

---

[1] I am an independent network engineering consultant and policy analyst affiliated with High Tech Forum as founder and editor. These remarks are offered in my personal capacity and do not necessarily represent the opinions of any client or sponsor. I have previously offered comments in several FCC dockets, have offered testimony at the FCC En Banc Public Hearing on Broadband Network Management Practices in Cambridge on February 25, 2008 as an invited technical expert, and have testified before Congress on Internet privacy. My CV is available at http://www.bennett.com/resume.pdf.

[2] Federal Communications Commission, "Open Internet Order" (Federal Communications Commission, February 26, 2015), https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf at ¶463.

[2] Federal Communications Commission, "Open Internet Order" (Federal Communications Commission,

Internet using techniques such as deep packet inspection)."

The relevant portion of the Access comments is the following paragraph:

> To implement traffic management, ISPs often use tools with highly invasive capacities that can execute blocking, shaping, or filtering of data for unlawful political, social, and commercial purposes. These tools include deep packet inspection (DPI) technology. DPI allows ISPs - and anyone tapped into their networks - to identify and filter content while it traverses the internet, and make a copy of the traffic. DPI is the go-to mechanism governments across the world employ to invade user privacy and censor communications and content with staggering breadth and depth. In 2006, AT&T and the NSA were caught using DPI-capable technology in San Francisco to sort through all traffic flowing through a major switching station, in order to pick out specific messages based on targets like an e-mail address. Left unregulated, under paid priority schemes, ISPs will be incentivized to increase use of DPI to scour internet traffic in search of content to prioritize or degrade, down to the level of individual subscribers.[3]

The Access comments display a faulty technical understanding of the Internet, and incorrect grasp of the NSA's *Stellar Wind* program and a troubled relationship with fact and logic generally. The Access comments assert that ISPs routinely break the law; they confuse DPI with simple data replication (AKA "mirroring"); and they make an extraordinary connection between NSA surveillance and the bogeyman of the Open Internet Order, "paid prioritization."

Most importantly, these fear-mongering comments overlook the fact that Stellar Wind *aggregated* data mirrored by *multiple* ISPs and then *decrypted* that data in the agency's massive computer facilities. Without aggregation and decryption, no ISP has anything like the surveillance capability represented to the FCC by this misguided NGO. While it's understandable that the NGO would fail to grasp the facts, it's not acceptable for the FCC, an expert agency endowed with exceptional regulatory power, to accept this weak analysis as if it were factual.

Oddly, the privacy threat of greatest concern to Access is not commercial data gathering but NSA surveillance. By itself, this is an odd basis upon which to rely for justification for not forbearing from Section 222.

Code Breaking

NSA surveillance is accomplished in large part by a tool that ISPs lack, a comprehensive code-breaking capacity. In the case Access cites, AT&T, other ISPs, and transit providers mirrored packets passing through some of their optical switches to NSA, who performed the analysis, including decryption. Without the NSA's decryption capability, the potential for information gathering afforded to ISPs by virtue of their "position" in the Internet infrastructure is greatly diminished. And the FCC's privacy order does not appear to

[3] Access, "Comment Re: Notice of Proposed Rulemaking on Protecting and Promoting the Open Internet" (Federal Communications Commission, July 18, 2014), https://ecfsapi.fcc.gov/file/7521700196.pdf.

regulate the NSA.

The "position" to which the Access comments refer – by way of reference to an article Access cites from Wired Magazine – is not the position of the ordinary ISP.[4] Access refers to a surveillance operation known as Stellar Wind that collected data from telephone calls and email on peering links between AT&T and other telephone and Internet transit operators and Internet Exchange Points such as the Palo Alto Internet Exchange (PAIX) and Metropolitan Area Exchange, West (MAE-West).

Although the lawsuit filed by (my former co-worker) Tash Hepting against AT&T for its participation in Stellar Wind purported to represent the interests of AT&T's residential Internet users, Stellar Wind Internet data was not limited to AT&T's or Verizon's residential customers.[5] Participants in Stellar Wind were in the Internet transit business. This means that Stellar Wind participants had access to packets flowing between Internet users with no ISP business relationships with the firms who mirrored their packets to NSA.

These information packets were not analyzed or inspected by Stellar wind participants using any form of deep packet inspection. As the declaration of former AT&T technician Mark Klein in the lawsuit indicated, NSA got this data from mirrors attached to fiber optic links at the premises of the transit networks in question facing the Internet Exchanges.[6]

NSA's Unique Position

This is to say that the FCC relies on a representation by Access to impose telephone-era privacy regulations on ISPs – the claim that ISPs "are in a position to obtain vast amounts of personal and proprietary information about their customers" – when the NSA surveillance case that animates Access's concerns had nothing to do with ordinary Internet service or with the actual capabilities of ISPs.

In Stellar Wind NSA was "in a position to obtain vast amounts of personal and proprietary information" because it was able to draw upon data passing through not one but many ISPs and transit networks. In this respect alone – even if we overlook the encryption/decryption capacity of NSA – Stellar Wind was in a different position with respect to Internet traffic than is any individual ISP. Even if AT&T, Comcast, and Verizon were able to decode each information packet flowing through their networks, these firms would only be able to see the information generated and requested by their own customers.

---

[4] James Bamford, "The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)," *WIRED*, March 15, 2012, https://www.wired.com/2012/03/ff_nsadatacenter/all/.

[5] Electronic Frontier Foundation, National Security Agency Telecommunications Records Litigation; Hepting v. AT&T (United States District Court Northern District of California 2009).

[6] Mark Klein, "Declaration of Mark Klein in Support of Plaintiffs' Motion for Preliminary Injunction" (United States District Court, Northern District of California, June 8, 2006), https://www.eff.org/files/filenode/att/mark_klein_unredacted_decl-including_exhibits.pdf.

The reality of the Internet is that each edge service or application has the unfettered ability to see the data it exchanges with each of its customers. Google, Facebook, Amazon, and Netflix see customer-generated messages in plain text, after decryption. Similarly, these firms have unfettered access to the information they send to their customers before encrypting it.

There is a gap in the edge view of the Internet insofar as each edge service only sees information from its own customers. But this gap is reduced for advertising networks that are able to populate third party pages with ads. When an edge service operates both its own application and an advertising network – as many do – the gap becomes extremely small.

The ISP also has a limited view of the Internet for three reasons:

1. Each ISP can only see information generated or received by its own customers;
2. Most of this customer data handled by the ISP is encrypted; and
3. The data the ISP can see is devoid of context.

The first limitation is shared by ISPs, edge services, and advertising networks insofar as each can only view data exchanges involving its own customers. But this factor argues for regulating ISPs less heavily than the large edge and ad companies because the number of users each ISP has is much smaller than the corresponding number in the edge and ad space. The largest wireline ISP, Comcast, has 23 million customers.[7] Netflix has 81 million customers worldwide;[8] Amazon had 244 million users in 2014;[9] Facebook has 1.59 billion customers;[10] Google has seven different services with over a billion users *each.*[11] There is no dearth of advertising-relevant data for edge services to capture and use. For ISPs to catch up in terms of user counts, each would need to grow by one to two orders of magnitude, signing up more Internet users than the planet contains.

As noted, the increased use of encryption reduces the value of the customer data passing through ISP facilities. Unless ISPs are willing to invest in an NSA-caliber code-breaking facility, the only elements of sensitive transactions visible to ISPs are destination IP address, data volume, application type (e.g., web page vs. video stream vs. phone call), and transaction time of day. DNS lookups duplicate IP addresses and can be exported to third party DNS providers in any case (and would be, if such activities were truly valuable).

---

[7] Jon Brodkin, "Comcast Shrugs off Years of Cord-Cutting Losses, Adds 89K TV Customers," *Ars Technica*, February 3, 2016, http://arstechnica.com/business/2016/02/comcast-shrugs-off-years-of-cord-cutting-losses-adds-89k-tv-customers/.
[8] "Netflix : Overview," accessed July 7, 2016, https://ir.netflix.com/.
[9] "How Many Customers Does Amazon Have? -- The Motley Fool," accessed July 7, 2016, http://www.fool.com/investing/general/2014/05/24/how-many-customers-does-amazon-have.aspx.
[10] "Here's How Many People Are on Facebook, Instagram, Twitter and Other Big Social Networks," accessed July 7, 2016, http://adweek.it/1qqjteI.
[11] "Google Has 7 Products With 1 Billion Users | Popular Science," accessed July 7, 2016, http://www.popsci.com/google-has-7-products-with-1-billion-users.

The context factor is extremely significant and often overlooked. Raw packet streams contain more noise than signal, while application transactions take place in a coherent context. When we perform an Internet search, the search engine knows we're doing a search and which search terms we use without expending any processing resources to speak of.

Examining a stream of packets to determine the same information is much more processing-intensive when it can be done at all; Google, Bing, and Yahoo encrypt Internet searches. But even if they didn't, extracting searches from IP packets does indeed require DPI, a considerable expenditure of processing power.

Creating context for social network interactions from raw packet streams also requires a great deal of processing that isn't required by the social network itself. The business of the social network is all about keeping track of the people and subjects that attract our interest. For an ISP to develop the dossiers social networks maintain on users would require at least an equal expenditure of processing power as that expended by the social network in addition to the processing power necessary for the ISP to conduct its business as an ISP. And the ISP would need to apply this processing power in a different way for each edge service whose interactions it wanted to track. This is probably unrealistic.

Consequently, ISPs are not the NSA and they don't have the ability to comprehensively survey every – or even many – of the transactions that take place over the Internet.

Conclusion

Like the game of *Telephone*, the facts of Stellar Wind are distorted by the Hepting/EFF lawsuit, further twisted by the *Wired* article, misrepresented by Access, misconstrued by the FCC's Open Internet Order and confused again by the FCC's Privacy NPRM. ISPs do not have the surveillance advantage over edge services and advertising networks the NPRM attributes to them.

Consequently, the privacy NPRM lacks a coherent factual foundation for the claim that ISPs must be regulated differently than edge services because of their unique vantage point in the Internet.

In reality, edge services, browsers, operating systems, advertising networks, and transit networks all have better and more comprehensive knowledge of user interactions with edge services than ordinary ISPs do. As this is the case, the FCC's decision to impose Section 222 with a new set of rules deeply at odds with the FTC Privacy Framework is irrational.

The more prudent course is to forbear from imposing the Section 222 opt-in provision on Internet service providers and to generally harmonize ISP privacy regulations with the FTC framework. Opt-in is appropriate for sensitive information but not for generic interactions.

Supporting Material

The following includes recent blog posts pertinent to the Privacy NPRM as well as written testimony I gave to the House Energy and Commerce Communications Technology and the Internet Subcommittee on Internet privacy in April, 2009.

The blog posts provide technical analysis of the current state of privacy in the Internet and of the debate about Internet privacy policy.

This testimony precedes my employment in the public policy field. The testimony discusses the origin and use of deep packet inspection tools and offers a comprehensive picture of threats to Internet privacy. The testimony is available online at HighTechForum.org http://hightechforum.org/wp-content/uploads/2016/07/Privacy-Testimony-2009.pdf

The blog posts are first and the Congressional testimony follows.

Appendix A: Bringing Privacy Into the Open

This High Tech Forum blog post from January 26, 2016 addresses a letter sent to the FCC by a group of privacy advocates. It is available at http://hightechforum.org/bringing-privacy-into-the-open/

Appendix B: CDT's Diagram Muddies the Waters

This High Tech Forum blog post from February 9, 2016 addresses a memo from CDT on the issues facing the FCC as it begins a privacy rulemaking. The memo conveyed errors of fact and analysis that I sought to correct. It is available at http://hightechforum.org/cdts-diagram-muddies-the-waters/

Appendix C: FCC Confused about Privacy

This High Tech Forum blog post from March 10, 2016 addresses the vantage point error drawn into the Privacy NPRM from the OIO. It is available at http://hightechforum.org/fcc-confused-about-privacy/

Appendix D: Internet Architecture vs. Section 222

This High Tech Forum blog post from June 10, 2016 addresses the fundamentally different architectures of the Internet and the telephone network and how those differences way on the expectation of and responsibility for privacy. Available at http://hightechforum.org/internet-architecture-vs-section-222/

Appendix E: Congressional Testimony, April 2009

This is the Congressional testimony I offered on Internet privacy in April 2009 while working as a software engineer in Silicon Valley. I include it here because the copy on the House web server suffers from link rot. A copy is available at http://hightechforum.org/wp-content/uploads/2016/07/Privacy-Testimony-2009.pdf

Appendix F: A Google monopoly today means packet snooping tomorrow: A plan to protect our privacy

This is an opinion column I wrote for The Register, the leading European technology news site, on June 29, 2009. It covers the implications of the April hearing in the House, arguing that regulations on data collection are less important to consumers than regulations on data protection and resale. The headline prediction is prescient, of course. Available at http://www.theregister.co.uk/2009/06/29/bennett_google_privacy/