



GEORGETOWN LAW

Paul Ohm
Professor of Law

July 29, 2016

Chairman Greg Walden
Subcommittee on Communications and Technology
U.S. House of Representatives Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Walden,

Thank you for the opportunity to testify to the subcommittee on June 14, 2016. I truly appreciated the opportunity to share my thoughts with Members about the FCC's important proposal to protect the privacy of consumers of broadband Internet.

I also appreciate the additional questions for the record you have asked me. My answers follow. Please do not hesitate to let me know if you have any other questions for me.

Answers to Additional Questions for the Record

- 1. In your 2009 working paper titled, "The Rise and Fall of Invasive ISP Surveillance", you write that ISPs have "an amazingly pristine track record" when it comes to respecting consumer privacy. It appears from your testimony that you believe that they are, nonetheless, deserving of regulation to protect consumers. Could you give specific examples, other than the FTC's enforcement actions levied against ISPs, in which ISPs appear to have violated consumers' privacy, justifying your stance?**

Answer: It is my great regret that this statement from seven years ago is no longer true. Although I hesitate to claim that there is an epidemic of reported violations of consumer privacy by ISPs, there is a worryingly long and growing list of examples I can point to. Simply put, ISPs seem to be abandoning their historical reticence to intrude into consumer privacy in ways that I find highly problematic. Let me give you three examples.

Example 1: Verizon Wireless and UIDH. In October 2014, researchers discovered that for two years Verizon Wireless had been injecting a unique tracking number, known as

a Unique Identifier Header or UIDH, into the private communications of its customers.¹ A unique identifier is like a fingerprint, which allows a user to be tracked as he or she moves around the web, and can actively subvert user efforts to preserve a modicum of privacy surrounding their online behavior.

For example, if a user follows standard consumer protection advice and clears his cookies from his browser, the UIDH will give any observer on the web the ability to completely undo this action, restoring whatever profile the user had attempted to clear. Because of the way a UIDH works, this power to subvert user wishes extends not only to Verizon Wireless and its business partners, but it is instantly available to *any* entity online that communicates with the user. Because of this user-expectation-defeating characteristic, researchers have referred to the UIDH as a “supercookie” or a “permacookie,” both terms that carry a significant negative connotation.²

There is even documented evidence (to be clear, not about this specific example) that non-commercial actors such as intelligence agencies exploit commercial unique identifiers to further their own surveillance activities.³ It is thus no exaggeration to say that the Verizon Wireless UIDH subverted the lawful efforts by citizens to protect their communications from tracking by domestic and international governments.

In my expert opinion, Verizon Wireless’s silent deployment of this technology without asking for consent represented a breach of online norms, a violation of technical edicts such as the end-to-end principle, and a potential violation of consumer protection laws.

This example also underscores the importance of Section 222, the very authority under which the FCC purports to promulgate the rule that was the subject of my testimony. After Verizon Wireless’s actions came to light, the FCC opened an investigation under the authority of Section 222. In March of this year, the FCC and Verizon Wireless reached a settlement in which the company agreed to obtain opt-in consent—the very form of consent proposed by the FCC its new rule—and to pay a fine of \$1.25 million.⁴

Example 2: CableOne’s use of FICO Scores. In May of this year, Thomas Might, the CEO of Cable One, revealed that his company takes a customer’s FICO score into account

¹ Robert McMillan, *Verizon’s ‘Perma-Cookie’ is a Privacy-Killing Machine*, WIRED, Oct. 27, 2014, <http://www.wired.com/2014/10/verizons-perma-cookie/>.

² See Craig Timberg, *Verizon, AT&T Track Their Users with ‘Supercookies,’* WASH POST, Nov. 3, 2014, available at http://www.washingtonpost.com/business/technology/verizon-atandt-tracking-their-users-with-supercookies/2014/11/03/7bbb382-6395-11e4-bb14-4cfea1e742d5_story.html; Jacob Hoffman-Andrews, *Verizon Injecting Perma-Cookies to Track Mobile Customers, By-Passing Privacy Controls*, Electronic Frontier Foundation, November 3, 2014, available at <https://www.eff.org/deeplinks/2014/11/verizon-x-uidh>.

³ Ashkan Soltani, Andrea Peterson & Barton Gellman, *NSA Uses Google Cookies to Pinpoint Targets for Hacking*, WASH POST, Dec. 10, 2013, <https://www.washingtonpost.com/news/the-switch/wp/2013/12/10/nsa-uses-google-cookies-to-pinpoint-targets-for-hacking/>.

⁴ FCC, *Verizon Wireless to Pay \$1.25 million to Settle Investigation*, https://apps.fcc.gov/edocs_public/attachmatch/DOC-315501A1.pdf (July 31, 2012).

when deciding whether to provide adequate customer service.⁵ Speaking at an industry conference, Mr. Might explained that “We don’t turn people away,” but that they would not allow their support staff to “spend 15 minutes setting up an iPhone app” for a customer with a poor credit history. He defended this as a way to “pinpoint where churn and bad debt was coming from.”⁶

After receiving criticism from consumer advocates and policymakers, the company backtracked, contradicting its CEO in a letter to the FCC.⁷ In this letter, the company is reported to have explained that FICO scores are used to “determine the size of the deposit and the installation charge” but does not use it to later dole out customer service. Although the company characterized this letter as a clarification, it appears to flatly contradict the earlier revelation by the CEO, at the very least raising serious questions about whether this company has systematized the violation of customer privacy.

Example 3: DNS Hijacking. In the Swire Report, which has generated much commentary in this FCC proceeding, the authors describe the growing trend of users configuring their computers to send DNS directory lookup requests to an entity other than their ISP.⁸ The suggestion is that this is one other way market developments and user self-help has blinded ISPs to the traffic of their users. The report fails to mention many well-documented examples of ISPs embracing a questionable tactic known as “DNS Hijacking” to subvert this user choice and to restore visibility into a user’s browsing activity.⁹ Once again, this conduct violates well-established norms of appropriate online behavior as well as intrudes into user privacy.

The bottom line is that ISPs have demonstrated on multiple occasions that the restraint and respect for user privacy I complimented in 2009 has unfortunately dissipated in the intervening years. These developments justify the fear I expressed in that article, Congress’s prescient decision to treat telecommunications services as deserving of a sectoral privacy law in enacting Section 222, and the FCC’s proposal to enact this law in its proposed rule.

- 2. You state that it is true that other online entities are beginning to rival BIAS providers with regard to the information they collect. You highlight social networking sites. Is it your contention that other parts of the online ecosystem like these should be more heavily regulated—sector specific—with regard to online privacy—yes or no?**

Yes.

⁵ Daniel Frankel, *Cable One using FICO Scores to Qualify Video Customers, Might Says*, FIERCECABLE, May 23, 2016, <http://www.fiercecable.com/story/cable-one-using-fico-scores-qualify-video-customers-might-says/2016-05-23>.

⁶ *Id.*

⁷ Daniel Frankel, *Cable One Clarifies FICO Score Usage with FCC, Says it has its own System for Determining Customer Value*, FIERCE CABLE, June 28, 2016, <http://www.fiercecable.com/story/cable-one-clarifies-fico-score-usage-fcc-says-it-has-its-own-system-determi/2016-06-28>.

⁸ Peter Swire, et al., *Online Privacy and ISPs* (May 2016).

⁹ Cade Metz, *Comcast Trials Domain Helper Service/DNS Hijacker*, THE REGISTER, July 28, 2009, http://www.theregister.co.uk/2009/07/28/comcast_dns_hijacker/;

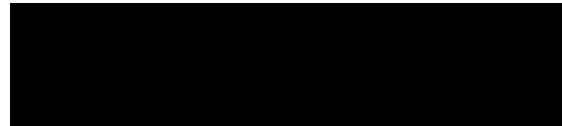
To be clear, I am far from unusual in decrying the state of online privacy and elaborating the useful role that Congress can serve in addressing this problem. Survey after survey reveals that consumers are dissatisfied with the level of privacy they enjoy online as well as hopeful that their elected officials will enact smart, measured new laws to address these concerns.¹⁰

In addition, policymakers have agreed, calling for new privacy laws for online activity. The White House issued a widely hailed 2012 call for a “consumer privacy bill of rights,” specifically urging Congress to codify these rights in new legislation.¹¹ Successive Chairs of the FTC, together with FTC Commissioners from both parties have urged Congress to enact new comprehensive privacy and data security legislation.¹² To date, Congress has not enacted any laws in response to these calls.

To be more specific, Congress should enact a sectoral privacy law for entities that possess precise geolocation information. It should enact a sectoral privacy law limiting the use of facial recognition systems. It should enact a law to regulate the activities of data brokers. Wise and measured proposals on each of these topics have been proposed but unfortunately have languished in recent Congresses. I am happy to elaborate on my support for specific bills, if you would find it useful.

Thank you once again for giving me the opportunity to express my opinions about these vital issues. I truly admire the hard work and thoughtfulness with which your subcommittee has been engaging with this vital topic.

Sincerely,

A large black rectangular redaction box covering the signature of Paul Ohm.

Paul Ohm

¹⁰ Berkeley Law, Berkeley Consumer Privacy Survey, <https://www.law.berkeley.edu/research/bclt/research/privacy-at-bclt/berkeley-consumer-privacy-survey/> (series of studies); Pew Research, Online Privacy and Safety, <http://www.pewresearch.org/topics/privacy-and-safety/> (collecting studies).

¹¹ <https://www.whitehouse.gov/sites/default/files/privacy-final.pdf>.

¹² *E.g.*, https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-balancing-privacy-and-innovation-does-presidents/120329privacytestimony.pdf; http://www.americanbar.org/news/abanews/aba-news-archives/2015/02/ftc_chair_edith_rami.html.