Perspectives from FSF Scholars
November 10, 2021
Vol. 16, No. 59

FTC Staff Report on ISP Privacy Practices: Understates Tools for Consumers, Underscores Need for Federal Legislation

by

Andrew Long *

At its October 21, 2021, Open Commission Meeting, the Federal Trade Commission released a staff report on the privacy practices of six Internet service providers (ISPs) and three affiliated digital advertisers. Properly understood as a critique of the "notice-and-consent" legal framework that governs data privacy today, the report alleges no specific violations of applicable laws, regulations, or the ISPs' publicly available privacy policies. Rather, it simply highlights the need for federal privacy legislation – a point that Free State Foundation scholars repeatedly have made.

Below, I highlight two noteworthy aspects of the report and its adoption. One, the report presents an incomplete and out-of-date picture regarding the extent to which encryption-based technologies – specifically, HTTPS, DNS-over-HTTPS, and VPNs – shield specifically from ISPs' view their customers' online activity.

Two, the Democrats on the Commission, Chair Lina M. Khan and Commissioner Rebecca Kelly Slaughter, each chose to leverage the report's release to discuss the appropriate regulatory classification of high-speed Internet access services under the Communications Act, a question

that falls squarely and exclusively within the FCC's jurisdiction. As explained below, this appears to be part of a troubling Biden Administration trend involving, to date, both the Treasury Department and the Department of Agriculture, to impose public utility-like net neutrality mandates on Internet service providers by employing legally dubious backdoor means.

The FTC report, "A Look At What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers," is based on responses to Orders to File Special Reports issued in August 2019 pursuant to Section 6(b) of the FTC Act. The inquiry targeted six ISPs – AT&T Mobility, Verizon Wireless, Charter Communications, Comcast Cable, T-Mobile, and Google Fiber – and three affiliated advertising companies.

Those advertising companies are AT&T's Appnexus Inc. (now operating as Xandr) and two entities affiliated with Verizon, Verizon Online LLC and Oath Americas Inc. (since rebranded as Verizon Media). Notably, and even though the report does acknowledge that (1) the advertising market is "dominated by Google, Facebook, and Amazon," and (2) Google Fiber's parent company Alphabet Inc. "accounted for 28.9% of all digital advertising revenue in the United States in 2020," Alphabet Inc. itself was not asked to respond.

The report, which concludes that "many of the ISPs in our study amass large pools of sensitive data, and that their uses of such data *could* lead to significant harms" (emphasis added), is organized around five rather prejudicially labeled categories: (1) Opacity; (2) Illusory Choices; (3) Lack of Meaningful Access; (4) Data Retention and Deletion; and (5) Accountability.

Even after conceding that "ISPs are small players in … the $152.72 billion U.S. digital advertising industry" and that "in 2020, the three largest players, Google, Facebook, and Amazon, received almost two-thirds of all U.S. digital advertising spend," the report nevertheless highlights privacy concerns – concerns, not violations of law, regulation, or privacy policies – specific to ISPs. The primary justification the report provides for doing so is the assertion that "many of the ISPs in our study have access to 100% of consumers' unencrypted Internet traffic." On its face, this statement is misleading. The reason for that is because the report minimizes, seemingly intentionally, the extent to which Internet traffic is encrypted.

As I described in "Maine's ISP-Only Privacy Law Will Not Protect Consumers," an April 2020 *Perspectives from FSF Scholars*, two widely used encryption-based technologies – HTTPS and DNS-over-HTTPS (DoH) – prevent ISPs from seeing what their customers are doing online. HTTPS encryption limits ISPs from gleaning anything more than the identity of the website a customer visits. DoH, meanwhile, obscures even that information. A third option, Virtual Private Networks (VPNs), provide those consumers concerned about ISP visibility into their online activity with yet another powerful security tool.

Citing an article from 2016, a lifetime ago in Internet time, the report claims that "more than 85% of the top 50 sites still failed to encrypt browsing by default." As I noted over 18 months ago in the *Perspectives* mentioned above, however, by early 2019, 87 percent of web traffic was encrypted. More recent data indicates that, as of October 2019, over 90 percent of web traffic was encrypted. Thus, the widespread use of HTTPS encryption, which appears to be approaching ubiquity, significantly shields the bulk of customer online activity from the view of ISPs.

DoH, meanwhile, goes a step further, encrypting the identity of the websites requested through what are known as domain name server (DNS) queries: that is, the messages sent to servers that translate domain names (for example, freestatefoundation.org) into IP addresses (in this instance, 34.83.19.155). As Jack Wallen, an online security expert, wrote for *TechRepublic* in September of this year:

> DNS-Over-HTTPS hides your DNS queries from third-party observers so they cannot sniff out your packets and see what you're searching for or what sites you're about to access. Most of the major web browsers allow you to enable this functionality, and it should be considered a must-do for every browser you use.

As I wrote last April, DoH is enabled in the Firefox browser by default. In a footnote, the FTC report does point out that "[a]t least one" of the six ISPs "has partnered with internet browsers and committed to deploying" DoH – but then states that, "since DoH is largely browser dependent, the breadth of its deployment is an open question and therefore, so is the impact that it will have on consumer internet privacy."

Another tool that privacy-conscious consumers can, and increasingly do, use are VPNs. As CNET recently explained, "[a] VPN keeps your internet traffic private and hidden from anyone looking to snoop on what you do online – whether it's your ISP, your employer, your school, network administrators, hackers on public Wi-Fi, web trackers or government agencies."

However, the report claims that "the prevalence of VPNs remains low, with only 6.26% of North American internet users adopting the technology" – but then goes on to state that "the pandemic has led to a surge in VPN adoption." According to a study released by Security.org on November 8, 2021, 41 percent of adult respondents "said they use a VPN for personal or business reasons." In 2020, that number was even higher: 49 percent. Contradicting the report's assertion, Security.org attributed that decline to the fact that, due to the pandemic, "many workers remain at home."

Thus, despite the report's attempts to establish a false equivalency as to the relative access that ISPs and edge providers have to personal online data, the technological reality is that (1) the vast majority of web sites today encrypt traffic using HTTPS (and therefore hide from ISPs all but the top-level domain names of the sites their customers visit); (2) DoH is a widely available tool that empowers consumers to cloak from their ISPs' view the entirety of their web traffic; and (3) VPNs, by the FTC's own account, are enjoying a "surge" in adoption.

By contrast, any data collection performed by the sites that ISPs' users visit, including those operated by Google, Facebook, and Amazon – the three Big Tech titans that, to quote the report, "dominate[]" the advertising market – are not similarly constrained by the use of these encryption-based tools, which are designed to secure online data only while in transit, not after it reaches its destination.

* * *

In the prepared text for her Oral Remarks, Commissioner Christine S. Wilson wrote that "[t]he FTC's ability to conduct industry studies using our 6(b) authority is one of the agency's unique strengths." She also expressed her belief that "oversight of ISPs for privacy and data security issues should remain at the FTC" and – most notably – her disappointment regarding her "colleagues' choice to detract from the significant findings that staff shared with the public today by injecting the highly controversial topic of net neutrality into the discussion."

In her Remarks, Chair Khan went out of her way to champion efforts by the FCC to "once again put in place the nondiscrimination rules, privacy protections, and other basic requirements needed to create a healthier market." Similarly, Commissioner Slaughter in her Remarks opined that the FCC should "return ISPs to their proper classification as telecom services under Title II."

Incidentally, the FTC is not the only federal entity to encroach upon the FCC's jurisdictional domain by weighing in on the issue of the regulatory treatment of high-speed Internet access services. For example, the Department of Agriculture recently published the Evaluation Criteria to be used when considering applications for funding under the ReConnect Loan and Grant Program. Pursuant to those criteria, applicants will receive preferential consideration, in the form of "points," if they agree to advance various problematic and partisan priorities – including 10 points "[f]or applicants that commit to net neutrality."

In response, a group of 13 Republican Senators, led by Roger Wicker (MS), Ranking Member of the Senate Commerce Committee, and John Thune (SD), Ranking Member of the Subcommittee on Communications, Media, and Broadband, on November 5, 2021, wrote to Department of Agriculture Secretary Tom Vilsack warning him that "[a]ny effort to impose unnecessary 'net neutrality' restrictions would be dangerous to our nation's dynamic broadband economy and threaten future investments in broadband infrastructure," pointing out the Department of Agriculture's lack of authority and expertise regarding the regulatory classification of broadband service, and calling upon the Secretary to overturn the misguided decision to prioritize projects that embrace "net neutrality."

Of note, this comes on the heels of the Treasury Department's troubling actions to bring the Biden Broadband Plan back to life via the "Guidance for the Coronavirus Capital Projects Fund for States, Territories & Freely Associated States" it promulgated in September, a topic I addressed in the Halloween-themed "Treasury Department Resurrects the Scary Biden Broadband Plan," a recent Free State Foundation *Perspectives*.

* Andrew Long is a Senior Fellow of the Free State Foundation, an independent**,** nonpartisan free market-oriented think tank located in Rockville, Maryland. The views expressed in this *Perspectives* do not necessarily reflect the views of others on the staff of the Free State Foundation or those affiliated with it.

Further Readings

"Privacy Recap: Senate Commerce Committee Holds Hearing on Data Privacy; Op-Ed Authors Oppose FTC Privacy Rulemaking," *FSF Blog* (October 1, 2021).

"FTC Commissioner Wilson Recruits Student Researchers to Inform and Inspire Efforts to Pass a Federal Data Privacy Law," *FSF Blog* (September 29, 2021).

"Congressional Testimony of FTC Commissioner Wilson Addresses Agency Processes, Section 13(b), and Federal Privacy Legislation," *FSF Blog* (July 29, 2021).

"Inconsistent State Data Privacy Laws Increase Confusion and Costs," *Perspectives from FSF Scholars*, Vol. 16, No. 14 (March 16, 2021).

"Ohio Legislators Introduce the Latest Comprehensive State Data Privacy Bill," *FSF Blog* (July 20, 2021).

"Exhibit C(O) in the Case for a Federal Data Privacy Law: The Colorado Privacy Act," *FSF Blog* (July 15, 2021).

"Alaska Is the Latest State to Propose a Data Privacy Law," *FSF Blog* (April 9, 2021).

"Colorado Lawmakers Introduce Data Privacy Bill," *FSF Blog* (April 6, 2021).

"Inconsistent State Data Privacy Laws Increase Confusion and Costs," *Perspectives from FSF Scholars*, Vol. 16, No. 14 (March 16, 2021).

"Florida Vies for Bronze in Race to Create Patchwork of State Data Privacy Laws," *FSF Blog* (March 12, 2021).

"Virginia's Consumer Data Protection Act Soon Could Become Law," *FSF Blog* (February 5, 2021).

"California Voters Approve the California Privacy Rights Act: A Detailed Analysis of Its Requirements and Impact," *Perspectives from FSF Scholars*, Vol. 15, No. 60 (November 17, 2020).

"Privacy Recap: Senate Commerce Committee Holds Hearing, Republican Members Introduce SAFE DATA Act," *FSF Blog* (September 25, 2020).

"Federal Privacy Legislation: Bipartisan Discussions Devolve into Dueling Drafts," *Perspectives from FSF Scholars*, Vol. 14, No. 42 (December 4, 2019).

"California's Privacy Law: Recent Developments Underscore the Need for Preemptive Federal Law," *FSF Blog* (November 21, 2019).

"California's Heavy-Handed Approach to Protecting Consumer Privacy: Exhibit A in the Case for Federal Preemption," *Perspectives from FSF Scholars*, Vol. 14, No. 35 (October 28, 2019).