November 4, 2019

The Honorable Frank Pallone
Chairman
Committee on Energy and Commerce
U.S. House of Representatives

The Honorable Greg Walden
Ranking Member
Committee on Energy and Commerce
U.S. House of Representatives

The Honorable Jan Schakowsky
Chairwoman
Subcommittee on Consumer Protection
and Commerce
U.S. House of Representatives

The Honorable Cathy McMorris Rodgers
Ranking Member
Subcommittee on Consumer Protection
and Commerce
U.S. House of Representatives

The Honorable Michael F. Doyle
Chairman
Subcommittee on Communications
and Technology
U.S. House of Representatives

The Honorable Robert E. Latta
Ranking Member
Subcommittee on Communications
and Technology
U.S. House of Representatives

Dear Chairs and Ranking Members:

We are writing to express our concern about the privacy and security practices of internet service providers (ISPs), particularly as they relate to the domain name services (DNS) provided to American consumers. Our recent experience in rolling out DNS over HTTPs (DoH) - an important privacy and security protection for consumers - has raised questions about how ISPs collect and use sensitive user data in their gatekeeper role over internet usage. With this in mind, a congressional examination of ISP practices may uncover valuable insights, educate the public, and help guide continuing efforts to draft consumer privacy legislation.

During the last two years, Mozilla, in partnership with other industry stakeholders, has worked to develop, standardize, and deploy DoH, a critical security improvement to the underlying architecture of the internet. A complementary effort to our work to fight ubiquitous web tracking, DoH will make it harder to spy on or tamper with users' browsing activity and will protect users from DNS providers - including ISPs - that can monetize

personal data.[1] We believe that such proactive measures have become necessary to protect users in light of the extensive record of ISP abuse of personal data, including the following incidents:

- Providers sold the real-time location data of their mobile broadband customers to third parties without user knowledge or meaningful consent.[2] In one particular case, an intermediary was found to be selling particularly sensitive GPS data, which can pinpoint the location of users within a building, for over five years.[3]

- ISPs have repeatedly manipulated DNS to serve advertisements to consumers.[4] Comcast has previously injected ads to users connected to its public wi-fi hotspots, potentially creating new security vulnerabilities in websites.[5] And last year, CenturyLink injected ads for its paid filtering software and disabled the internet access of its users until they acknowledged the offer.[6]

- Verizon tracked the internet activity of over 100 million users without their consent through "supercookies" that could not be deleted or circumvented.[7] This allowed Verizon to closely monitor the sites that users visited and catalogue their interests without their knowledge.[8]

- AT&T operated a program that required users to pay an extra $29 per month to opt out of the collection and monetization of their browsing history for targeted ads.[9] While the

---

[1] Marshall Erwin, *DNS-over-HTTPS Policy Requirements for Resolvers*, Mozilla Security Blog, Apr. 9, 2019, https://blog.mozilla.org/security/2019/04/09/dns-over-https-policy-requirements-for-resolvers/.

[2] Joseph Cox, *Hundreds of Bounty Hunters Had Access to AT&T, T-Mobile, and Sprint Customer Location for Years*, Motherboard, Feb. 6, 2019, https://www.vice.com/en_us/article/43z3dn/hundreds-bounty-hunters-att-tmobile-sprint-customer-location-data-years; Jennifer Valentino-DeVries, *Service Meant to Monitor Inmates' Calls Could Track You, Too*, N.Y. Times, May 10, 2018, https://www.nytimes.com/2018/05/10/technology/cellphone-tracking-law-enforcement.html.

[3] Cox, *supra* note 2.

[4] *See* Nicholas Weaver et al., Redirecting DNS for Ads and Profit, USENIX Workshop on Free and Open Communications on the Internet (Aug. 8, 2011), available at https://www.icsi.berkeley.edu/pubs/networking/redirectingdnsforads11.pdf (detailing how ISPs have manipulated DNS to redirect consumers from error pages to ad servers and created potential security risks).

[5] David Kravets, *Comcast Wi-Fi serving self-promotional ads via JavaScript injection*, Ars Technica, Sept. 8, 2014, https://arstechnica.com/tech-policy/2014/09/why-comcasts-javascript-ad-injections-threaten-security-net-neutrality/.

[6] Jon Brodkin, *CenturyLink blocked its customers' Internet access in order to show an ad*, Ars Technica, Dec. 17, 2018, https://arstechnica.com/tech-policy/2018/12/centurylink-blocks-internet-access-falsely-claims-state-law-required-it/.

[7] *See* Craig Timberg, *Verizon, AT&T tracking their users with 'supercookies'*, Wash. Post, Nov, 3, 2014, https://www.washingtonpost.com/business/technology/verizon-atandt-tracking-their-users-with-super-cookies/2014/11/03/7bbbf382-6395-11e4-bb14-4cfea1e742d5_story.html?utm_term=.d275117a9504; Jacob Hoffman-Andrews, *Verizon Injecting Perma-Cookies to Track Mobile Customers, Bypassing Privacy Controls*, Electronic Frontier Foundation (Nov. 3, 2014), https://www.eff.org/deeplinks/2014/11/verizon-x-uidh.

[8] Hoffman-Andrews, *supra* note 7.

[9] Jon Brodkin, *AT&T to end targeted ads program, give all users lowest available price*, Ars Technica, Sept. 30, 2016, https://arstechnica.com/information-technology/2016/09/att-to-end-targeted-ads-program-give-all-users-lowest-available-price/.

company ended the program after public criticism, it has considered reviving it in the current deregulated environment.[10]

Unsurprisingly, our work on DoH has prompted a campaign to forestall these privacy and security protections, as demonstrated by the recent letter to Congress from major telecommunications associations.[11] That letter contained a number of factual inaccuracies. These have been examined in detail by others and as such will not be given an in-depth treatment here.[12] Nonetheless, it is important to highlight the underlying premise of that letter: telecommunications associations are explicitly arguing that ISPs need to be in a position to collect and monetize users' data.[13] This is inconsistent with arguments made just two years earlier regarding whether privacy rules were needed to govern ISP data use.[14]

With the 2017 Congressional repeal of the Broadband Privacy Order, a substantial gap in consumer privacy protection was created. That gap still exists today. ISPs are people's gateway to the Internet. That gateway can serve as a data collection point, providing ISPs with unique access into sensitive browsing information.[15] That is why broadband privacy rules would have required ISPs to get clear consent to use and share subscribers' information. However, those rules are no longer in place.

Our approach with DoH attempts to close part of this regulatory gap through technology and strong legal protections for user privacy. Mozilla's policy establishes strict requirements for potential Firefox DNS resolvers, including requiring that data only be retained for as long as is necessary to operate the resolver service, that data only be used for the purpose of operating that service, and that partners maintain a privacy notice specifically for the resolver that

[10] Karl Bode, *AT&T May Soon Return To Charging Broadband Subscribers More For Privacy*, Techdirt, Jun. 26, 2017, https://www.techdirt.com/articles/20170626/05434737666/att-may-soon-return-to-charging-broadband-subscribers-more-privacy.shtml.

[11] *But see* Letter from Consumer Reports, Electronic Frontier Foundation, and the National Consumers League to Senate and House Committee Chairmen and Ranking Members (Oct. 22, 2019), available at https://www.eff.org/files/2019/10/22/effcr_and_ncl_letter_on_doh_to_congress.pdf (outlining factual errors and misrepresentations made by internet service providers in correspondence with Congress regarding the deployment of DoH). *See also* Joseph Cox, *Comcast Is Lobbying Against Encryption That Could Prevent it From Learning Your Browsing History*, Motherboard, Oct. 23, 2019, https://www.vice.com/en_us/article/9kembz/comcast-lobbying-against-doh-dns-over-https-encryption-browsing-data.

[12] Timothy B. Lee, *Why big ISPs aren't happy about Google's plans for encrypted DNS*, Ars Technica, Sept. 30, 2019, https://arstechnica.com/tech-policy/2019/09/isps-worry-a-new-chrome-feature-will-stop-them-from-spying-on-you/.

[13] Letter from NCTA, CTIA, and US Telecom to Senate and House Committee Chairmen and Ranking Members (Sept. 19. 2019), available at https://www.ncta.com/sites/default/files/2019-09/Final%20DOH%20LETTER%209-19-19.pdf ("[DoH] could inhibit competitors and possibly foreclose competition in advertising and other industries.").

[14] One argument made to justify the repeal was that privacy rules were unnecessary because technology developments, such as the use of virtual private networks (VPNs), were making it harder for ISPs to access DNS data. Now that those rules have been repealed, the same ISPs are fighting to stop the deployment of technologies that would remove access to that data.

[15] Aaron Rieke et al., Upturn, What ISPs Can See (2016), available at https://www.upturn.org/reports/2016/what-isps-can-see/ (finding that collection and use of DNS queries is "practical, cost effective, and happens today on ISP networks").

publicly attests to data collection and policies. Unfortunately, ISPs often do not maintain privacy notices for their DNS services. As a result, their policies are opaque to users - it is unclear what data is being retained, how it is being used, or who it is being shared with.

At Mozilla, we believe that to truly protect privacy, a combination of technical and regulatory solutions must be put in place. Over the last year, we have launched privacy features in the Firefox browser while strongly advocating for federal privacy legislation. We believe that more information regarding ISP practices could be useful to the Committee as it continues its deliberations on this front, and we encourage the Committee to publicly probe current ISP data collection and use policies.[16]

Sincerely,

Marshall Erwin

Senior Director of Trust and Security
Mozilla Corporation

[16] While the FTC is currently conducting its own investigation into ISP privacy practices, a parallel congressional investigation can serve a valuable purpose by bringing these issues into broader public view and providing a platform for Members to ask specific questions that may help guide federal privacy legislation.