October 22, 2019

The Honorable Lindsey Graham
Chairman
Committee on the Judiciary
United States Senate
Washington, DC 20510

The Honorable Dianne Feinstein
Ranking Member
Committee on the Judiciary
United States Senate
Washington, DC 20510

The Honorable Jerrold Nadler
Chairman
Committee on the Judiciary
United States House of Representatives
Washington, DC 20515

The Honorable Doug Collins
Ranking Member
Committee on the Judiciary
United States House of Representatives
Washington, DC 20515

The Honorable Roger Wicker
Chairman
Committee on Commerce, Science,
and Transportation
United States Senate
Washington, DC 20510

The Honorable Maria Cantwell
Ranking Member
Committee on Commerce, Science,
and Transportation
United States Senate
Washington, DC 20510

The Honorable Frank Pallone
Chairman
Committee on Energy and Commerce
United States House of Representatives
Washington, DC 20515

The Honorable Greg Walden
Ranking Member
Committee on Energy and Commerce
United States House of Representatives
Washington, DC 20515

The Honorable Ron Johnson
Chairman
Committee on Homeland Security
and Governmental Affairs
United States Senate
Washington, DC 20510

The Honorable Gary Peters
Ranking Member
Committee on Homeland Security
and Governmental Affairs
United States Senate
Washington, DC 20510

The Honorable Bennie G. Thompson
Chairman
Committee on Homeland Security
United States House of Representatives
Washington, DC 20515

The Honorable Mike Rogers
Ranking Member
Committee on Homeland Security
United States House of Representatives
Washington, DC 20515

Dear Chairmen and Ranking Members,

We write in response to a recent letter from NCTA, CTIA, and US Telecom (the "ISP Letter") about an Internet privacy technology called DNS-over-HTTPS ("DoH"). As privacy and consumer advocates, we've been excited about the progress of this technology and the ways that it can help protect Internet users.

Unfortunately, the ISP Letter misstated some aspects of DoH, especially the deployment plans of major browsers and the relative risks and benefits of those plans.

DNS over HTTPS Technology Carries Global Benefits for the Internet

DoH would result in greater security and privacy for users. We see DoH as part of an important trend toward the greater use of encryption on the Internet—remedying a situation in which all sorts of sensitive user data were exposed to an enormous range of eavesdroppers. As we've often stressed, sensitive information includes not only the content of pages that users access (now increasingly protected by encryption through HTTPS), but also the names of the sites they access. This can reveal sensitive personal information about users' political, religious, medical, or sexual affiliations and interests—even including their relationships with particular religious congregations, political parties, or medical providers. In today's Internet, this information is often highly exposed, both to Internet infrastructure providers and to people simply sharing a wifi network.

DoH would prevent some methods of censorship by authoritarian regimes.
To put in context how these vulnerabilities are exploited and why DoH represents a technological breakthrough for Internet freedom, authoritarian regimes that run their own ISP for their citizens will lose significant control over user activity with systemic adoption of DoH.
Today it is also possible for malicious DNS resolvers or on-path routers to tamper with DNS requests, blocking users from accessing sites through censorship. DoH prevents this, which is vitally important to protecting freedom of expression in countries like Iran and China that don't allow for the same liberties of speech and assembly we regularly enjoy in the United States.

Countries like China and Turkey have also used control over DNS as a means of blocking their citizens' access to foreign websites, a method of censorship which will be made much more difficult by the availability of DoH.

DoH's Origins Reach Well Beyond Google

DoH is one of a set of technical upgrades that helps address these ongoing privacy leakages. It was created through an open standards process at the IETF lasting over two years and including contributions and input from many different sectors[1]. It is now being implemented in a variety of software and by a number of different kinds of ISPs and other Internet organizations.

Based on our understanding of plans from Google and Mozilla—the browser makers on the leading edit of this issue—we believe the ISP Letter misrepresents the facts, risks, and benefits of their deployment plans. The ISP Letter is especially preoccupied with competition and centralization harms if Google's popular Chrome browser and Android operating system were set to automatically use Google's public DoH service. In this case, Google would get access to a large volume of information about the sites that individual Internet users visit, including non-Google sites. This kind of Internet centralization would be a concern in general; further, the use of this data for advertising and profiling purposes could be both a privacy and competition concern. But these particular effects **are not in any way inherent to DoH itself** and **do not reflect Google's publicly-announced plans with respect to its use of the technology**[2]. Public documents state that Google will make Chrome attempt to use *individual ISPs' own DoH services,* which means if all DNS providers adopt DoH, which would yield the greatest privacy benefit to Internet users, then nothing will change after Google adopts DoH. Furthermore, a user can always indicate a different preferred DoH resolver—not just Google's 8.8.8.8 service, as dozens currently exist (Ongoing work at IETF is standardizing ways for ISPs to inform users' devices that an official ISP-provided DoH resolver service is available.)

---

[1] See https://datatracker.ietf.org/wg/doh/ (IETF homepage for DoH working group); https://tools.ietf.org/html/rfc8484 (DoH standard finalized in October 2018).

[2] The most detailed statement of Google's plans is available at https://docs.google.com/document/d/15Ss0OaJeb-T3g2RMwgikHvsC0CPKd-MLeGeetv1wYY4/, although other public statements from Google are also available.

We think this is an appropriate and reasonable policy, and it will help users get privacy benefits from DoH, while **not giving Google any new information about Chrome users' browsing**, except for those users who individually prefer Google's DNS service to their ISPs' services. We strongly encourage the ISPs to preserve the status quo by adopting DoH on their own DNS resolvers. They can do this themselves immediately rather than run to Congress for intervention that is both unnecessary and counterproductive to user privacy.

Mozilla, the developer of the Firefox browser, has a different plan for DoH support in its browser: by default, Firefox users in the U.S. will use a DoH service provided by Cloudflare ("1.1.1.1"). This plan involves different costs and benefits. By switching users from their existing DNS provider, it will ensure that a larger portion of the user base receives the security benefits of DoH. It does however provide users' data to a different party. Cloudflare has agreed to a strict privacy policy with respect to its use of the resulting data, including never using it for any advertising or user profiling purposes whatsoever[3]. This policy is more privacy-protective than many U.S. ISPs' existing privacy policies; Chrome users who prefer it could individually opt in to using this service, or any of several dozen public DoH resolver services.[4] Mozilla has stated that is also exploring ways to easily allow users to choose among other DoH services, including those provided by the users' ISPs or by other public providers that agree to strong privacy protections for user data.

Systemic Implementation of DoH Should be Supported by Congress

It is understandable that your Committees would want to scrutinize whether or how Google is using its market dominance, and we have no objection to such inquiries. Indeed, we have supported Congressional antitrust inquiries[5] and recommended that the legislature take a more active role in reinvigorating Internet competition (as well as broadband access competition)[6]. However, the information provided to Congress is not reflective of what DoH represents, which is a long-overdue Internet privacy upgrade that can be used by *any* DNS

---

[3] See https://developers.cloudflare.com/1.1.1.1/commitment-to-privacy/privacy-policy/firefox/ (Cloudflare's policy) as well as https://wiki.mozilla.org/Security/DOH-resolver-policy (criteria for a public resolver to be recommended by Mozilla).

[4] List of publicly available servers can be found at https://github.com/curl/curl/wiki/DNS-over-HTTPS#publicly-available-servers.

[5] See https://www.eff.org/deeplinks/2019/09/senate-antitrust-hearing-explores-big-techs-merger-mania

[6] See https://www.eff.org/issues/competition

resolver service. The various concerns raised by the ISP Letter are not reasons to hold up the deployment of this technology as they are premised on the idea that they have a right to exposed user data.

We hope all of the entities that connect users to the Internet and provide services over the Internet implement DoH on their own existing DNS services. Everyone involved should work towards a future in which users can easily choose the encrypted DNS resolver services that they feel best meet their needs.

A long-overdue technological shift toward online privacy is underway. Congress should not aim to hinder this shift and leave the Internet less secure out of sympathy to the commercial interests of those who have exploited insecurities. Any privacy gaps that remain over time should be remedied through state and federal legislation expanding individuals' remedies for privacy breaches.

Congress should support systemic adoption of DoH in order to close up one of the largest privacy gaps remaining on the Internet while furthering the cause of Internet freedom in many parts of the world in dire need of it.

Sincerely,

Consumer Reports
Electronic Frontier Foundation
National Consumers League