September 19, 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

Chairmen and Ranking Members:

We would like to bring to your attention an issue that is of concern to all our organizations. Google is beginning to implement encrypted Domain Name System lookups into its Chrome browser and Android operating system through a new protocol for wireline and wireless service, known as DNS over HTTPS (DoH). If not coordinated with others in the internet ecosystem, this could interfere on a mass scale with critical internet functions, as well as raise data competition issues. We ask that the Committee seek detailed information from Google about its current and future plans and timetable for implementing encrypted DNS lookups, as well as a commitment not to centralize DNS lookups by default in Chrome or Android without first meeting with others in the internet ecosystem, addressing the implications of browser- and operating-system-based DNS lookups, and reaching consensus on implementation issues surrounding encrypted DNS.

DNS acts as a telephone directory for the Internet and has historically been broadly dispersed, on a de-centralized "local basis." When an end user types in the name of a website (*e.g.*, www.wikipedia.org), the end user's Internet Service Provider or other provider performs a "DNS look-up" by consulting a directory that translates the website name into a string of numbers that is used to connect the end user to the website. End users can choose a DNS provider other than their ISP, and many customers do so, in particular enterprise customers who manage their own private networks.

Google is unilaterally moving forward with centralizing encrypted domain name requests within Chrome and Android, rather than having DNS queries dispersed amongst hundreds of providers. When a consumer or enterprise uses Google's Android phones or Chrome web browser, Android or Chrome would make Google the encrypted DNS lookup provider by default and most consumers would have limited practical knowledge or ability to detect or reject that choice. Because the majority of worldwide internet traffic (both wired and wireless) runs through the Chrome browser or the Android operating system, Google could become the overwhelmingly predominant DNS lookup provider.

While we recognize the potential positive effects of encryption, we are concerned about the potential for default, centralized resolution of DNS queries, and the collection of the majority of worldwide DNS data by a single, global internet company. By interposing itself between DNS providers and the users of the Chrome browser (> 60% worldwide share) and Android phones (> 80% worldwide share of mobile operating systems), Google would acquire greater control over user data across networks and devices around the world. This could inhibit competitors and possibly foreclose competition in advertising and other industries.

Moreover, the centralized control of encrypted DNS threatens to harm consumers by interfering with a wide range of services provided by ISPs (both enterprise and public-facing) and others. Over the last several decades, DNS has been used to build other critical internet features and functionality including: (a) the provision of parental controls and IoT management for end users; (b) connecting end users to the nearest content delivery networks, thus ensuring the delivery of content in the fastest, cheapest, and most reliable manner; and (c) assisting rights holders' and law enforcement's efforts in enforcing judicial orders in combatting online piracy, as well as law enforcement's efforts in enforcing judicial orders in combatting the exploitation of minors. Google's centralization of DNS would bypass these critical features, undermining important consumer services and protections, and likely resulting in confusion because consumers will not understand why these features are no longer working. This centralization also raises serious cybersecurity risks and creates a single point of failure for global Internet services that is fundamentally at odds with the decentralized architecture of the internet. By limiting the ability to spot network threat indicators, it would also undermine federal government and private sector efforts to use DNS information to mitigate cybersecurity risks.

For these reasons, we ask that the Committee call upon Google not to impose centralized, encrypted DNS as a default standard in Chrome and Android. Instead, Google should follow the Internet Engineering Task Force best practice of fully vetting internet standards, and the internet community should work together to build consensus to ensure that encrypted DNS is implemented in a decentralized way that maximizes consumer welfare and avoids the disruption to essential services identified above.

Sincerely,

CTIA
NCTA – The Internet & Television Association
US Telecom – The Broadband Association