September 19, 2019
TO: NCOSE Friends and Allies
FR: National Center on Sexual Exploitation (NCOSE)
RE: Online Child Safety Jeopardized as Google Begins Rerouting and Centralizing DNS traffic

Our Request
We call on Congress, the FBI, the Federal Trade Commission, and the National Association of Attorneys General to recognize the potentially serious impacts that unilateral implementation of a DoH protocol by Google, together with Mozilla/Cloudflare, will have on efforts to: 1) Protect children online; 2) Prohibit the spread of child sexual abuse images (i.e., child pornography); and 3) Identify criminals engaged in child sexual abuse image production and distribution. The process, as devised by Google and Mozilla/Cloudflare, fundamentally changes the flow of Internet traffic by rerouting and centralizing all web-lookup traffic, by default, to their preferred DNS resolvers, potentially breaking many DNS-based controls. The magnitude of potential threats to public safety requires public officials to take immediate steps to delay the launch until thorough risk assessments have been conducted, and there is reasonable assurance that tools and systems to protect children and others from online sexual exploitation remain in place, or are developed and implemented as necessary.

Background
- The Domain Name System (DNS) is the system by which we retrieve information on the Internet through domain names like Congress.gov. Commonly referred to as the “phone book” of the Internet, the DNS converts website names to Internet Protocol (IP) addresses.
- The current system is open and decentralized; Internet Service Providers (ISPs) route, or direct, Internet traffic based on the visibility of user domain-name requests for specific sites. This “architecture” facilitates both policing and filtering. Internet safety tools and filters used by parents, libraries, and schools often rely on the ability of ISPs to “see” DNS addresses, in order to keep children safe online.
- Internet security experts are working to increase Internet privacy and security—necessary and worthy goals—by securing domain name searches, which at present can be monitored, intercepted, and misdirected. One option developed by the Internet Engineering Task Force (IETF) is a new protocol, DNS over HTTPS (DoH), which encrypts user domain-name queries over a secure, HTTPS connection to a DNS server, rather than by a standard unencrypted DNS connection.
- Key browser and mobile operating system providers are set to deploy DoH on a centralized basis. This will dramatically change the Internet by rerouting web traffic in ways that could make some child protection tools and filters obsolete.

Google’s Current Plan
- Google intends to roll out its DoH protocol as the default setting on its Chrome browser starting October 22. Google is also poised to implement this system on Android devices. Mozilla Firefox, in partnership with Cloudflare, is expected to launch DoH in late September. Together these companies hold approximately 70% of the browser market share.
- Google appears to be rolling out this protocol without investing time or research into analyzing its weaknesses, without taking into account its impact on industry stakeholders, and without assessing how to protect children under a new system. A recent statement by Google suggests it
is now taking some steps to mitigate potential negative impacts. However, neither Google nor Mozilla/Cloudflare have adequately tested the system or engaged with stakeholders to ensure that their implementation of DoH preserves child protection tools and systems.

The Problem

- All search activity using Google browsers will be encrypted and hidden from everyone—including law enforcement—except Google. Google will in effect, encrypt all information funneled through its products and direct it to land on its own server where Google will house all of our data. Thus, DNS will be centralized by one major entity: Google.

- Because this iteration of DoH will make it harder to identify illegal content normally blocked by the ISPs, it could disrupt the way many tools function to protect children in homes, libraries, and schools. Since all domain-name queries will be encrypted, traditional tools developed for child safety may be broken.

- Experts have also warned of the inability to fulfill government-mandated regulations and court orders, as the centralized location of DNS resolvers will likely be outside of their jurisdictional control. Law enforcement’s ability to conduct the most basic web investigations without turning to Google/Mozilla and relying on their cooperation will be drastically impacted. This is particularly concerning considering Google’s apparent track record of protecting Backpage.com, now under federal prosecution for sex trafficking, as well as Cloudflare’s practice of keeping data for just 24 hours, acknowledgement of breaking U.S. law, and its public statements pledging resistance to legislative or jurisdictional pressures.

- Countless images of child sexual abuse victims could potentially become widely accessible.

- There are also serious security risks that implementation of this iteration of DoH poses. Although Google will no doubt claim it is adopting its protocol in the name of privacy and security, the system could break malware protections, including programs used by schools. In effect, Google is using the security issue to take control of massive amounts of financially valuable, personal information.

- In the United Kingdom, members of parliament considered these issues and, together with the Internet Watch Foundation, pushed back against Google. As a result, Google has postponed UK/European implementation, focusing efforts on North America.

Conclusion

- The implementation by Google and Mozilla/Cloudflare of such a significant restructuring of Internet operations without full consideration of the public impact and potential harms is both arrogant and irresponsible. The safety and wellbeing of children is not a tech “experiment” we can entrust to these corporations. All stakeholders need to be involved in the implementation; child safety must no longer be an afterthought to the tech industry.

- In light of the magnitude of potential threats to public safety, public officials should take all available measures to delay the current implementation of DoH as devised by Google and Mozilla/Cloudflare until full risk assessments have been conducted, and the public can be assured that effective tools and systems to protect children and others from online sexual exploitation have been developed, tested, and implemented.

2 Thomas Claburn, “Mozilla Firefox to Being Slow Rollout of DNS-over-HTTPS by Default at the End of the Month,” (September 9, 2019), theregister.co.uk/2019/09/09/mozilla_firefox_dns.

3 Shane Tews, “Should Big Tech be the Sole Operator of the Internet’s Domain Name Infrastructure” (June 25, 2019), aei.org/publication/should-big-tech-be-the-sole-operator-of-the-internets-domain-name-infrastructure.


7 Fred Langford, “DNS over HTTPS: Why We’re Saying DoH could be Catastrophic,” Internet Watch Foundation (July 17, 2019), iwf.org.uk/news/dns-over-https-why-we’re-saying-doh-could-be-catastrophic.

8 Tews, ibid.

9 Doffman, ibid; Tews, ibid; Andy Fidler, “Potential ISP Challenges with DNS over HTTPS,” *BT Technology*, (April 9, 2019), indico.uknof.org.uk/event/46/contributions/668/attachments/898/1109/UKNOF43_Potential_ISP_challenges_with_DNS_over_HTTPS_Issue_1A_050419.pdf.


16 Tews, ibid.