September 17, 2019

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

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

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

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

Dear Chairmen and Ranking Members:

The undersigned advocacy organizations write to bring to your attention a potentially dangerous new plan by Google, Mozilla, and others that could exacerbate the spread of exploitative content on the Internet, including, but not limited to, online grooming for sexual abuse and sex trafficking and the solicitation and distribution of child sexual abuse images (i.e., child pornography). These changes would also make it more difficult to filter harmful content using, for example, parental controls.

While regulators and watchdogs across the globe are actively working to restrict the spread of exploitative content online, we have recently learned that this plan, which is scheduled to be implemented beginning this month in the United States, could do the opposite: Make it exceedingly difficult to find and prevent online crimes against children.

Known as DNS over HTTPS (DoH), the plan backed primarily by Google, and in partnership with Mozilla/Cloudfare, is being pitched as a privacy technology to make web surveillance more difficult through encryption of DNS queries and by masking them as encrypted web traffic. DNS, often described as the telephone directory for the Internet, is the system through which an Internet web address such as House.gov is resolved to the underlying IP address that computers use to route the request (143.231.249.141).

Historically, the DNS functionality has been dispersed among many players around the globe on a de-centralized basis, a key feature of the Internet's design that has helped make it highly resilient over the past few decades. These players have included third-party DNS providers, network operators, and ISPs. But under the new centralized and encrypted DoH plan, a small handful of players led by Google can, in essence, take over DNS resolution for the overwhelming majority of DNS requests on the Internet each day.

Moreover, these companies plan to accomplish this by imposing it on users by default. Google, for instance, would eventually encrypt all DNS traffic from users of its Android operating system and Chrome browser, thus making the company *the* centralized encrypted DNS provider for the majority (70% in the U.S.) of the Internet.

Last May, in the United Kingdom, Internet safety watchdogs and the National Cyber Security Centre initiated emergency crisis talks with Google, Mozilla, and others, fearing that the companies' unilateral implementation of DoH would make it impossible to detect and block harmful material, including child-abuse images and terrorist propaganda.

The Internet Watch Foundation (IWF), a U.K.-based charity focused on minimizing the online availability of child sexual abuse content (also known as child pornography), has warned that this planned implementation of DoH's encryption protocol could be catastrophic for two reasons: 1) perpetuating online child abuse by making online crimes against children harder to track by law enforcement and Internet watchdogs, and; 2) making it harder to remove illegal content normally blocked by network operators, ISPs, and other third-party DNS providers under British law.

Fred Langford, the deputy CEO of IWF remarked that under the proposed DoH plan, millions of images and videos of child sexual abuse could suddenly be unshielded from public view. Currently, IWF provides ISPs and investigators a "block list" of live webpages of child sexual abuse used by DNS resolvers to prevent millions of criminal images from being made available on the Internet. Langford believes that DoH's forced and centralized encryption could soon render such tools obsolete by hiding user "requests," bypassing filters and parental controls, and making globally criminal material freely accessible.

Here in the U.S., under the current de-centralized DNS regime, Internet watchdogs and law enforcement can, with appropriate court orders, ask those provisioning DNS for vitally important information – what websites are hosting child sexual abuse images, for instance.

While in theory the same information could be requested from Google and Mozilla/Cloudflare under a DoH regime, the forced encrypted nature of the DNS requests may make it impossible for these companies to assist legitimate investigations or even block illegal content even if they wanted to, given the short period of time they purportedly retain logs. Cloudflare, for instance, has previously said that it

only logs DNS requests for 24 hours before deleting them. Additionally, some existing controls in use today by parents and schools will no longer work, creating confusion and allowing harmful illegal content to spread before solutions can be formulated.

To be clear, our aim is not to demonize technology, and we clearly recognize that Internet users' data should be secure. Furthermore, we are not calling for DoH to be banned, and we acknowledge that Internet encryption can serve useful security and privacy purposes.

While Google and others are rightly striving to protect privacy, they have failed to prioritize child safety by not adequately accounting for the potential unintended consequences of encryption. Although Google claims filtering technology will be unaffected by these rollouts, third party technology, child development, sexual exploitation, and law enforcement experts are alarmed by the rollout of these changes without sufficient subject matter consultation on whether those claims will prove accurate.

We therefore strongly urge you to look into the unforeseen consequences of the plan by Google, Mozilla/Cloudfare, and others to initiate DoH technology and seek ways to delay its implementation until potential unintended consequences to child safety have been thoroughly investigated and addressed.

Sincerely,

Craig Cobia
Co-Founder
Citizens for Decency, Idaho

Erin Walker & Chelsea Winterholler
Co-Directors
End Exploitation Montana, Montana

Benjamin Nolot
Founder & CEO
Exodus Cry, California

Bethenee Syversen
Founder & Executive Director
ExPOSE, New Hampshire

Katey McPherson
Founder
Get Screen Smart, Utah

Heather Cowan
Owner
Kids Go For Gold, Utah

Melody Bergman
Founder
Media Savvy Moms, Virginia

Patrick Truman
President & CEO
National Center of Sexual Exploitation, Washington, DC

Jesse Siegand & Sarah Siegand
Co-Founders
Parents Who Fight, Tennessee

Brittany Homer
Creator & Host
Raising Today's Kids, Montana

Vauna Davis
Founder & Director
Reach 10, Utah

Staci Sprout
LICSW, CSAT, Owner r.evolution psychotherapy, Author of
Naked in Public: A Memoir of Recovery From Sex Addiction And Other Temporary Insanities
Washington State

Derek VanLuchene
Founder & President
Ryan United, Montana

Linda Smith (U.S. Congress 1994-1998)
Founder & President
Shared Hope International, Vancouver, WA, Washington, DC

Robin Reber
Admissions Director
Star Guide Wilderness, Utah

Stacie Rumenap
President
Stop Child Predators, Washington, DC

Autumn Burris
Founder & Executive Director
Survivor's for Solutions, Colorado

Susan Ingram
President
Walk Her Home, Pennsylvania

Kimberly Perry
Founder
We Stand Guard, North Carolina

Deanna Lambson
Founder & Director
White Ribbon Week, Utah