CDT comments on Mozilla DoH implementation

The Center for Democracy & Technology (CDT) is a non-partisan, non-profit U.S.-based civil society organization that works globally to defend human rights and civil liberties online. For 25 years CDT has played a leading role in shaping the policies, practices, and norms that have empowered individuals to more effectively use the internet as speakers, entrepreneurs, and active citizens. CDT brings legal and technical expertise, thought leadership, and coalition-building skills to its work with domestic and global policy institutions, regulators, standards bodies, governance organizations, and courts.

As we have become increasingly aware that internet use, in particular web browsing, exposes user data that is monetised by companies and can be used by censorious regimes to implement online blocking and filtering, key internet infrastructure providers have been working hard to update the Domain Name System (DNS) to make internet use more privacy-respecting and secure for end users. CDT supports these updates because they serve the public interest by improving the privacy and security of the internet.

We respectfully submit the following comments to Mozilla, the creator of the FireFox Browser, on its technical implementation of private DNS protocols and, importantly, its supporting policy approach, including its Trusted Recursive Resolver policy, user privacy and security, online safety and collaboration in the internet infrastructure ecosystem.

General comments on Mozilla's Trusted Recursive Resolver (TRR) policies

CDT applauds Mozilla's TRR policies, generally, because they set a higher standard for user privacy across all recursive DNS resolvers. We encourage more providers of DNS resolvers to adopt such policies, regardless of their relationship with Mozilla. However, we would like to raise additional questions, including:

- What is Mozilla's proposed process to monitor compliance with the TRR policies?
- Are binding legal agreements with TRRs the main compliance mechanism?
- How does Mozilla handle user concerns, questions and complaints against a TRR? And what is the expected recourse?

We note that its TRR policies firmly place Mozilla's FireFox in the role of infrastructure distributor based on its pro-privacy reputation, which it has leveraged for the public interest in this case. While we reiterate our support for this consumer-protective action, we also raise questions about the broader impacts of Mozilla's role in the provision of internet infrastructure and services. For example, how might Mozilla's associations with TRRs (who may act in

untrustworthy ways) ultimately impact its reputation? What happens to the ecosystem if FireFox becomes unavailable to users? For the former, we encourage Mozilla to be prepared to take strong, public actions against violations of its TRR policies and to put in place mechanisms to regularly monitor for compliance and allow for proactive user complaints. For the latter, we encourage Mozilla and other browser providers to move toward greater redundancy, such that as the ecosystem evolves, consumer-protective and privacy-respecting services are not dependent on a single provider.

Respecting privacy and security

Mozilla's approach to implementing DNS privacy benefits users. With respect to user data and data protection more generally, CDT supports third-party audits for internet service providers of all kinds, including those operating resolvers. However, to promote broader inclusion in the TRR program, audits should be designed and implemented in ways that do not create prohibitive barriers to entry. Otherwise, some potential providers may be unable to participate in the TRR program thereby undercutting Mozilla's efforts to move away from consolidated service provision.

In addition, the TRR program should ensure that auditors are free of conflicts of interest, are diverse, and include consumer/user privacy advocates. Truly independent, professional, and diverse auditors inject valuable reviews that can enhance and be applied to Mozilla's TRR policies. Finally, to the extent that they are not already, resolver transparency reports should be included within required privacy notices so that users can be more informed in their choices for both web browsers and DNS resolvers.

Online safety

Through the TRR program, Mozilla distributes to end users the DNS resolution services of other intermediary internet service providers. Although some may argue that this makes Mozilla the ideal entity to make decisions about whether to resolve queries for domains hosting objectionable content, we believe such a role would be inappropriate for Mozilla because the scope of impact for such decisions would likely be far broader than necessary, potentially impacting access to lawful content for millions of internet users. As Mozilla prepares to expand the TRR program globally, such decisions made at such scale become even more problematic. Instead, we suggest that individual TRR partners are better suited to make these decisions, so long as they comply with TRR policies, including transparency reporting.

CDT supports transparency reporting as an accountability mechanism, and trusts that Mozilla will make a good-faith effort to hold itself and TRR partners accountable. We also understand that making decisions about filtering or blocking content will be more difficult to track and account for when made at a more granular level. However, we suggest that the negative impacts associated with the alternative, in which filtering and blocking decisions are made by

Mozilla and implemented across the TRR program, outweigh the costs of making such decisions (and the associated costs to transparency reporting) at a more granular level.

CDT issued a report about why DNS blocking is generally a poor approach to content moderation. We caution Mozilla that some intermediaries tend to block more content than necessary and urge Mozilla to consider including in its TRR policies clauses to discourage, if not prohibit, resolvers from blocking domains unless they are so ordered by courts or honor requests by individual users.[1] In terms of auditing, including in transparency reports copies of court orders would help auditors and end users better understand and verify actions taken by resolvers. Although making such information available to end users would be both novel and challenging, CDT would welcome the opportunity to work with Mozilla to develop policies and practices to implement this level of transparency.

Building a better ecosystem

Many applications and services that run on the internet, and much of the internet's infrastructure have become increasingly consolidated. Consolidation of browsers is an issue of special importance for DNS privacy measures because an overwhelming majority of internet users access content on the internet by first querying domain information when accessing the web. Browser-based DNS privacy, such as DoH, leverages this universal behaviour to implement broad improvements to end users' privacy. However, it also shifts protocol preferences into the application layer and creates a potential risk of reducing resolver traffic diversity.

Civil society has wrestled with the tension between DNS privacy and decentralisation directly. Reports by Open Rights Group and the Electronic Frontier Foundation detail the ways in which the privacy enhancements resulting from implementation of DoH/DoT come at some expense to the public interest in a decentralised internet, and yet still come out in favour of the use of these DNS privacy tools. To mitigate the consolidation effects, ORG recommends that "developers creating applications and devices which rely on third-party encrypted DNS servers should avoid becoming complicit in the increasing centralisation of power among a handful of large cloud providers" and that "developers and application providers should offer users a choice of provider if their product enables encrypted DNS by default."

Because most internet users do not have the technical expertise to make an informed decision about which resolver they trust, default settings become increasingly important. For more technically savvy users, tools to enable meaningful user agency and intuitive, accessible controls in user agents like browsers and other applications promote more engagement toward protecting their own privacy.

Governments and private companies have cited centralisation as a primary concern with DNS privacy measures. CTIA, NCTA, and US Telecom wrote to members of the United States Congress, criticising Google's use of DoH for Chrome and Android and citing concerns of

[1] Filtering in response to user requests should only be implemented on a per user basis and should not apply more broadly.

consolidation of the internet.[2] Yet perhaps there are roles for consolidators when centralisation provides useful functions, such as easily deploying privacy enhancements like DoH/DoT via software to as many end users as possible in all corners of the globe. More research might make a case for one approach over another in the public interest.

Other CDT comments

As CDT has stated previously, "despite the privacy and security enhancements offered by encrypted transport protocols, the DNS resolver's privacy policy is important because the service still has the ability to see, store, or use the DNS query history associated with individual IP addresses, or in some cases, individual devices. That is, even though encrypted DNS protects users from eavesdropping, they must still trust the DNS resolver with their data. CDT hopes to see more DNS resolvers adopt both the technical and the policy measures necessary to protect users against privacy and security harms."

CDT understands the relationship between privacy and censorship for end users, which is why we are in support of better internet protocols like DNS-over-HTTPS, and commend Mozilla for helping to design the standard and leveraging its market power and reputation to roll out DoH quickly and to so many end users. Mozilla's TRR can help empower access to information in countries conducting censorship through DNS blocking and surveillance through online user data.

[2] CTIA, NCTA, & US Telecom. (2019, September 19). *Final DOH LETTER 9-19-19.pdf*. https://www.ncta.com/sites/default/files/2019-09/Final%20DOH%20LETTER%209-19-19.pdf.