Designing for Tussle in Encrypted DNS

Austin Hounsel
Princeton University

Paul Schmitt
USC/ISI

Kevin Borgolte
Ruhr-University Bochum

Nick Feamster
University of Chicago

Abstract

Recent concerns over the privacy implications of the Domain Name System (DNS) have led to encrypting DNS queries and responses through protocols like DNS-over-HTTPS (DoH) and DNS-over-TLS (DoT). Although the trend towards encryption is a positive development, the accompanying centralization of the DNS has fomented tussles involving ISPs, browser and device vendors, content delivery networks, and users. This paper articulates several current DNS tussles and offers principles to guide system design and implementation such that all stakeholders in the space could participate. We argue that refactoring name resolution in a stub resolver that is separate from devices and applications can preserve the benefits of encrypted DNS while satisfying other architectural desiderata, including performance, resilience, and privacy.

CCS Concepts

• **Networks** → **Network protocol design**; **Network design principles**.

Keywords

Network protocol design, network design principles, DNS

ACM Reference Format:
Austin Hounsel, Paul Schmitt, Kevin Borgolte, and Nick Feamster. 2021. Designing for Tussle in Encrypted DNS. In *The Twentieth ACM Workshop on Hot Topics in Networks (HotNets '21), November 10–12, 2021, Virtual Event, United Kingdom.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3484266.3487383

HotNets '21, November 10–12, 2021, Virtual Event, United Kingdom

ACM ISBN 978-1-4503-9087-3/21/11.
https://doi.org/10.1145/3484266.3487383

1 Introduction

DNS has long been insecure and vulnerable to eavesdropping, but that reality is changing, as protocols for encrypted DNS have recently been developed and deployed, notably DNS-over-TLS (DoT) and DNS-over-HTTPS (DoH). DoH has seen rapid adoption, as browser vendors and device manufacturers have begun to move name resolution into browsers and devices. DoH deployment requires some coordination between the stub resolver on the client (e.g., in the browser or operating system) and the operator of the trusted recursive resolver (TRR). In some cases, that coordination is straightforward because the same organization operates both the browser and the TRR (e.g., Google offers both a browser and a public DNS service). In other cases, two organizations coordinate deployment—for example, Mozilla has collaborated with Cloudflare to deploy an encrypted DNS service in Firefox, with Cloudflare serving as the primary trusted resolver. Although several providers now offer encrypted DNS resolution services, browsers and devices typically send all DNS queries to a single, default provider.

DNS encryption is unquestionably a positive trend, but it is accompanied by a potentially problematic consequence: the *increased centralization of a critical part of the Internet infrastructure* that introduce concerns for resilience, competition, and privacy. This organizational centralization makes the DNS infrastructure itself less resilient to disruption from misconfiguration, attack, and manipulation. These threats are more than theoretical: For example, an attack on DNS infrastructure in 2016 rendered many websites unreachable [33]. DNS queries are ripe for widespread manipulation, resulting in information control and censorship. DNS misconfiguration is also commonplace [4]. Centralization also has potentially adverse effects on competition, introducing new barriers to entry as organizations who operate recursive resolvers have access to DNS queries that can be used for a competitive advantage in other market sectors, from content delivery to advertising [3]. The increased centralization of DNS data into a handful of entities has also raised privacy concerns about tracking users' browsing patterns through their queries. Recent centralization trends in Internet infrastructure are not unique to DNS. Yet, the centralization of DNS is somewhat unique due to the rapid nature at which it is transpiring, as well as *how* it is transpiring, with

certain dominant entities (i.e., browser vendors) exercising their leverage to fundamentally alter the Internet architecture.

Many stakeholders in the Internet ecosystem have an interest in (encrypted) DNS queries: it is the quintessential *tussle space* [6] (which Clark *et al.* define as a part of the Internet architecture where different stakeholders have "adverse interests" and "vie to favor those interests"). Internet service providers (ISPs) and enterprise networks rely on observation of DNS queries to detect everything from compromised devices to botnets, or to offer services such as parental controls. Content delivery networks sometimes rely on DNS options to efficiently map clients to the nearest CDN replica. Users are concerned about ensuring that their Internet use (e.g., browsing patterns, device usage) remain private from eavesdroppers, which could include ISPs, enterprise networks, and CDNs.

The high-stakes tussle associated with control over encrypted DNS has given rise to heated arguments and political battles from mailing lists to standardization bodies, such as the Internet Engineering Task Force (IETF), whereby each of these stakeholders seeks to retain control over the DNS [11, 36, 37]. Faced with the prospect of losing visibility into DNS queries, some organizations have partnered with Mozilla to become trusted recursive resolvers [28, 31]. Left behind in all of these power struggles is the user, who is often left with no choice but to rely on a centralized DNS operator, either by coercion or through opt-out tactics, default configurations, and obscure menu configuration options. Users who have privacy concerns over their ISPs eavesdropping on their DNS traffic might be concerned by this development. On the other hand, users who are concerned with advertisers seeing their browsing patterns would be rightfully concerned that the IoT devices that they purchase from these same companies default to sending DNS queries to the TRR of the same company (e.g., many of Google's IoT products are hard-wired to use Google Public DNS as a TRR [36]).

In spite of the various tussles playing out between stakeholders, current designs for encrypted DNS resolution, which primarily couple DNS resolution to the browser or device, violate many principles for resolving tussles. In particular, Clark *et al.* outline several design principles for resolving tussles: (1) design for choice; (2) don't assume the answer; (3) make the consequence of choice visible; and (4) modularize along tussle boundaries [6]. **The current designs for encrypted DNS violate all four of Clark's principles.**

Current browser- and mobile-based approaches to encrypted DNS typically send all DNS queries to a *single* centralized TRR operator (e.g., Cloudflare, Google), without giving the user an option for others. In some cases, even attempts to change the TRR will render the device inoperable. Second, existing configurations, which default to resolving encrypted DNS queries at a single TRR, assume that this is the correct "answer", precluding other designs that might offer users improved performance, privacy, or some tradeoff between these types of concerns. Third, the notion that one can choose a TRR is largely invisible to users; the consequences of these choices are even more obscure. Fourth, there is a clear modular boundary between application functionality (e.g., web browsing, the functions of some IoT device), and resolving DNS names; current architectures do not respect this boundary.

Centralization is being driven not by technical decisions, but rather by ongoing trends of Internet consolidation, coupled with the bundling of critical functionality like name resolution into applications themselves. In 2017, researchers found that on average, 33% of DNS traffic from Tor is resolved via Google Public DNS [15]. More recent statistics have shown that more than 30% of DNS queries to ccTLDs come from five large cloud providers, two of whom offer their own centralized DNS service [27]. A small number of organizations who operate DNS resolvers are gaining increased market share. The contribution of this paper is not to presume a solution or pick a winner in the encrypted DNS tussle. Rather, it is to explore how the DNS infrastructure might allow tussles to play out such that all stakeholders can have a voice. There are *many* possible outcomes for the future of the DNS infrastructure. But, the DNS infrastructure must allow these tussles to take place without bias, so that the technology can evolve towards the best outcome for all. It is time for the community to re-think the DNS architecture so that these tussles can play out.

2 How DNS Became a Tussle Space

We provide background on encrypted DNS protocols and explain how they have led to a centralization of DNS.

2.1 Encrypted DNS Protocols

DNS queries and responses have historically been unencrypted, which has garnered increasing concern in recent years, given research that has demonstrated that DNS traffic can be used to discover private information about users, ranging from the websites and webpages that they visit to the "smart" devices that they use (and how they operate them) [1]. The Federal Communications Commission (FCC) has expressed similar concerns about these risks, from public hotspots to ISPs [13].

Increasing concern over the privacy risks of DNS has led to the development and deployment of protocols that encrypt DNS queries and responses. Two prominent developments are DNS-over-TLS (DoT) [18] and DNS-over-HTTPS (DoH) [17]. Many public DNS providers, including Google,

Cloudflare, Quad9, and others now provide services for both DoT and DoH. The challenge, naturally, concerns configuring clients to adopt these protocols. Recent proposals from Mozilla and Google involve sending DoH queries directly from the browser to a recursive resolver (sometimes simply referred to as a "resolver") as configured in the browser. Similarly, the Android OS makes it possible to route all DNS queries via DoT to a Google-operated resolver [24].

2.2 The Centralization of DNS

Although the encryption of DNS is largely a positive development, an emergent side effect is centralization. Specifically, clients that are configured to use DoT or DoH operate using *centralized* architectures, whereby the client sends all DoT or DoH queries to a single recursive resolver. Conventional DNS would initially appear to share the same characteristics: a client typically sends all queries to its local resolver, typically one that is configured via DHCP. Yet, encrypted DNS creates the potential for additional centralization for several reasons. First, all clients may have the tendency to use the same encrypted DNS resolver (*e.g.*, Cloudflare, Google), *regardless* of their network attachment point. This scenario contrasts with the status quo, where different clients use different DNS resolvers corresponding to their local ISP. Second, because the selection of the resolver is bundled with the browser or device, users may have no easy or viable option to change this configuration.

These centralization trends have occurred rapidly. In June 2018, Mozilla announced a partnership with Cloudflare to deploy DoH to Firefox desktop users in the United States [26]. Mozilla implements DoH in the browser and Cloudflare operates a recursive resolver that supports DoH. Initially, this option was enabled in Firefox Nightly builds; over the course of 18 months, Mozilla transitioned to sending all DNS queries to Cloudflare via DoH by default. In February 2020, Mozilla enabled DoH by default for all Firefox users in the United States—in many cases doing so with minimal information about the transition [7].

Although encrypted DNS protocols do provide privacy benefits, their deployment over the past three years has created concern about the potential for further centralization of Internet infrastructure. The Internet standards community was initially concerned that by only selecting a single DoH provider, Mozilla was centralizing DNS [19, 20]. Operators of the DNS root servers such as Verisign have expressed concerns about how these developments may affect their ability to localize clients [22]. Meanwhile, ISPs, who rely on the DNS for Internet security and network management purposes, have scrambled to deploy their own Trusted Recursive Resolvers [28].

3 Tussle Spaces in (Encrypted) DNS

In this section, we explore the tussles concerning (encrypted) DNS in more detail, explain how the current architecture fails to resolve (and in some cases, exacerbates) them, and suggest various approaches for designing DNS architecture to account for these tussles.

3.1 Users vs. Public Resolvers & ISPs

What Is The Tussle? When Mozilla announced that Cloudflare would be the initial default recursive resolver for their DoH rollout to Firefox desktop users in the United States, users expressed concern over Cloudflare's potential motivations for participating in the program [19]. Some argued that the program would centralize DNS data at Cloudflare, raising concerns about robustness, competition, and privacy. On the other hand, researchers have found that Google's public resolver already sees a comparatively large portion of DNS queries over any other DNS resolver [27]. Thus, some may argue that the DNS is *already* centralized into a handful of resolvers. At the same time, as ISPs begin to deploy encrypted DNS, other users may not want their ISP to see all of their DNS queries, either.

Why Hasn't The Tussle Resolved? Most stub resolvers and applications that support encrypted DNS send all of a users' queries to a single recursive resolver that is configured on the operating system or by an application that embeds a stub resolver. Users should be able to choose how their DNS queries are resolved, and be able to do so in a way that comports with their preferences regarding privacy, performance, and availability. Yet, in the case of browsers, choices are not exposed to users in meaningful ways; in the case of other devices (e.g., IoT devices), users may not be able to choose their TRR at all.

3.2 Public Resolvers vs. Each Other

What Is The Tussle? Organizations that operate public recursive resolvers compete with one another and have specific interests in seeing users' DNS queries. Cloudflare and Google both operate content delivery networks; Comcast, who recently launched a TRR service, also delivers its own content (Comcast is owned by NBC Universal). To improve the performance of the delivery of content on their own CDNs, Cloudflare and Google may use DNS data to direct users to their local caches. ISPs who operate trusted recursive resolvers may offer additional services, such as parental controls, that depend on seeing DNS traffic [11].

Why Hasn't The Tussle Resolved? Despite the fact that there are hundreds of DoH resolvers deployed [8], only a few DoH resolvers are currently available as options in Firefox through Mozilla's trusted recursive resolver (TRR) program [30, 32]. Approved TRRs must not retain DNS logs for

more than 24 hours, and these logs cannot be sold or shared with other parties [12]. Although this program may be ultimately be beneficial to users' privacy, it affects competition between resolvers and effectively makes the browser vendor the gatekeeper for which organizations can participate in the DNS tussle space.

This arrangement favors some incumbents, while balkanizing the tussle space along various market segments. Notably absent from Mozilla's TRR program is Google's public DoH resolver [32]. Thus, if users wish to use Google's DoH resolver in Firefox, they must manually configure it within the browser [30]. On the other hand, as of May 2020, Google Chrome assigns users to a DoH resolver that is consistent with the user's preferences and settings. If Chrome finds that the DNS resolver configured on a user's operating system is included in a pre-defined table of DoH resolvers, then Chrome will assign that user to the corresponding DoH resolver [2].

3.3 Public Recursive Resolvers vs. ISPs

What Is The Tussle? Because ISPs often rely on visibility into DNS queries for everything from malware detection to parental controls, the loss of visibility complicates certain aspects of network management for ISPs; it is thus no surprise that some are pushing back, even offering their own TRRs. When Mozilla announced that they were deploying DoH to all Firefox desktop users in the U.S. in 2020, Cloudflare and NextDNS were the default recursive resolvers [29]. ISPs contend that current deployment models of DoH favor large public resolvers over ISPs. In 2020, Comcast announced a collaboration with Mozilla to deploy their recursive resolver to Firefox users that use Comcast's networks [28]. Comcast became a member of Mozilla's trusted recursive resolver program; part of that arrangement involved agreeing to audits of their DNS data and various privacy requirements.

Why Hasn't The Tussle Resolved? Although Mozilla rolled out DoH to U.S. Firefox users in 2020, as of 2021, the Internet standards community is still developing techniques to support local DoH resolver discovery [7, 21]. Thus, customization remains cumbersome and obscure: in many cases, users can only use an ISP's DoH resolver if they know the information for the resolver in advance and configure the resolver manually. It remains unclear whether users that use ISPs that are a part of Mozilla's trusted recursive resolver program will exclusively use the ISP-provided resolvers or whether queries will also be distributed across third party recursive resolvers. It is also unclear which ISP resolver Firefox will use when users switch between networks whose DNS resolvers are all members of the trusted recursive resolver program (e.g., when a Comcast subscriber who has opted for ISP resolution migrates to a non-Comcast network).

4 Designing for Tussle

We outline Clark et al.'s principles for designing for tussle [6] and explain their implications for the DNS.

4.1 Design for Choice

Principle. Clark et al. argue that protocols should be designed such that users can choose who they communicate and exchange data with: "It is important that protocols be designed in such a way that all the parties to an interaction have the ability to express preference about which other parties they interact with. Protocols must permit all the parties to express choice [6]."

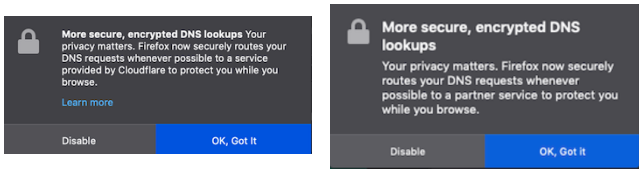
Implications for DNS. When addressing DNS tussles (*e.g.*, users not placing trust in a particular resolver), we not only interpret "design for choice" to mean that users should always be able to decide how DNS resolution is performed, but also that DNS configuration options should be presented in ways that are meaningful to users. Users should then be able to apply these configurations across any application on a device. Applications (or devices acting in the interests of their designers) should not be able to choose where DNS resolution is performed that violate users' wishes or in ways that users cannot override.

Many scenarios in today's Internet are not designed for choice. For example, Google Chromecast has reportedly used Google's public DNS resolver by default, and has lost function if network operators force another resolver to be used [36]. Users can technically set up a resolver on the local network to respond to queries destined for Google's resolver, but this requires significant expertise and is not a feasible choice for most users. The lack of choice in DNS resolution has significant implications for both privacy and reliability.

4.2 Don't Assume the Answer

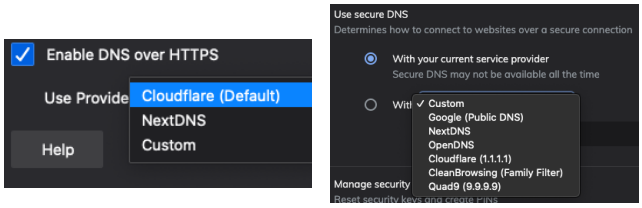
Principle. Clark et al. argue that when it comes to Internet architectures and protocols, there is no such thing as value-neutral design: "What choices designers include or exclude, what interfaces are defined or not, what protocols are open or proprietary, can have a profound influence on the shape of the Internet, the motivations of the players, and the potential for distortion of the architecture. Don't assume that you design the answer. You are designing a playing field, not the outcome." [6]

Implications for DNS. DNS clients can select resolvers in a variety of ways, rather than designing a "playing field". As previously discussed, various applications and devices have made default choices for recursive resolvers that have been



(a) *February 2020* **(b)** *September 2020*

Figure 1: *Firefox pop-up menus for opting out of encrypted DNS have changed over time. Initially, Cloudflare was explicitly mentioned. Over time, the consequences of this opt-out choice became more opaque to users*



(a) *Firefox* **(b)** *Brave*

Figure 2: *Different browsers have different default settings for DNS resolution; most users are likely unaware of these options and wouldn't even understand them even if they could find them at all.*

met with criticism. For example, when Mozilla launched its trusted recursive resolver program for DoH in the United States with Cloudflare as the default recursive resolver, users expressed concern over DNS centralization at an entity separate from their default DNS providers. Users were presented with a choice via a one-time, obscure pop-up menu, to opt out of using DoH (and Cloudflare's resolver) by default, DNS (and in turn, DoH), as shown in Figure 1; this option became increasingly more obscure, and in Firefox 85.0, the option was enabled by default with no opt-out. Disabling or changing these default settings is possible, but the options are buried multiple levels deep in configuration menus that users may find difficult to locate or change, as shown in Figure 2.

In some cases it may also be appropriate to assign different default resolvers to different populations of users by default. For example, Mozilla's deployment of the trusted recursive resolver program with Cloudflare as the default provider for Europe may be problematic, since Cloudflare is a United States-based company, and European users can have different expectations—and regulations—governing data protection practices [20]. Other regions may also have laws, regulations, or circumstances that require different configurations.

Applications and devices should not assume that all users wish to resolve DNS queries in the same way. Rather, they should enable users to express preferences about resolver selection. For example, when a local resolver supports DoH and the application or device is aware of multiple public resolvers that also support DoH, clients may want the local resolver to take precedence. Other clients may want public resolvers to take precedence, only using the local resolver when the configured public resolvers are unavailable. Some clients may wish to split their queries across multiple recursive resolvers, preventing any single resolver from having access to all of their queries. In short, clients should be able to express preferences about how to select between multiple recursive resolvers—making fine-grained decisions about how their queries are resolved—rather than only sending queries to a single resolver by default.

4.3 Modularize Along Tussle Boundaries

Principle. Clark et al. argue for modularization, such that tussles over one part of the architecture do not affect other parts: "Functions that are within a tussle space should be logically separated from functions outside of that space, even if there is no compelling technical reason to do so. Doing this allows a tussle to be played out with minimal distortion of other aspects of the system's function." [6]

Implications for DNS. Traditionally, operating systems have performed DNS resolution on behalf of applications running on a device. Today, applications decide which DNS transports and recursive resolvers should be used, independent of what the operating system learns from the network or configures on its own. Devices have also reportedly ignored the DNS configurations learned from the network [36]. Such behavior prevents stakeholders the ability to resolve tussles. Users that wish to change how DNS resolution is performed on their devices may need to make changes in multiple locations, for example, in both the web browser and the operating system's stub resolver. If each application on a device handles recursive resolver selection differently, then DNS tussles over privacy, trust, centralization, and reliability will continue as applications and devices make decisions about DNS resolution that are challenging for users to override.

5 A Place to Resolve Tussles

Refactoring DNS resolution into a stub resolver that is independent of other parts of the architecture (i.e., operating system, device, browser) makes it possible for stakeholders to resolve tussles. Of course, this architectural proposal is in some sense "back to the future". We argue, however, that such a design allows stakeholders a tussle space to vie for

competing interests, and where various designs for DNS resolution can play out, without compromising security or performance.

To demonstrate this proof of concept and provide a platform for future innovation and experimentation, we forked the open-source `dnscrypt-proxy` stub resolver to demonstrate the feasibility of distributing queries across multiple recursive resolvers [9]; the prototype is publicly available (https://github.com/noise-lab/dnscrypt-proxy). The proxy supports *design for choice* by offering different protocols, resolvers, and distribution strategies across multiple resolvers and supports DoH and DNSCrypt. Our particular modifications concern distributing queries across resolvers, but the most important aspect of the prototype is that it allows for such modification. It *doesn't assume the answer*: a single, system-wide configuration file allows easy configuration of resolution options. Finally, it *modularizes along tussle boundaries* by placing DNS resolution in a separate stub resolver that provides the various stakeholders with a well-defined location for control of DNS functionality.

This architecture does not *guarantee* that all tussles will resolve: device and browser vendors may continue resolve encrypted DNS in devices and browsers, and intercepting those queries at a stub is challenging. Yet, such an architecture makes future work in exploring various DNS resolution strategies *possible* and demonstrating this feasibility may ultimately make such an architecture appealing, particularly if users have choices among device and browser vendors.

6 Related Work

Internet Tussle Spaces. Clark et al. first introduced tussle spaces in 2002 to describe parts of the Internet ecosystem where stakeholders have opposing interests and vie to favor those interests [6]. Although Clark et al. did not foresee the current tussle space two decades ago, Walfish et al. did highlight another tussle in DNS: control over the namespace hierarchy [38]; that tussle concerned which parties controlled the use of certain Internet names and advocated for an alternative flat namespace.

DNS Security and Privacy. DNSSEC provides integrity to DNS [10]. T-DNS[39] address security issues with DNS, such as lack of confidentiality and amplified denial-of-service attacks. T-DNS has not been widely adopted, but it served as the primary inspiration for DNS over TLS (DoT) [18]. DNS over HTTPS (DoH) [17] aims to solve the same problems as DoT, but uses HTTP as a transport protocol. Other work investigated the adoption of secure DNS and their real-world benefits. Lu et al. [25] have found that the adoption of encrypted DNS improved, but it remains low compared to unencrypted DNS, and it currently suffers from deployment issues, like the use of invalid TLS certificates. Bushart et al. [5] and Siby et al. [35] studied the privacy benefits of DoT and DoH in a web browsing scenario. Oblivious DNS (ODNS) [34] hides the queried domain names from a user's recursor; ODNS has been extended to DoH (ODoH) [23], supported by Apple and Cloudflare.

Centralization of DNS. Foremski et al. find that the top 10% of DNS recursors serve approximately 50% of DNS traffic [14]. Moura et al. [27] also encounter centralization in their study of DNS requests to two country code top-level domains (ccTLD), with five large cloud providers being responsible for over 30% of all queries for the ccTLDs of the Netherlands and New Zealand. Hoang et al. [16] propose and evaluate K-resolver, which distributes queries over multiple DoH recursors, so that no single resolver can build a complete profile of the user and each recursor only learns a subset of domains the user resolved.

7 Summary and Future Directions

Recent trends in encrypted DNS architectures and deployments over the past two years have introduced new tussles in DNS between users, ISPs, CDNs, and device and browser vendors. The architectures that are currently being deployed do not conform to Clark et al.'s recommendations for designing for tussle, thus igniting heated disputes on mailing lists, as well as practices that threaten competition, user privacy, and the security an resilience of the Internet as a whole.

In this paper, we have argued that the current situation largely results from the bundling of DNS resolution with browsers and devices, in ways that are opaque to users. We make a case that this trend could be at least partially reversed by modularizing DNS resolution in a separate stub resolver that can be configured and customized by all stakeholders, thereby allowing tussles to play out. This paper and the architecture we have introduced raises more questions than it answers, among them: the most effective strategies for distributing queries across TRRs, the best interfaces for presenting choices to users, and how to handle various implementation corner cases (e.g., embedded devices that use encrypted DNS and thus bypass the proxy). In this sense, we view the role of our work as both raising community awareness of these developments, and presenting an architecture where both industry and the research community can explore questions concerning encrypted DNS, from the evaluation of different TRR resolution strategies to the best way to present these (increasingly complex) choices to users.

Acknowledgments. This work was funded in part by NSF Award CNS-1953513.

References

[1] Noah Apthorpe, Danny Huang, Dillon Reisman, Arvind Narayanan, and Nick Feamster. 2019. Keeping the Smart Home Private with Smart(er) Traffic Shaping . In *Symposium on Privacy Enhancing Technologies (PETS)*. Stockholm, Sweden, 128–148. https://content.sciendo.com/view/journals/popets/2019/3/article-p128.xml

[2] Kenji Baheux. 2020. *A safer and more private browsing experience with Secure DNS.* https://blog.chromium.org/2020/05/a-safer-and-more-private-browsing-DoH.html

[3] Kevin Borgolte, Tithi Chattopadhyay, Nick Feamster, Mihir Kshirsagar, Jordan Holland, Austin Hounsel, and Paul Schmitt. 2019. How DNS over HTTPS is Reshaping Privacy, Performance, and Policy in the Internet Ecosystem. In *Proceedings of the Research Conference on Communications, Information and Internet Policy* (48 ed.) (2019-09). SSRN, Washington DC, USA, 1–9. https://doi.org/10.2139/ssrn.3427563

[4] Kevin Borgolte, Tobias Fiebig, Shuang Hao, Christopher Kruegel, and Giovanni Vigna. 2018. Cloud Strife: Mitigating the Security Risks of Domain-Validated Certificates. In *Proceedings of the 25th Network and Distributed System Security Symposium (NDSS)* (25 ed.) (San Diego, CA, USA, 2018-02), Patrick Traynor and Alina Oprea (Eds.). Internet Society (ISOC). https://doi.org/10.14722/ndss.2018.23327

[5] Jonas Bushart and Christian Rossow. 2020. Padding Ain't Enough: Assessing the Privacy Guarantees of Encrypted DNS. In *10th USENIX Workshop on Free and Open Communications on the Internet (FOCI '20)*. https://www.usenix.org/system/files/foci20-paper-bushart.pdf

[6] David D Clark, John Wroclawski, Karen R Sollins, and Robert Braden. 2002. Tussle in cyberspace: defining tomorrow's internet. In *Proceedings of the 2002 conference on Applications, technologies, architectures, and protocols for computer communications*. 347–356.

[7] Selena Deckelmann. 2020. *Firefox continues push to bring DNS over HTTPS by default for US users .* https://blog.mozilla.org/blog/2020/02/25/firefox-continues-push-to-bring-dns-over-https-by-default-for-us-users/

[8] Frank Denis. 2021. *DNSCrypt: public-resolvers.* https://download.dnscrypt.info/resolvers-list/v3/public-resolvers.md

[9] DNSCrypt. 2021. *dnscrypt-proxy 2: A flexible DNS proxy, with support for encrypted DNS protocols.* https://github.com/DNSCrypt/dnscrypt-proxy

[10] Donald E. Eastlake and Charles W. Kaufman. 1997. *Domain Name System Security Extensions.* RFC 2065. RFC Editor. http://www.ietf.org/rfc/rfc2065.txt (Internet Standard).

[11] John Eggerton. 2019. *ISPs Seek Hill Intervention in Encryption-Related Google DNS Change.* https://www.nexttv.com/news/isps-seek-hill-intervention-in-encryption-related-google-dns-change

[12] Marshall Erwin. 2019. *Trusted Recursive Resolvers - Protecting Your Privacy With Policy and Technology.* https://blog.mozilla.org/netpolicy/2019/12/09/trusted-recursive-resolvers-protecting-your-privacy-with-policy-technology/

[13] Federal Communications Commission. 2016. *FCC Adopts Broadband Consumer Privacy Rules.* https://www.fcc.gov/document/fcc-adopts-broadband-consumer-privacy-rules

[14] Pawel Foremski, Oliver Gasser, and Giovane C. M. Moura. 2019. DNS Observatory: The Big Picture of the DNS. In *Proceedings of the 19th Internet Measurement Conference (IMC)* (Amsterdam, The Netherlands, 2019-10), Phillipa Gill and Robert Beverly (Eds.). Association for Computing Machinery (ACM). https://doi.org/10.1145/3355369.3355566

[15] Benjamin Greschbach, Tobias Pulls, Laura M. Roberts, Philipp Winter, and Nick Feamster. 2017. The Effect of DNS on Tor's Anonymity. In *NDSS*. The Internet Society. https://nymity.ch/tor-dns/tor-dns.pdf

[16] Nguyen Phong Hoang, Ivan Lin, Seyedhamed Ghavamnia, and Michalis Polychronakis. 2020. K-resolver: Towards Decentralizing Encrypted DNS Resolution. In *Proceedings of The NDSS Workshop on Measurements, Attacks, and Defenses for the Web 2020* (San Diego, CA, USA) *(MADWeb '20)*. Internet Society, 7 pages. https://doi.org/10.14722/madweb.2020.23009

[17] Paul Hoffman and Patrick McManus. 2018. *DNS Queries over HTTPS (DoH).* RFC 8484. RFC Editor. https://www.ietf.org/rfc/rfc8484.txt (Proposed Standard).

[18] Zi Hu, Liang Zhu, John Heidemann, Allison Mankin, Duane Wessel, and Paul Hoffman. 2016. *Specification for DNS over Transport Layer Security (TLS).* RFC 7858. RFC Editor. https://www.ietf.org/rfc/rfc7858.txt (Proposed Standard).

[19] Bert Hubert. 2019. *Centralised DoH is Bad for Privacy, in 2019 and Beyond.* https://blog.powerdns.com/2019/09/25/centralised-doh-is-bad-for-privacy-in-2019-and-beyond/

[20] Bert Hubert. 2019. *The big DNS Privacy Debate at FOSDEM.* https://blog.powerdns.com/2019/02/07/the-big-dns-privacy-debate-at-fosdem/

[21] Internet Engineering Task Force. 2021. *Adaptive DNS Discovery (add).* https://datatracker.ietf.org/wg/add/documents/

[22] Burt Kaliski. 2020. *A Balanced DNS Information Protection Strategy: Minimize at Root and TLD, Encrypt When Needed Elsewhere.* https://blog.verisign.com/security/a-balanced-dns-information-protection-strategy-minimize-at-root-and-tld-encrypt-when-needed-elsewhere/

[23] Eric Kinnear, Patrick McManus, Tommy Pauly, and Christopher A. Wood. 2021. *Oblivious DNS Over HTTPS.* RFC draft-pauly-dprive-oblivious-doh-04. RFC Editor. https://tools.ietf.org/id/draft-pauly-dprive-oblivious-doh-04.txt

[24] Erik Kline and Ben Schwartz. 2018. *DNS-over-TLS Support in Android P.* https://android-developers.googleblog.com/2018/04/dns-over-tls-support-in-android-p.html

[25] Chaoyi Lu, Baojun Liu, Zhou Li, Shuang Hao, Haixin Duan, Mingming Zhang, Chunying Leng, Ying Liu, Zaifeng Zhang, and Jianpeng Wu. 2019. An End-to-End, Large-Scale Measurement of DNS-over-Encryption: How Far Have We Come?. In *Proceedings of the 19th Internet Measurement Conference (IMC)* (Amsterdam, The Netherlands, 2019-10), Phillipa Gill and Robert Beverly (Eds.). Association for Computing Machinery (ACM). https://doi.org/10.1145/3355369.3355580

[26] Patrick McManus. 2018. *Improving DNS Privacy in Firefox.* https://blog.nightly.mozilla.org/2018/06/01/improving-dns-privacy-in-firefox/

[27] Giovane CM Moura, Sebastian Castro, Wes Hardaker, Maarten Wullink, and Cristian Hesselman. 2020. Clouding up the Internet: how centralized is DNS traffic becoming?. In *Proceedings of the 2020 Internet Measurement Conference (IMC)* (Virtual Event, 2020-10), Fabián Bustamante and Nick Feamster (Eds.). Association for Computing Machinery (ACM). https://doi.org/10.1145/3419394.3423625

[28] Mozilla. 2020. *Comcast's Xfinity Internet Service Joins Firefox's Trusted Recursive Resolver Program.* https://blog.mozilla.org/blog/2020/06/25/comcasts-xfinity-internet-service-joins-firefoxs-trusted-recursive-resolver-program/

[29] Mozilla. 2020. *The Facts: Mozilla's DNS over HTTPs (DoH).* https://blog.mozilla.org/netpolicy/2020/02/25/the-facts-mozillas-dns-over-https-doh/

[30] Mozilla. 2021. *Firefox DNS-over-HTTPS.* https://support.mozilla.org/en-US/kb/firefox-dns-over-https

[31] Mozilla. 2021. *Firefox extends privacy and security of Canadian internet users with by-default DNS-over-HTTPS rollout in Canada.* https://blog.mozilla.org/en/mozilla/news/firefox-by-default-dns-over-https-rollout-in-canada/

[32] Mozilla. 2021. *Mozilla Policy Requirements for DNS over HTTPs Partners.* https://wiki.mozilla.org/Security/DOH-resolver-policy

[33] Nicole Perlroth. 2016. *Hackers Used New Weapons to Disrupt Major Websites Across U.S.* https://www.nytimes.com/2016/10/22/business/internet-problems-attack.html

[34] Paul Schmitt, Anne Edmundson, Allison Mankin, and Nick Feamster. 2019. Oblivious DNS: Practical Privacy for DNS Queries. In *Proceedings of the 19th Privacy Enhancing Technologies* (19 ed.) (Stockholm, Sweden, 2019-07), Carmela Troncoso and Kostas Chatzikokolakis (Eds.). Sciendo, 228–244. https://doi.org/10.2478/popets-2019-0028

[35] Sandra Siby, Marc Juarez, Claudia Diaz, Narseo Vallina-Rodriguez, and Carmela Troncoso. 2020. Encrypted DNS -> Privacy? A Traffic Analysis Perspective. In *Proceedings of the 27th Network and Distributed System Security Symposium (NDSS)* (27 ed.) (San Diego, CA, USA, 2020-02), Xu Dongyan and Ahmad-Reza Sadeghi (Eds.). Internet Society (ISOC). https://doi.org/10.14722/ndss.2020.24301

[36] Paul Vixie. 2019. *My Chromecast Ultra Would Not Start Until I Began Answering 8.8.8.8.* https://mailarchive.ietf.org/arch/msg/dnsop/WCVv57IizUSjNb2RQNP84fBclI0/

[37] Paul Vixie. 2019. *Re: Cloudflare CEO on DoH.* http://lists.encrypted-dns.org/scripts/wa-ENCDNS.exe?A2=ENCRYPTED-DNS;fa478328.1909&S=

[38] Michael Walfish, Hari Balakrishnan, and Scott Shenker. 2004. Untangling the Web from DNS. In *Proceedings of the 1st USENIX Symposium on Networked Systems Design and Implementation (NSDI)* (1 ed.) (San Francisco, CA, USA, 2004-03), Robert Morris and Stefan Savage (Eds.). USENIX Association. https://dl.acm.org/doi/10.5555/1251175.1251192

[39] Liang Zhu, Zi Hu, John Heidemann, Duane Wessels, Allison Mankin, and Nikita Somaiya. 2015. Connection-oriented DNS to Improve Privacy and Security. In *Proceedings of the 36th IEEE Symposium on Security & Privacy (S&P)* (36 ed.) (San Jose, CA, USA, 2015-05), Vitaly Shmatikov and Lujo Bauer (Eds.). Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/sp.2015.18