# How DNS over HTTPS is Reshaping Privacy, Performance, and Policy in the Internet Ecosystem

Kevin Borgolte, Tithi Chattopadhyay, Nick Feamster, Mihir Kshirsagar,
Jordan Holland, Austin Hounsel, Paul Schmitt
Princeton University and The University of Chicago

## Abstract

Internet communication relies on the Domain Name System (DNS), which maps a human-readable Internet destination to an IP address. A recent proposal for transmitting DNS over HTTPS (DoH) enhances client privacy by tunneling DNS over secure HTTP (HTTPS). In this paper, we explore the policy implications of consolidated DoH by systematically analyzing the marketplace, measure its performance effects, and investigate how it affects the different stakeholders, including consumers. We enumerate the agents in the marketplace as well as their market incentives. We then examine the performance of DoH through client-based measurements compare unencrypted DNS with DoH. As DoH deployments change the competitive landscape of the market, we explore their effect on other operators, ISPs, and broadband access at the last mile, as well as the potential regulatory and policy implications of DoH deployments.

## 1 Introduction

Essentially all Internet communication relies on the Domain Name System (DNS), which maps a human-readable Internet destination to an IP address before two endpoints can communicate. Today, most DNS queries and responses are transmitted in cleartext, making them vulnerable to eavesdroppers and traffic analysis. To mitigate some of these privacy risks, ongoing work in both standards bodies and browser implementations transmits DNS over HTTPS (DoH) between clients and third parties who operate DoH resolvers.

Encrypting DNS transport offers certain privacy benefits, but doing so entails various architectural changes. Namely, the default operators of DNS, once largely Internet service providers, become content providers, content delivery networks, and essentially any other third party. This change has fundamental implications for performance, competition, and privacy in the Internet ecosystem. From the performance perspective, a shift to DoH would potentially impede the performance of conventional DNS lookups while accelerating the performance of content delivery when the content is co-located with the DoH resolver. This scenario is already the case today, where many DoH operators also operate content delivery networks (CDNs). This mode of operation may result in better performance for content that is hosted on these CDNs, effectively rekindling certain aspects of net neutrality, where content hosted by some parties is practically delivered with better performance than others.

Encrypted DNS traffic would also seem to improve privacy, but the net effect of DoH is ultimately a change whereby a single party can observe and monetize DNS traffic, where monetization might take many forms, ranging from the ability to more efficiently deliver content to the ability to deliver targeted advertising. DoH also has implications for competition dynamics among CDNs: certain CDNs use client localization techniques based on the location of the client's DNS resolver. In some cases, DoH makes this type of client localization more challenging, meaning that these CDNs would face significant operational costs merely to stay competitive. Whoever controls DNS controls client mapping to content, increasing the potential for anti-competitive behavior in content delivery. For example, a DoH operator could degrade the performance of content delivery from competitors—possibly unintentionally, through suboptimal server mapping—possibly in difficult-to-measure ways. Finally, the consolidation of DNS resolution that would result from a small number of DoH providers creates the potential for surveillance, censorship, manipulation, control, and coercion.

In this paper, we explore the policy implications of DoH by measuring its performance as compared to conventional DNS, analyzing the marketplace dynamics, and investigating the implications of architectural refactoring on regulatory policy. We first explore the competitive landscape, including the incentives of various stakeholders, from ISPs to CDNs. We then compare conventional unencrypted DNS to DoH using multiple DoH providers and while varying the network performance conditions. We then explore various policy implications. As DoH deployments can change the competitive landscape of the market, we explore their impact on other operators, ISPs, and broadband access at the last mile. Finally, we explore the potential regulatory and policy implications of current and future DoH deployments.

# 2 Market Structure and Competitive Landscape

A client or the user that wants to access a particular type of content, or application, does so by searching a domain name. These domain names then need to be mapped to IP addresses. Every device connected to the Internet has a unique IP address and the process of translating domain names to the IP address involves several different steps that are often performed by a DNS resolver. Traditionally, DNS resolvers have been managed by the user's ISP, and the process could often involve making repeated requests until the IP address is identified. In some cases this process is simplified by temporarily storing data closer to the client (DNS caching). Caching can be done at the ISP's resolver, the user's system, and the browser level. CDNs also play an important role in storing data closer to the client to improve performance and process queries faster. The process of DNS resolution involves the following agents: the client/user making the request, the web browser, the operating system, the ISP (that carries out DNS resolution), the content provider, and possibly a CDN.

The DNS queries transmitted to and from the ISPs are often unencrypted and insecure. Prior work has demonstrated that DNS queries can make users susceptible to eavesdropping and tracking [11]. These potential privacy risks have resulted in recent developments that include applying encryption techniques to DNS traffic [2, 5, 12, 15, 21, 26]. In this paper, we focus on DNS over HTTPS (DoH) [12]. The most common implementation of DoH has been through web browsers, like Mozilla Firefox and Google Chrome. They are able to implement and use this protocol because of collaborations and ties with CDN operators, who also operate DoH recursive resolvers. Although the agents involved in DoH are the same as for conventional DNS, the agent delivering the domain name resolution service is no longer the ISP, and the features and characteristics of the service have changed. This causes the interdependencies and relationships between the agents to shift. These changing interdependencies have an effect on overall market structure.

## 2.1 Competition and Adjacent Markets

**Direct Competition.** Traditional DNS resolvers operated by ISPs will be directly affected as they use DNS traffic analysis to enable parental control and malware detection and among some of their offerings. Current DoH implementations through web browsers and third party CDNs is in direct competition with ISPs because the older protocol is primarily run by ISPs. DNS queries that are now resolved through cloud services, as in DoH, directly compete with traditional ISPs that previously handled the resolution process.

**Consequences for Adjacent Markets (particularly ISPs and CDNs).** Several of the agents involved in implementation of the DoH resolvers have tie-ins with third party CDNs or operate in adjacent markets. These relationships lead to potential uses of monopoly leveraging in the adjacent market. In markets where the same provider operates in multiple complementary markets, it is possible that the provider can sustain loss of revenue in one market while they build up their customer base because of their ability to use their presence in the adjacent highly concentrated market to recover some of these losses. In cases where agents described above operate in multiple markets, it becomes critical to observe revenue generation strategies employed in other markets to squeeze out competition in a new market.

Several existing studies explore how complementary products can be used to preserve and create monopolies in the future and in emerging markets [3]. Their analysis focused on entry costs and network externalities and extends the analysis to the Microsoft case where a tie-in of Windows and Internet Explorer created a monopolistic market structure. This work can further be extended to areas where a setting is analyzed in which a monopolist can control the pace of innovations and the lifetime of a particular product. In the case of DoH, there is potential risk of impact to CDN localization and diversity if only a few concentrated applications (e.g., web browsers) and DNS resolvers control the global market.

**Bundling.** The practice of bundling products or services has commonly been used in the telecommunications and information industry. On one hand these industries are highly interconnected and benefit from better integration with complementary products and services [6]. This need for compatibility and standardization has often resulted in firms entering multiple complementary markets simply because they are able to provide higher quality products than their counterparts that are not integrated in the same way. Even when it is not the same firm operating in the two complementary markets, exclusive collaborations and partnerships can result in services that are more compatible and have better performance. It is possible that in the case of DoH, the use of Google Chrome and Google's public DNS resolver can lead to quicker resolution than two unrelated entities because of the potential to develop software and hardware that is more compatible.

Furthermore, consumers often like to avoid the high transaction costs that come with dealing with multiple providers (for billing, customer service and so on), and prefer to deal with just one firm that provides these bundled services. While there are significant benefits to bundling products that are highly interconnected, they often lead to issues of discrimination and eventually increased barriers to entry into a particular market. It is possible that Cloudflare and Google's content could enjoy performance benefits as a result of DoH resolution through their respective DNS servers. Additionally, while these services promise privacy through use of encrypted transport and by policies that prohibit user tracking, there are aggregate user patterns that are revealed to these third-party resolvers that can be beneficial to their own business as several of them also operate as CDNs and content providers.

## 2.2 Interconnection and Network Effects because of Web Browser/OS Tie-in

The effect on the competitive landscape primarily arises from the current implementation of DoH through a small number of global players in this market. This is largely due to the fact that most global traffic is associated with a relatively small number of web browsers. According to several web traffic measurement sources, over 80% of the global web traffic usage is from three web browsers: Google Chrome, Apple Safari and Mozilla Firefox (Internet Explorer if one considers only desktop browsers). While there are differences in their methods of measuring global traffic, these different measurement sites unanimously point toward a concentration of global players in the web browser market. Additionally these platforms tend to partner with other agents (third-party commercial DNS resolvers) that are also highly concentrated. The prevalence of highly concentrated complementary producers leads to a market that is lopsided because of network effects (even if there is no intent to jeopardize consumer welfare).

Network effects occur when the consumer's utility from a particular good is enhanced or improved as more consumers purchase the product or complementary products. There are two aspects to network creation that can potentially create an anti-competitive environment. The first aspect is the firm's desire to capture a larger market power by attracting more and more consumers, and the second is working together as a system with various other complementary products to ensure compatibility [18]. Most technologies in this industry often do not stand alone and are required to be compatible with other complementary products to survive. For example, device manufacturers partner with operating system and web platform providers. Additionally, some device manufacturers can also hard-code DNS resolvers, examples include Google Chromecast hard coding its resolvers to Google's public DNS (8.8.8.8).

These markets are often characterized by network effects that exist when the value of a customer joining a network is increased due to the purchase of compatible products. In this case, third-party commercial DoH resolvers find benefits from the consumers' choice of web browser or operating system. Unlike other markets where competition is usually encouraged, the Internet and information industry experiences significant benefits from consumers being in the same network or purchasing products from the same firm. In this case, it is possible that the consumer benefits from using a particular web browser (i.e., Mozilla Firefox), and experiences benefits when the collaboration with a single resolver (e.g., Cloudflare's resolver) results in better performance and privacy benefits. While a consumer may experience benefits from this arrangement, there are still welfare losses that can be incurred if competition is not encouraged in the long run.

### 2.3 Effects on Consumers

**Consequences for Areas with Poorer Network Coverage.** Broadband coverage and the quality of the network both globally and within the US has varied due to geographical challenges, density of population, and various other economic and regulatory reasons. It is no secret that there are areas within the US with more broadband providers and stronger network coverage, and other less-profitable areas with weaker coverage and fewer providers. The use of DoH according to our study has significant impact on areas with poorer network coverage, which further deepens some of our digital divide concerns. We expand on this in Section 3.

**Consumer Choice and Switching Costs.** DoH, which is primarily implemented through web browsers, has a direct effect on consumer choice. While some consumers are sophisticated and understand the options that their web browser provides them, most consumers interact with their web browsers in ways that are far simpler. Additionally, in a multiplatform and highly networked market with multiple producers providing services that require compatibility and standardization, consumers cannot often understand the impact of their choices on other related services. In these cases, the default offered by the web browser and an explanation of the user's choice is of paramount importance. Consumers need to have a clear understanding of trade-offs between these choices. A user should be able to choose between DNS privacy (and who they can trust) and other security and control features including parental controls (among others).

Further, web browsers and OS platforms are highly concentrated markets and DoH implementations through these platforms have significant impact on consumer switching costs. Previous studies have demonstrated that switching costs arise because of a user's need for compatibility between their current good or service and their future investments [19]. In the case of DoH, some switching costs for consumers may be associated with device ties to operating system and default browsers. Even in the scenario where a consumer is able to make an informed choice between their privacy preserving options and other performance related features, they may not be able to exercise these choices because of switching costs.

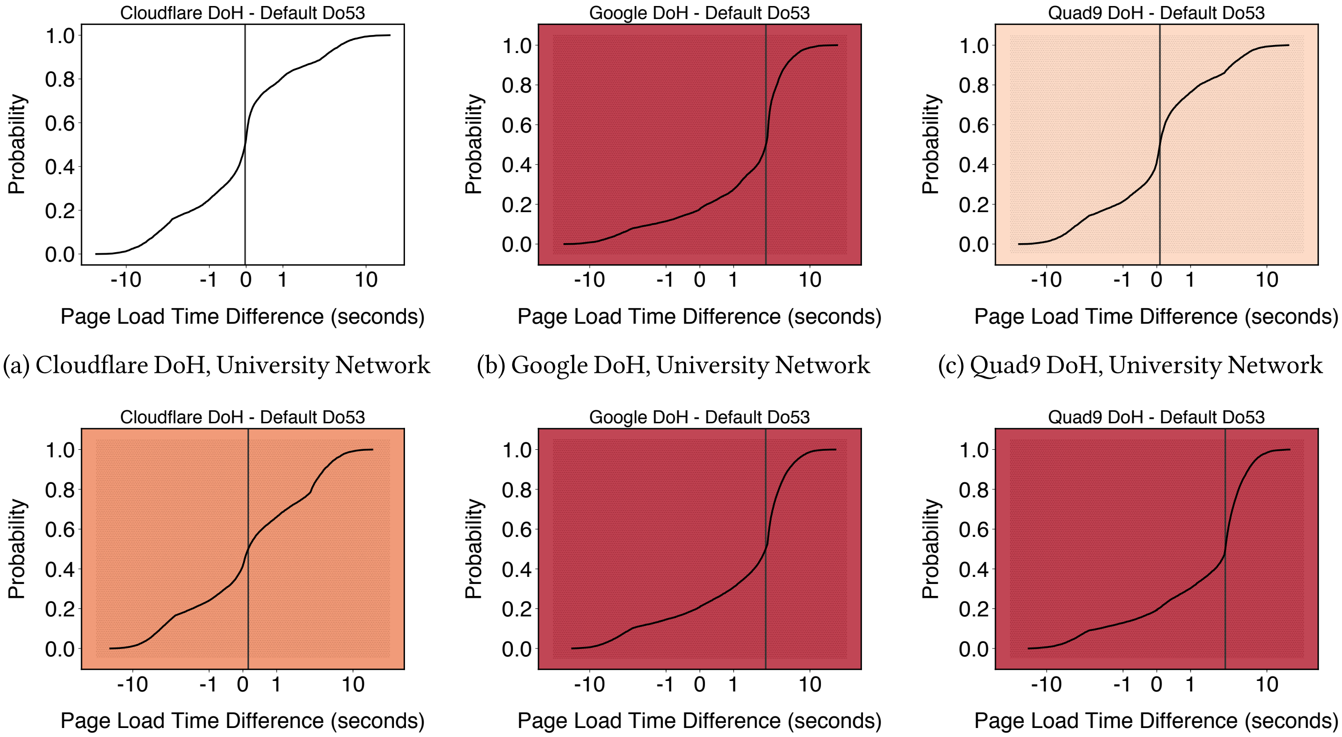
## 3 Performance Effects

An effect of centralized DNS resolution and the use of DoH is that performance can be greatly impacted by network conditions [13, 14]. To understand the relationship between DoH providers, network conditions, and DNS protocols, we measure page load times while using a default university-network DNS recursor as well as DoH recursors provided by Cloudflare, Google, and Quad9. Page load times are gathered by inspecting HTTP Archive objects (HARs), which can be collected from any webpage in Firefox [24]. We collect HARs for each website, which include timings for the onLoad event, as well as for individual components for each request that the browser made, including all resources of a page.

We perform our measurements using different ISP network scenarios, including conditions that emulate mobile network characteristics. First, we connect one machine to the Internet via a university campus network. The university has a 20 Gb/s connection to the Internet. It is a well-connected network to Cloudflare, Quad9, and Google, respectively. Second, we place a measurement node on the university network, but with traffic shaping applied to emulate 4G mobile network performance. We shape outgoing traffic with an additional latency of 53.3 ms and jitter set to 1 ms. We also dropped 0.5% of packets to mimic the loss that cellular data networks can exhibit. Finally, we shape our uplink rate to 7.44 Mb/s and our downlink rate to 22.1 Mb/s. These settings are based on an OpenSignal report of mobile network experience across providers [23]. Figure 1 compares page load times for DoH providers versus a university resolver with the two different network performance profiles. Each plot shows a CDF for the difference in page load times between a cloud provider's DoH implementation and the default university recursor. The shading indicates the severity of median difference between the DoH provider and the university, with darker shades meaning DoH resulted in slower page loads.

Page load times when using Cloudflare DoH on the university network are comparable to using the university resolver (Figure 1a). However, Google[1] and Quad9 DoH resolvers result in higher median page load times that the university resolver (Figures 1b and 1c, respec-

[1] At the time of our measurement the publicly available Google DoH resolver was advertised as "experimental," a likely contributing factor to its overall poor performance.



(a) Cloudflare DoH, University Network

(b) Google DoH, University Network

(c) Quad9 DoH, University Network

(d) Cloudflare DoH, 4G

(e) Google DoH, 4G

(f) Quad9 DoH, 4G

Figure 1: Web page load time comparisons between a default recursor and open DoH recursors operated by cloud providers with emulated network conditions.

tively). These results indicate that the choice of DoH provider, and by extension the choice of application as DoH recursors are often set in the application, can greatly impact the user experience.

When network conditions are less ideal than the well-connected university network (Figures 1d, 1e, and 1f), the gap in page load times between clients that use regular DNS and those that use DoH widens, with DoH clients performing worse. This means that applications that utilize DoH by default, such as web browsers, will lead to a worse end-user experience as network conditions deteriorate, or for users in areas with poor connectivity generally (i.e., areas with poor broadband connectivity), effectively broadening the Internet connectivity gap.

# 4 Regulatory and Policy Implications

If Internet users shift to routinely relying on third-party resolvers for DNS queries, that would have significant implications for how we regulate the Internet in at least three key areas. First, widespread adoption of DoH will challenge the Federal Communications Commission's reliance on the ISP-provided DNS look up system to justify its light touch regulation of ISPs by reclassifying them as information service providers. Second, it will have significant implications for how consumers and regulators protect privacy. Third, it will have implications for policies that require ISPs to filter or block sites using the DNS function.

## 4.1 Net Neutrality

In the FCC's most recent round of rulemaking on net neutrality, the 2018 Restoring Internet Freedom Order [9], one of the FCC's core arguments rests on the assertion that "the vast majority of ordinary consumers rely upon the DNS functionality provided by their ISP, and the absence of ISP-provided DNS would fundamentally change the online experience for the consumer" [9, Paragraph 34]. But, as discussed above, DoH allows browsers, applications or web sites to substitute for the ISP-provided DNS function without any noticeable impact to the end user experience. If ISP-provided DNS is no longer critical, then an important rationale for the treatment of Internet service as an information service falls away.

The FCC relied on the ISP-provided DNS architecture to justify its reclassification of Internet service as an "information service" rather than a "telecommunication service." This arcane distinction between the two types of services has a profound real-world implication as it determines the type of authority the agency has to regulate the conduct of ISPs. In the FCC's reading, ISP-provided DNS is an indispensable component of the total service offered to consumers. On this view, ISP-provided DNS makes the total Internet service offering an "information service" because that lets the ISP perform all the functions in the definition of an information service (e.g., acquiring, storing and processing information).

The view of ISP-provided DNS as a functionally integrated component of Internet service played a critical role to the United States Supreme Court decision in Brand X that upheld the FCC's classification of cable Internet service as an information service [22]. The Brand X majority observed that "the entire question is whether the products here are functionally integrated (like the components of a car) or functionally separate (like pets and leashes). That question turns not on the language of the Act, but on the factual particulars of how Internet technology works and how it is provided, questions [Supreme Court precedent] leaves to the Commission to resolve in the first instance" [22, p. 991].

The dissent vigorously disagreed with the Court's reliance on what it saw as a cramped reading of the statute. In Justice Scalia's colorful language, he explained that the majority conflated an offering of a service ("pizza" in his analogy) with another ("delivery"). He explained that the ISP's DNS function was merely adjacent to the core offering of a telecommunication service [22, pp. 1012–1013].

In subsequent cases challenging agency regulation, the legal debate concerning DNS has oscillated around these two poles: is ISP-provided DNS is a core integrated component of Internet service, or does it fit within a telecommunications management exception for functions that merely facilitate the delivery of the main service? The advent of DoH, however, challenges that debate's framing. Now DNS look up can be readily supported by a third-party resolver through a browser or application in a manner that does not appear functionally different from the ISP-provided service to the end user. As a result, rather than resolve the esoteric problem of how to view the significance of ISP-provided DNS service, the public debate can return to the core question about what is the appropriate regulatory structure for Internet service.

## 4.2 Privacy and Security

Widespread adoption of DoH could have significant implications for the privacy of DNS lookups. A core feature of the protocol is that it offers a significant improvement for the security and privacy for user activity by encrypting the transport to the resolver. But it also allows for third-party resolvers to collect sensitive information about user activity in a manner that the end user may not understand or consent to freely. Therefore it raises important questions about what should be done to ensure that third party DNS resolvers adequately inform users about the data collection and limit any commercial use of that information absent user consent.

DNS privacy is increasingly a significant concern and design consideration. Research has shown that DNS lookups can reveal various aspects of user activity including the apps they use, web sites they visit, the devices in their home and how they are using them. This can be done even if the web site or app has content that is encrypted. As a result, various efforts have been developed to send DNS queries over encrypted transport protocols. The use of encrypted transports makes it impossible for passive eavesdroppers to observe DNS queries, like an attacker for devices on a shared network (e.g., a wireless network in a coffee shop). This limits the potential for a man in the middle attack. These transports also allow clients to send encrypted DNS queries to a third-party resolver (e.g., Google or Cloudflare), preventing a user's ISP from seeing the DNS queries of its subscribers. As such, from a privacy perspective, DoT and DoH are attractive protocols, providing a measure of confidentiality that DNS previously lacked. But the user's queries are still being collected by the DNS resolver and are subject to exploitation.

Curiously, major ISPs have not attempted to monetize the user data generated from DNS lookups. Some ISPs, however, have tried to monetize "error traffic" on a more limited basis [25]. Similarly, third-party resolvers, such as Google or Cloudflare, have promised that they will not attempt to monetize the user data from DNS queries [4, 10]. As discussed above, there is no fundamental economic reason for DNS providers to shun making a profit from DNS lookup data. The reluctance to commercialize the information flow likely stems from a concern about the predictable consumer and regulatory backlash that would ensue if a company collected, processed and sold such sensitive user data. In addition, the business model of ISPs, which previously provided most of the lookup services, historically did not depend on commercializing consumer data. By contrast, exploiting consumer data is at the core of the business model of a third-party resolver such as Google. As a result, there is little reason to believe that a company such as Google lacks the profit motive to avoid monetizing DNS query data in perpetuity.

If the new third-party resolvers become major players in managing DNS queries, that could affect the current regulatory approach that has treated ISPs as having a unique role in resolving DNS. In 2016, the FCC recognized the potential for ISPs to attempt to monetize DNS data, among other things, and promulgated comprehensive regulations to govern such conduct [8]. Ultimately, those broadband privacy rules were not approved by Congress after the change in administration. But the concern animating the FCC remains; namely that relying on voluntary commitments by DNS resolvers to maintaining user privacy may not be enough. Indeed, one of the key contentious issues was whether ISPs should be treated differently from edge providers in applying limits to the collection, use and sale of user data [7]. While ISPs argued for a level playing field, the proponents of the new regulations emphasized the ISPs had a unique role in resolving all DNS queries for its subscribers and therefore had a near monopoly on access to that sensitive information. If third-party resolvers become widely adopted, the argument for equal treatment all entities that manage sensitive DNS queries becomes much stronger.

### 4.3 Filtering and Blocking

The third area where the shift to third-party resolvers has potential policy implications concerns restrictions on access to certain websites. In the United States, legislators have made several unsuccessful attempts to task ISPs with the responsibility for filtering or blocking web sites with objectionable content using their DNS lookup function. Most recently, the proposed federal Stop Online Piracy Act and the Protect Internet Privacy Act, required ISPs to implement DNS blocking [20]. Those proposals failed to pass Congress, however, because, among other things, the security risks posed by the changes to the DNS function the bills would require. Any future attempts to regulate in this space will now have to also contend with the additional challenge of making third-party resolvers comply with new policies.

More generally, there are constitutional challenges with requiring any resolver to apply DNS filtering [1]. The leading decision in this area struck down a Pennsylvania law requiring ISPs to use DNS filtering to block access to child pornography because the proposed mechanism violated the First Amendment [17]. In that case, the law gave the Pennsylvania Attorney General permission to seek a court order requiring an ISP to "remove or disable items residing on or accessible through" an ISP's service upon a showing of probable cause that the item constitutes child pornography. Once the ISP was notified that a court order was issued, it had five days to block access to the specified content or face criminal liability. The court conducted an in-depth trial, where the court heard testimony from experts and network operators. At the trial's conclusion, the court ruled that with the current state of technology, the law "cannot be implemented without excessive blocking of innocent speech in violation of the First Amendment." Specifically, the court found that DNS filtering would block requests for all sub-pages under the blocked domain name. In other words, requests for all of the independent pages on the site, not just the page that displays the targeted child pornography item would be blocked. The court also found that such DNS filtering mechanisms were not effective because they could be readily circumvented by those who can use anonymous proxy servers or anonymizers to shield their conduct.

In the United Kingdom, the country's ISP association recently nominated Mozilla as an "Internet Villain" for "their proposed approach to introduce DNS-over-HTTPS in such a way as to bypass UK filtering obligations and parental controls, undermining Internet safety standards in the UK" [16]. After a public outcry, the association withdrew that nomination and the entire "Internet Villain" category. But it noted the concern that applications that provide parental controls through DNS filtering may no longer work as intended.

In the United States, there are fewer rules about the types of parental controls ISPs must offer. A handful of states (Louisiana, Maryland, Nevada, Texas and Utah) have passed laws that require ISPs to give subscribers access to parental controls that enable blocking or filtering of websites available to subscribers. And some of the parental controls use DNS filtering to restrict access. It is possible that these states (or others like them) could require third-party resolvers to offer similar options for parents to exercise control. But the challenge is that a state does not have the same type of jurisdiction over the service as it does over an ISP that has a physical presence within its borders as a result of providing Internet service to subscribers.

## 5 Conclusion

DNS queries have historically been transmitted in unencrypted cleartext and resolved by a user's Internet service provider (ISP). Recent developments aim to use HTTPS as the transport for DNS, in a protocol called DNS over HTTPS (DoH). Today, most operators of DoH resolvers are not ISPs but rather content delivery networks and other third parties. In this paper, we have taken an initial look at the implications of this architectural refactoring for performance, privacy, competition, and regulatory policy. These developments certainly warrant continued vigilance, to ensure that Internet performance—and ultimately consumer experience—benefits from DoH deployments. In this vein, Internet measurements such as those we have presented can and must play a pivotal role. For example, such measurements can continue to shed light on the ultimate effects of DoH on user experience, from DNS lookup time to web page load time; Measurements can also help us better understand how DoH providers are mapping clients to Web content. Ultimately, as with Internet performance measurements writ large, continual vigilance through Internet measurement can reduce the likelihood that DoH provider behavior is either discriminatory or anti-competitive.

## References

[1] Jack M. Balkin. "Old School/New School Speech Regulation". In: *Harvard Law Review* 127 (May 6, 2014).

[2] Daniel J. Bernstein. *DNSCurve: Usable Security for DNS.* URL: https://dnscurve.org/ (visited on 07/26/2019).

[3] Dennis W Carlton and Michael Waldman. "The strategic use of tying to preserve and create market power in evolving industries". In: *The Rand Journal of Economics* 33.2 (2002).

[4] Cloudflare. *Privacy – Cloudflare Resolver.* URL: https://developers.cloudflare.com/1.1.1.1/commitment-to-privacy (visited on 07/26/2019).

[5] Frank Denis and Yecheng Fu. *DNSCrypt.* URL: https://dnscrypt.info/ (visited on 07/26/2019).

[6] Joseph Farrell and Garth Saloner. "Installed Base and Compatibility: Innovation, Product Preannouncements, and Predation". In: *The American Economic Review* 76.5 (1986). URL: http://www.jstor.org/stable/1816461.

[7] Nick Feamster. *RE: Docket No. 16-106, Protecting the Privacy of Customers of Broadband and Other Telecommunications Services.* URL: https://ecfsapi.fcc.gov/file/60002079344.pdf (visited on 07/26/2019).

[8] Federal Coommunications Commission (FCC). *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services.* FCC-16-148. Docket 16-106. 31 FCC Rcd 13911 (17). Nov. 2, 2016.

[9] Federal Coommunications Commission (FCC). *Restoring Internet Freedom.* FCC-17-166. Docket 17-108. 33 FCC Rcd 311 (1). Jan. 4, 2018.

[10] Google. *Your Privacy – Public DNS – Google Developers.* URL: https://developers.google.com/speed/public-dns/privacy (visited on 07/26/2019).

[11] Benjamin Greschbach, Tobias Pulls, Laura M Roberts, Philipp Winter, and Nick Feamster. "The Effect of DNS on Tor's Anonymity". In: *arXiv preprint arXiv:1609.08187* (2016).

[12] Paul Hoffman and Patrick McManus. *DNS Queries over HTTPS (DoH).* Tech. rep. 8484. (Proposed Standard). RFC Editor, Oct. 2018. URL: http://www.ietf.org/rfc/rfc8484.txt.

[13] Austin Hounsel, Kevin Borgolte, Paul Schmitt, Jordan Holland, and Nick Feamster. "Analyzing the Costs (and Benefits) of DNS, DoT, and DoH for the Modern Web". In: Extended abstract. Colocated with IETF 105. July 22, 2019. DOI: 10.1145/3340301.3341129.

[14] Austin Hounsel, Kevin Borgolte, Paul Schmitt, Jordan Holland, and Nick Feamster. "Analyzing the Costs (and Benefits) of DNS, DoT, and DoH for the Modern Web". Full paper. July 18, 2019. arXiv: 1907.08089 [cs.NI].

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

[16] Internet Service Providers' Association (ISPA UK). *ISPA announces finalists for 2019 Internet Heroes and Villains: Trump and Mozilla lead the way as Villain nominees*. July 2, 2019. URL: https://www.ispa.org.uk/ispa-announces-finalists-for-2019-internet-heroes-and-villains-trump-and-mozilla-lead-the-way-as-villain-nominees/ (visited on 07/26/2019).

[17] Judge Jan E. DuBois. *Center for Democracy & Technology v. Pappert*. Civil Action No. 03-5051. United States District Court, Eastern District of Pennsylvania, Sept. 10, 2004.

[18] Michael L. Katz and Carl Shapiro. "Technology Adoption in the Presence of Network Externalities". In: *Journal of Political Economy* 94.4 (1986). DOI: 10.1086/261409. URL: https://doi.org/10.1086/261409.

[19] Paul Klemperer. "Markets with Consumer Switching Costs*". In: *The Quarterly Journal of Economics* 102.2 (May 1987). DOI: 10.2307/1885068. URL: https://doi.org/10.2307/1885068.

[20] Mark Lemley, David S. Levine, and David G. Post. "Don't Break the Internet". In: *Stanford Law Review Online* 64 (Dec. 19, 2011).

[21] Paul Schmitt, Anne Edmundson, Allison Mankin, and Nick Feamster. "Oblivious DNS: Practical Privacy for DNS Queries". In: *Proceedings of the 19th Privacy Enhancing Technologies*. July 2019. DOI: 10.2478/popets-2019-0028.

[22] United States Supreme Court. *National Cable & Telecommunications Association v. Brand X Internet Services*. 545 U.S. 967. Docket 04-277. June 27, 2005.

[23] *USA Mobile Network Experience Report January 2019*. URL: https://www.opensignal.com/reports/2019/01/usa/mobile-network-experience (visited on 05/05/2019).

[24] W3C. *HTTP Archive (HAR) Format*. URL: https://w3c.github.io/web-performance/specs/HAR/Overview.html (visited on 05/05/2019).

[25] Nicholas Weaver, Christian Kreibich, and Vern Paxson. "Redirecting DNS for Ads and Profit". In: *Proceedings of the 1st USENIX Workshop on Free and Open Communications on the Internet (FOCI)*. Aug. 8, 2011. URL: https://www.usenix.org/legacy/events/foci11/tech/final_files/Weaver.pdf (visited on 07/26/2019).

[26] Liang Zhu, Zi Hu, John Heidemann, Duane Wessels, Allison Mankin, and Nikita Somaiya. "Connection-oriented DNS to Improve Privacy and Security". In: *Proceedings of the 36th IEEE Symposium on Security & Privacy (S&P)*. May 2015. DOI: 10.1109/sp.2015.18.