User Awareness and Behaviors Concerning Encrypted DNS Settings in Web Browsers

Alexandra Nisenoff [†*], *Ranya Sharma*[*], *Nick Feamster*[*]
[*]*University of Chicago* [†]*Carnegie Mellon University*

Abstract

Recent developments to encrypt the Domain Name System (DNS) have resulted in major browser and operating system vendors deploying encrypted DNS functionality, often enabling various configurations and settings by default. In many cases, default encrypted DNS settings have implications for performance and privacy; for example, Firefox's default DNS setting sends all of a user's DNS queries to Cloudflare, potentially introducing new privacy vulnerabilities. In this paper, we confirm that most users are unaware of these developments—with respect to the rollout of these new technologies, the changes in default settings, and the ability to customize encrypted DNS configuration to balance user preferences between privacy and performance. Our findings suggest several important implications for the designers of interfaces for encrypted DNS functionality in both browsers and operating systems, to help improve user awareness concerning these settings, and to ensure that users retain the ability to make choices that allow them to balance tradeoffs concerning DNS privacy and performance.

1 Introduction

The Domain Name System (DNS) is an Internet protocol that maps human-readable domain names to Internet Protocol (IP) addresses. Conventionally, DNS queries have been unencrypted, leaving both queries and responses vulnerable to passive eavesdropping and active manipulation. In recent years, major browser and operating system vendors have begun to deploy protocols such as DNS-over-TLS (DoT) and DNS-over-HTTPS (DoH), which encrypt queries and DNS. With the emergence of this functionality, browsers now have different default settings for encrypted DNS, as well as various configuration options to allow users to customize how their browser performs DNS lookups. As is the case with browser vendors, the "Private DNS" mode on Android uses DNS-over-TLS (DoT) to encrypt DNS queries and responses in between the client and the DNS resolver. Encrypted DNS settings are implemented in subtly different ways, and the settings have a variety of defaults.

These differences lead to the setting behaving in ways with implications users may not understand. Getting users to make informed choices of encrypted DNS settings is difficult due to their technical nature [33]. The obscurity of these settings may be further exacerbated by the lack of information provided to users when they modify these settings. Nevertheless, the implications of these settings are significant: depending on how users configure encrypted DNS, for example, all of a user's DNS queries may be sent to a single DNS provider, such as Google or Cloudflare. Occasionally, such configurations are even changed without a user's awareness, with browser vendors pushing changes to default settings with browser version and operating system upgrades. Although users can typically change these settings, doing so requires an awareness that configuring encrypted DNS settings is possible, knowledge about different configuration choices, and the ability to change these settings. It is important to give careful consideration to default settings and interfaces in light of the fact that they often go unmodified by users [56]. Furthermore, previous research has observed that encrypted DNS is what Clark *et al.* have described as an Internet "tussle space" [11], where various Internet stakeholders may vie for control through technical protocol design. Indeed, Hounsel et al. have identified encrypted DNS as a tussle space [26], and highlighted the importance of designing the encrypted DNS infrastructure and user interfaces in ways that *preserve user choice*. Clark explains the profound importance of maintaining user choice in Internet protocols as follows, "It is important that protocols be designed in such a way that all the parties to an interaction have the ability to express a preference about which other parties they interact with...it matters if the consequence of choice is visible." [11].

The design choices in the encrypted DNS ecosystem have implications for market consolidation and power, corporate visibility into and control over user data, as well as user privacy on the Internet. Given the significant implications of these settings, and users' ability to change them, it is critical to understand how users understand these settings and interact with them, which is inherently dependent on how they are presented by vendors.

In this paper, we study encrypted DNS settings in Brave, Chrome, Edge, Firefox, Opera, and the Android mobile operating system. (We exclude Safari because, both at the time of our study and as of February 2023, it does not offer an encrypted DNS setting.) Previous small-scale (approximately ten users) research [40] included a preliminary study of these questions involving Android's Private DNS setting. In this study, we expand on these results to give a larger scale look at how users interact with these settings in the context of browsers. We study the following questions:

- Do users know about and trust encrypted DNS and its

stakeholders? (Section 5.1)
- What encrypted DNS settings do users have enabled in their browsers and phones? (Section 5.2)
- When shown encrypted DNS settings for different browsers, which settings do users choose, and why? (Section 5.3)
- When the technical aspects of these systems are explained to users, do their preferences for settings change? (Section 5.4)

Summary of findings. Many users have heard of DNS but do not know what it does. Even users who believed they knew about DNS's function were often incorrect in describing it. Users typically had the default settings enabled in their own browsers. When users deviated from the default, they tended to select either Cloudflare or Google as their recursive resolver or simply disabled the setting. In many cases, the default setting opportunistically encrypts their DNS queries. In mobile devices, a surprising number of users had the "Private DNS" setting disabled, despite that not being the default setting.

More than 70% of participants continued to use the default encrypted DNS settings without additional information being provided, and this tendency varied across different interfaces. Moreover, the way the settings were described played a role in users' decision making. 37% of participants chose to change their encrypted DNS settings after receiving an explanation of DNS and encrypted DNS. Although the defaults remained popular, users did select a variety of settings after receiving more information. The setting to enter a custom resolver was not often selected, but when participants did attempt to specify a custom resolver, none of the participants entered text that would have functioned properly. Participants seemed to understand the settings better after an explanation, yet they still had problems understanding the differences in functionality and privacy guarantees among the different resolvers.

Summary of recommendations. These results lead to a number of practical recommendations for designers of encrypted DNS interfaces, standards bodies, and other policymakers, which we detail in Section 6. In particular, users need a basic primer on DNS, its associated privacy risks, the guarantees that encrypted DNS can (and cannot) provide, and an intuitive way to understand the implications of the choices for different recursive resolvers. Users also need easier ways to customize the choices for trusted recursive resolvers, once the implications of these choices are clear. Future work can and should expand on our initial findings to explore interfaces for configuring encrypted DNS that provide users choices for configuration, as well as a clear understanding of the implications of these choices.

2 Background and Related Work

This section surveys background and related work on encrypted DNS, including the basic operation and privacy risks of DNS queries, the functionality of encrypted DNS, and the history of the introduction of encrypted DNS into modern browsers and operating systems. We also survey past related work concerning users' awareness of privacy settings in browsers, including encrypted DNS.

2.1 Background: DNS and Encrypted DNS

Most Internet connections are preceded by a Domain Name System (DNS) lookup, which maps a human-readable name to an Internet protocol (IP) address that a client can use to ultimately connect to a remote destination or service. DNS queries and responses have historically been unencrypted, and they may contain sensitive information including information about the site that a user is visiting. Previous research has shown that observing a user's DNS queries can allow users to be tracked across multiple websites [9, 22, 38]. Beyond tracking users online, DNS traffic can also be used to infer what "smart" Internet of things (IoT) devices are present in a home, and may even expose information on how people use them [5, 6, 34]. Some Internet service providers have logged DNS queries to their resolvers and shared them with third parties [14]. Because these queries are typically made in plaintext, anyone who can observe a user's network traffic could see the contents of these queries. Outside of the privacy implications of the DNS, there are also potential concerns with integrity, where the responses to DNS queries may be modified resulting in users receiving the incorrect IP for a website; a censor may be able to implement this type of manipulation to block access to a legitimate website or redirect users to another website entirely [9, 44].

To mitigate some of the security and privacy issues with DNS, Internet operators and vendors have introduced DoT and DoH, both of which send DNS queries using encrypted protocols, with subtle differences in their implementations [24, 30]. Encrypting DNS queries and responses prevents passive eavesdroppers from observing the content of users' DNS queries. DoT sends queries over a Transport Layer Security (TLS) connection using port 853, while DoH uses HTTPS rather than TLS for the transport protocol, typically on port 443. Because DoT uses a dedicated port, it is easier to monitor and detect (and potentially block); on the other hand, DoH uses port 443 for transport and thus DoH traffic tends to be more difficult to identify, particularly when combined with other HTTPS traffic [41]. Although both of these protocols encrypt DNS queries and responses, they are still susceptible to various attacks, ranging from downgrade attacks to traffic analysis-based inference attacks [29, 31, 32, 48, 53].

Using DoH and DoT can provide users with many benefits, but there are downsides to using these protocols as well. Many existing systems such as parental filtering, safe search, or malware detection tools rely on access to the content of DNS queries. However, encrypting those queries while using DoH or DoT can sometimes inhibit the functioning of these systems [13, 14, 27, 35, 37]. Similarly, because Internet service providers (ISPs) can be required by government to block

access to certain illegal content, implementation of encrypted DNS may in some cases prevent ISPs from complying with these laws [45]. On the privacy front, because DoH and DoT need to communicate with resolvers that support these protocols, encrypted DNS may result in users' queries being sent to fewer resolvers, allowing them to see more of a user's online behavior, given that fewer entities can observe more of a user's DNS queries [8, 27]. This consolidation is evident in the growing consolidation of hosting authoritative DNS resolution in general [55].

Although DoH and DoT provide security for the queries while they are in transit, these protocols do not prevent the operators of these DNS resolvers from learning about users' queries or ensuring that the DNS resolver returns the correct response. Other proposed improvements to DNS designed to address these issues include: Oblivious DNS [47], Oblivious DNS over HTTPS [54], secure DNS (DNSSEC) [7, 15], query name (QNAME) minimization [10], and dividing queries across multiple resolvers [23, 28].

2.2 User Awareness of Encryption and Privacy Settings

This study focuses on user awareness concerning encrypted DNS and its configuration through common interfaces, but many other studies have investigated how to communicate security and privacy concepts to users. While usually less buried in setting menus, private browsing modes are included in browsers and do not store browsing history, cookies, or temporary files across sessions. Research has shown that users have many misconceptions about what these settings actually do. Much like encrypted DNS settings, each browser provides a unique description of each setting, which both play a role in what protections the users think the setting provides and have been shown to be insufficient in correcting common misconceptions about what the settings do [18, 59]. Other research into the communication of security risks to users have covered topics such as SSL warnings [4, 16, 50], visual icons [17, 21], privacy policies [51, 57], privacy notices [46], social media privacy settings [36], and cookie consent interfaces [20]. In the realm of encrypted DNS settings, one small-scale exploratory study found that users do not understand the impact of different setting options in the PrivateDNS setting on Android and that most users would initially choose the default options, but when given more information on the setting, some users did choose to modify their choice [40]. In this paper, we expand on those ideas and explore encrypted DNS settings in the browsers on a larger scale.

Several studies have shown that users make incorrect assumptions about the security guarantees of encryption, have doubts about the protection from adversaries, misunderstand phrases like end-to-end encryption, or have incorrect mental models relative to protection provided in different contexts [2, 3, 12, 19, 49, 58]. Technical jargon, paired with inconsistent terminology, can also make tools that use encryption even more difficult for the average user to use correctly [1]. Beyond how users react to and interact with settings, it is also helpful to understand users' perception of encryption in other contexts. If individuals use encryption tools incorrectly, they can have a false sense of security or get themselves into situations where they can no longer perform the tasks they were originally attempting to do.

3 Interfaces for Configuring Encrypted DNS

Vendors have increasingly added support for encrypted DNS, including Web browsers and mobile devices. In this section, we survey the current state of the interfaces for configuring encrypted DNS in common Web browsers. We focus in particular on the interfaces for configuring encrypted DNS in five different popular browsers—Chrome, Brave, Firefox, Microsoft Edge, and Opera—and one mobile operating system, Android. We focus on how these settings are presented to users in the United States; these interfaces may differ in other regions or countries.

Figure 1 shows the encrypted DNS setting interfaces for Brave, Chrome, Edge, Firefox, and Opera. Table 1 and Table 2 have detailed descriptions of the encrypted DNS interfaces and the resolvers that they support. Encrypted DNS interfaces fall into two categories: (1) Chromium-based interfaces (Brave, Chrome, and Edge) and (2) Firefox/Opera. Chromium-based browsers refer to encrypted DNS as "secure DNS" and default to opportunistically using the user's default DNS resolver, while falling back to sending unencrypted DNS queries if the encrypted DNS resolver is unavailable. Edge provides many of the same options for settings to users, but does so in a slightly different way: When a user selects a resolver from the drop down menu, Edge automatically fills the text box for selecting a custom resolver with the resolver's URL allowing it to be edited by the user.

In contrast to Chromium-based browsers, Firefox and Opera refer to the encrypted DNS setting as "DNS-over-HTTPS" and do not provide support for an opportunistic mode, where the browser will encrypt queries if the DNS resolver they were already using supports DoH, as Chromium browsers do. Firefox's default behavior is to use encrypted DNS with Cloudflare as the default resolver; in contrast, Opera disables encrypted DNS by default. When encrypted DNS is enabled, Opera uses Cloudflare as the default resolver. Only Opera explicitly mentions that DoH uses third-party services; rather than falling back to unencrypted queries, it alerts users that a page was inaccessible, mentioning that the DNS-over-HTTPS setting may be to blame. As far as selection options of resolvers shown to users, Mozilla operates a Trusted Recursive Resolver (TRR) program, which ensures that DoH providers recommended by Firefox best protect privacy by not over-collecting and sharing data [39]. Some of the resolvers shown in these interfaces offer additional features

[1]This was a best-effort attempt to identify the first version where the setting appeared, based on news articles, GitHub issues, and release notes.

Platform	Browsers: Chromium	Browsers: Firefox	Browsers: Opera	Mobile: Android
Version Where Introduced[1]	Brave 1.7, Chrome 83, Edge 86	Firefox 73	Opera 65 Beta	Android 9 Pie
Setting Name	Secure DNS	DNS over HTTPS	DNS-over-HTTPS	Private DNS
Protocol	DoH	DoH	DoH	DoT
Default	Opportunistic	Cloudflare	Disabled	Opportunistic
Support for Opportunistic use of Encrypted DNS	●	○	○	●
Warning for Malformed Custom DNS Resolver URL	●	●	○	○
Links to Privacy Polices for Resolvers Shown to Users	●	○	○	No resolvers shown

Table 1: *Summary of encrypted DNS interfaces.*

Browser	Cloudflare	CleanBrowsing	Google	NextDNS	OpenDNS
Chrome	●	●	●	●	●
Firefox	●	○	○	●	○
Edge[2]	●	●	●	●	●
Opera[3]	●	○	●	○	○
Brave[2]	●	●	●	●	●

Table 2: *Resolvers listed in encrypted DNS settings interfaces by different browser vendors.*

such as blocking malware or adult content.

"Private DNS" in Android is the only mobile operating system that we include in our analysis. Unlike the browser-based settings, "Private DNS" supports DoT rather than DoH. By default, DoT encrypts DNS queries to whichever resolver the user has selected; Android's private DNS will fall back to unencrypted queries if DoT fails. In contrast to the settings in browsers, Private DNS does not give the user any suggestions of resolvers, forcing the user to input their own URL for a resolver. This mode will not fall back to unencrypted queries and can cause web pages or resources to become unavailable if, for example, the user inputs an invalid URL.

4 Method

To learn more about participants' understanding of encrypted DNS settings in browsers, we designed a two-part survey. In the first part of the survey, we asked participants about their usage of different browsers. Based on the answers from the first part of the survey, the second part of the survey then asked users to interact with a high-fidelity interface for encrypted DNS settings designed to resemble their browsers. We also asked users about encrypted DNS settings in their own browsers. In this section, we first describe the survey design and recruitment methods; we then discuss the limitations of our survey design, as well as the ethical considerations

[2]After the survey was distributed Quad9 was removed from the list of resolvers in Brave & Edge.

[3]Opera offers multiple versions of the Cloudflare resolver, including versions that block adult content and malware.

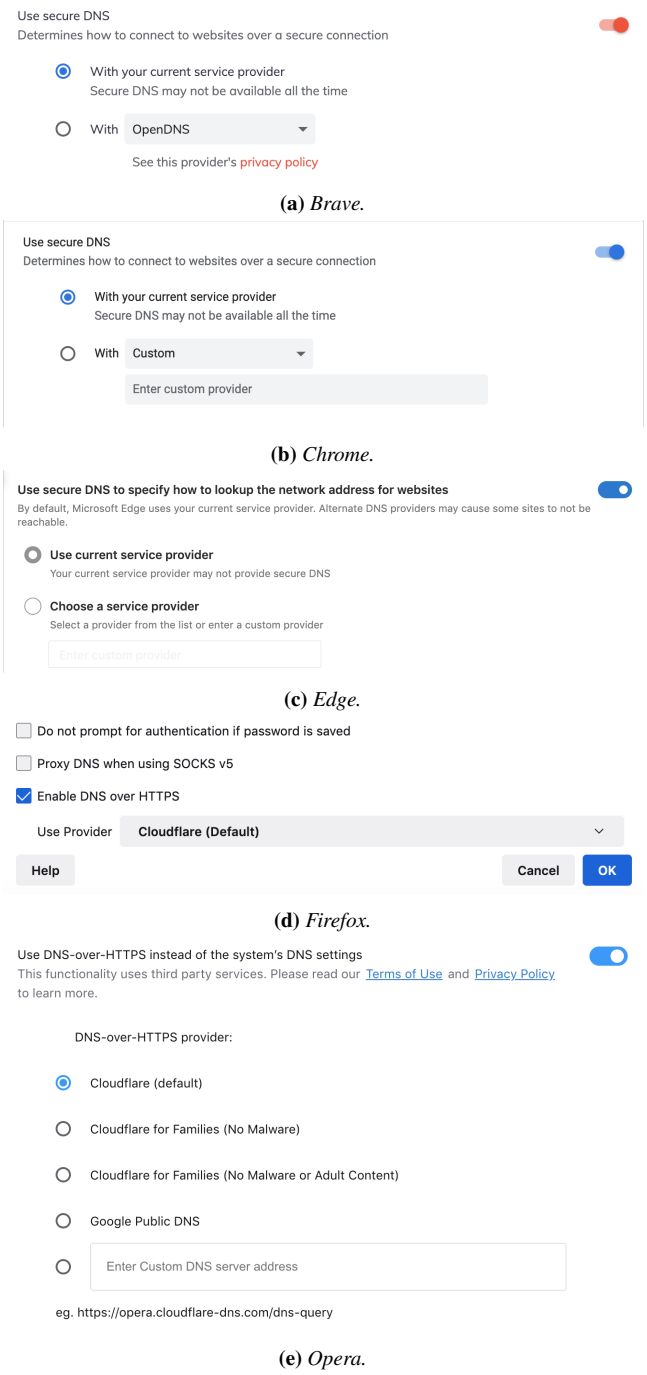
Initial Browser	# in Pool	# Took Survey Before Filtering
Brave	56	34
Chrome	424	50
Edge	110	50
Firefox	126	50
Opera	23	5
Total	**739**	**189**

Table 3: *Eligible survey participants and initial assignments to subgroups before filtering. Figure 2 reflects the number of participants after filtering and reassignment to browsers based on access at the time they took the second survey.*

associated with our survey design. This study was approved by our university's Institutional Review Board (IRB).

4.1 Study Design

Overview: Two-Phase Survey. Before starting either of the surveys, respondents were asked to read a consent form and agree to participate in the study. If a participant was not eligible to participate (e.g., only having access to browsers not included in our study), the participant was immediately redirected to a survey termination page. In the initial survey, we asked 800 participants about their use of different popular web browsers as well as filler questions about their mobile and Internet service providers. Based on their responses to these questions, we assigned participants to subgroups determined by the browsers they reported using at least once a week. Table 3 shows the distribution of users who were assigned to each sub-group. We included users who reported using multiple browsers at least once a week in the grouping for the least commonly used browser they mentioned, to balance out sample sizes across browsers, and to ensure that we recruited participants who used a variety of major browsers that offer encrypted DNS. We excluded participants that failed attention checks, as indicated by the differing number of participants



(a) *Brave.*

(b) *Chrome.*

(c) *Edge.*

(d) *Firefox.*

(e) *Opera.*

Figure 1: *Encrypted DNS settings interfaces for different browsers.*

at different phases of Figure 2.

Participant Assignment. After assigning participants to subgroups according to each browser type, we invited up to 50 participants from each group to participate in a second, longer survey. For some of the less-commonly used browsers (Brave and Opera), we were only able to recruit a lower number of participants. In the second survey, following the consent form, we asked participants if they had heard of the DNS before

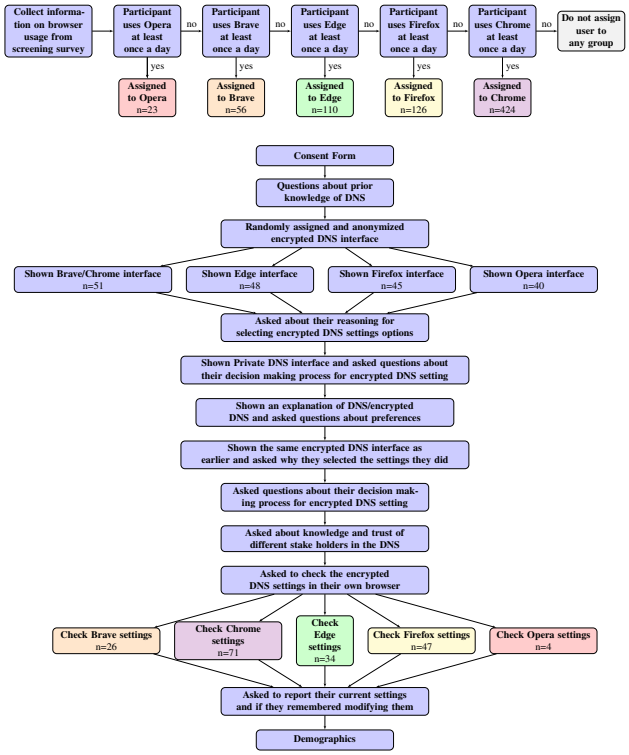


Figure 2: *Overview of Survey Structure. The numbers presented in this figure represent the final number of participants whose data were analyzed after all filtering.*

this study, and if they knew what DNS did. To discourage dishonest responses, we informed participants that they did not need to have prior knowledge of the DNS to continue with the survey. After this step, we randomly assigned participants to an anonymized version of actual DNS settings that can be found in browsers. Because we only had a small number of participants who used browsers with smaller market shares, our intent with randomization was to achieve a better sample of responses for interfaces with less-popular browsers, without biasing those responses based on the user's current browser. Rather than simply showing them a screenshot of their assigned interface or just giving them a multiple choice question with the different settings options, we embedded interactive versions of the browser directly in the survey so that participants could interact with them in the same way they would in their own browser.

Data Collection. We recorded information about how participants interacted with the interface they were shown. We logged not only the final options that they selected, but also how they interacted with the interface before making a final selection to gain better information about whether a user may have been confused by settings options or interfaces. Before being shown the interface, each user was asked to select the setting that they would choose if they encountered it in their own browser. These interfaces were based on Chrome, Brave, Edge, Firefox, and Opera. We removed any reference to the

browser itself from the interface to reduce potential reputation bias, but we opted to leave the actual company names for any recommended resolvers as this best simulates a real browser interface. We merged the Chrome and Brave interfaces because the interfaces used the same terminology and layout; we showed users all of the resolvers that are available in both browser interfaces. After interacting with the settings screen, we asked all participants about their rationale for choosing different options, as well as their understanding and perceptions of the different options. We also showed participants an interactive version of the Private DNS settings on Android and asked about the settings that they would choose.

After collecting participants' responses, we then described the DNS and checked the participants' understanding through a multiple-choice question about the basic functionality of DNS. To ensure that our descriptions of DNS and encrypted DNS were understandable, we performed informal think-aloud pilot tests with six people from various backgrounds and iteratively edited the description. For participants who met the inclusion criteria, we then explained, in more detail, how the specific settings work, and asked for their thoughts.

We then showed participants the interactive encrypted DNS settings screen that they saw earlier in the survey and asked them once again to decide what options they would choose and why. This allowed us to understand how respondents changed their settings after gaining a high-level understanding of what encrypted DNS does and the benefits it provides. We subsequently asked participants if they had heard of encrypted DNS before the survey. (We decided to ask this question after participants chose their setting in the anonymized interfaces because we did not want to bias them while they looked at the simulated settings interfaces that referred to encrypted DNS through different names.) We also briefly asked participants about their preferences between different ways of distributing DNS queries and other security trade-offs to better understand how participants viewed tradeoffs between usability and privacy associated with encrypted DNS.

The next section of the survey asked participants about their knowledge and trust in different DNS resolvers and other parties that are relevant to DNS, such as Internet Service Providers (ISPs) and browsers. Subsequently, we asked participants to report on the current DoH settings in a browser that they regularly use. We also asked about their experience with these settings. The browser that we showed to each participant depended on the respective response to the screening survey: If for some reason, a participant did not have access to the browser subgroup that we assigned them to, we reassigned the participant to another browser that they did have access to. In the case that they did not have access to any browser that offers an encrypted DNS settings interface they moved directly on to the next section of the survey. This was only the case for two users which explains the difference in Figure 2 between the number of participants that saw the anonymous interfaces and checked their own settings. We then asked participants about the operating system of their primary mobile phone. If a participant reported using a phone with an operating system that supported DoT, we asked the participant to check their DNS settings and answer questions about their use of those settings. We concluded the survey with basic demographics and an optional question for participants to leave feedback.

Data Analysis. We collected both quantitative and qualitative data. Qualitative coding was performed on all free-response questions that participants were shown. For each question, one member of the research team read through all of the responses to create a codebook and used it to assign codes to each response. A second member of the research team coded the same responses using the codebook created by the primary coder. All disagreements in codes were resolved through discussion between the primary and secondary coders. As an attention check, we excluded participants that incorrectly answered the question about the function of DNS after our explanation or answered free response questions with responses that were unrelated to the prompts. The statistics reported in this paper are statistically significant, based on the results of a t-test with a significance level of 0.05. For comparisons that looked at differences before and after we showed the user a description of DNS and encrypted DNS, we also applied a paired t-test with the same significance level.

4.2 Recruitment

We recruited participants via Prolific, where we required that they were at least 18 years old, live in the US, and have completed at least 100 surveys before the first survey with at least a 95% approval rating, all common techniques to increase the likelihood of quality crowdsourced responses. The recruitment text of the survey was phrased as a set of surveys where individuals would be asked about network settings and did not mention encrypted DNS or security to avoid self-selection bias. Participants were also asked to complete the survey on a desktop or laptop computer to avoid formatting issues. The first part of the survey was designed to take approximately four minutes while the second part was designed to take approximately 20 minutes. Participants were paid $0.50 and $3.30 for completing the first and second parts, respectively. Payments were made within 72 hours of the participants completing the survey through the Prolific platform. We only compensated participants who completed the full survey. Table 4 summarizes the demographics of our participants. Figure 2 illustrates the flow of the survey.

4.3 Limitations

This study design has several limitations. First, the encrypted DNS interfaces were shown to participants in the context of a survey, rather than in the context of other settings in their browser's settings menu. Showing users these menu options in the specific context of a study and survey on encrypted DNS might in some cases affect the nature of responses, given that users were only presented the part of the configuration menus

Gender	#	CS or CE or IT Background	#
Female	75	Yes	38
Male	109	No	140
Non-binary	0	Prefer not to answer	6
Prefer to self describe	0		
Prefer not to answer	0		
Age	**#**	**Education**	**#**
18 - 24	18	Less than high school	2
25 - 34	59	High school graduate	20
35 - 44	47	Some college	31
45 - 54	32	2 year degree	17
55 - 64	15	4 year degree	74
65 - 74	11	Professional degree	32
75 - 84	2	Doctorate	6
Prefer not to answer	0	Prefer not to answer	2

Table 4: *Participant demographics.*

specifically associated with encrypted DNS. Informing participants that their choice of encrypted DNS setting would not affect the settings of their actual browser may also have influenced the options that they chose in the survey, since users knew that their choices in the survey would ultimately not have any practical effect on their own user experience, or their privacy. The survey-based setup also prevented users from experimenting with different settings. In an actual browser, a user might experiment with several settings to see their impact, which was not possible in this survey.

Some of our survey questions, such as those concerning the operation and functioning of the DNS, asked participants to take their best guess, rather than asking them to specify an option such as "I don't know". This was done to avoid participants from guessing the correct answer, which would have introduced bias into the survey. However, this also means that we cannot determine how many participants did not know the answer to a question (i.e., it is impossible for these questions to distinguish a correct random guess from a user who actually knew the correct answer). Providing "I don't know" options has also been shown to cause participants to disengage from surveys [52]. It also might have made sense to provide a "no basis to judge" option for the question concerning trust in resolvers; we did ask users about their familiarity with each of these providers and did perform a separate analysis based on this subset, with no substantial differences in trends.

The participant sample also has some limitations, as the sample demographic (Prolific users) may not directly correspond to a population sample for the relevant target population (all browser users). Our sample of participants was skewed towards male participants. The results of this survey may thus not necessarily generalize to a broader population. Nevertheless, these survey results are still useful because the goal of this work is not to make general statistical claims about the broader population, but rather to gain insight into how users make choices with regard to encrypted DNS settings. In this case, a sample of the general population is likely to shed light on similar issues and insights as they pertain to encrypted DNS. It may not be advisable to cite percentages of respondents in this paper as they might pertain to the general population, but we do expect that the trends that appear in this study would also be *present* in the general population and thus, the issues that come to light in this study are some that designers of encrypted DNS interfaces should consider.

Limited attention is always a potential limitation. We mitigate this concern by removing participants that did not understand the description of DNS or gave answers to free-response questions that were consistently unrelated to the questions, as a form of attention check.

Finally, our survey design potentially introduces some ordering effects when attempting to understand the effects of prompting and education on how users make choices about encrypted DNS settings (e.g., survey respondents might feel as though they need to change their answers because they are being shown the same question once again). An alternative strategy would have been to conduct a randomized controlled trial, with a subset of participants given the explanation at the beginning of the survey instead of in the middle. We ultimately did not take this approach due to the complications of implementing a randomized controlled trial (RCT), such as full blinding, smaller sample sizes due to stratification; thus, our claims about the effectiveness of user education concerning encrypted DNS should likely be compared against a future RCT-based study. Nonetheless, although our results should not be used to draw causal relationships between education and informed choice, the effects of user prompting about encrypted DNS settings (as might be done in real-world interfaces) are nonetheless valid.

4.4 Ethics

This study was approved by our university's Institutional Review Board (IRB) and was designed following the ethical principles outlined in the Belmont Report: (1) respect for humans; (2) beneficence (risk vs. benefit); (3) justice (beneficiaries versus those who bear the risks). With regard to respect for humans, as the reviewers point out, tracking is naturally a concern.

Respect for humans was considered as part of the consent process and survey design: Due to the short nature of the screening and main surveys, participant fatigue was not expected or reported. Before taking either the screening or main surveys, participants provided their consent to participate via a form, which informed them about the structure of the survey and their rights as a participant. When participants were shown the simulated encrypted DNS settings interface, they were informed that their choice of setting would not affect the setting in their own browser. Participants potentially garnered some benefit from taking this survey by having the opportunity to learn more about the potential risks and benefits of encrypted DNS settings which might enable them to make more informed DNS settings choices in the future. From the

perspective of justice, the benefits of this survey are likely to benefit the same population as that of the respondents: Internet users who depend on web browsers and mobile operating systems (and the underlying DNS) to access websites and Internet services. Throughout the survey, we did not collect any personally identifiable information (PII) beyond general demographic information.

We note the low-risk nature of the data that we collected, specifically: the (a) timing of clicks and (b) the state of the interface within the embedded HTML. We used this timing data as both a sanity check to see that the HTML was functioning properly, as a redundant check to validate that users' final decisions were properly recorded, and for specific analysis (e.g., if users even saw the resolvers listed in drop-down menus). Note that all data collected was exclusively within the context of the survey itself; we do not collect any information about the user's interactions with their browser outside of the HTML interface embedded directly in the survey, or even interactions with other parts of the survey. The timing data contains the number of milliseconds since the page loaded and the interaction the user took at that time (e.g., toggled encrypted DNS off, opened drop-down menu of DNS resolvers, the incorrect URL format warning was shown, etc.). We implemented these interfaces, adding code to observe user clicks on specific elements of interest in the custom HTML and a log of the resulting effects from the code (e.g., the drop-down menu closed because they clicked on the "my current service provider" option).

Due to both the minimal nature of the data collected (i.e., timing data only) and the context in which it was collected (i.e., exclusively within the context of the survey form), we reasoned that there was minimal risk of harm (the IRB concurred). The users consented to participate in the study at the beginning of the survey, but disclosing that we were timing certain interactions could have invalidated our results, because it would have impacted how they interacted with the interfaces or survey at large (e.g., knowledge about being timed or otherwise under time pressure might affect their process, such as rushing to make a decision). Given the minimal risk, we applied the Belmont Report principle of beneficence, reasoning that the benefits of not disclosing this part of the process to users outweighed the risks of potentially invalidating the results.

5 Results

In this section, we present the results from our survey and highlight prevailing themes that emerged during our analysis.

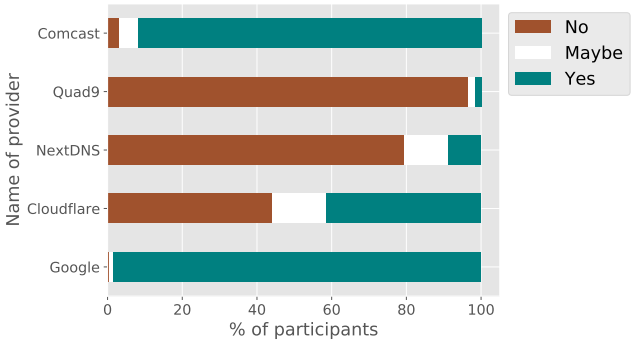


Figure 3: *Percentage of participants who had heard of different stakeholders in the encrypted DNS ecosystem.*

5.1 Do users know about and trust encrypted DNS and its stakeholders?

> Many participants had heard of DNS before the survey, yet fewer had heard of encrypted DNS. Of the participants that had heard of DNS, most did not know what it did, and many who thought they knew what it did were unable to correctly describe its primary function.
> Participants were largely ambivalent about their trust in companies that are not well-known in contexts other than DNS, while they had stronger opinions on their trust in other well-known companies, as well as other stakeholders in the DNS ecosystem with whom they had preexisting relationships (e.g., their primary browser or ISP).

Participants frequently reported having heard of DNS, but often did not know what it did or had incorrect assumptions about its function. 73% of all participants reported having heard of DNS before the survey, with 36% of the participants believing that they knew the functionality that DNS provides. Although participants could overstate their knowledge of DNS, we attempted to mitigate this possibility by asking the question at the beginning of the survey and clearly stating that individuals would be able to participate in the survey regardless of whether they had any knowledge of the DNS. The majority of participants who self-reported having a background in computer science, computer engineering, or information technology stated that they had heard of DNS and knew what it does. Over three times as many participants that did not report having a background in these areas reported having heard of DNS but not knowing what it does or having never heard of DNS than reported that they knew what DNS does.

When participants who claimed to know the purpose of DNS were asked to describe it in their own words, fewer than half mentioned the DNS as being responsible for translating domain names to IP addresses. The other participants had

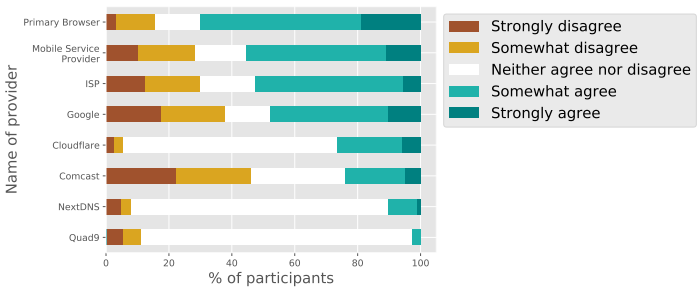


Figure 4: *Percentage of participants who trust their encrypted DNS provider.*

varying misconceptions of its purpose, including identifying computers on a network and connecting a device to the Internet. One participant (P98) stated that DNS was a "denial of service. blocks access to a website. prevents connection." Another (P95) explained, "It is a device naming system that connects devices to the Internet with unique identifiers." Thus, fewer than 18% of the participants could describe what DNS does before being provided with a definition. Of the participants who reported having heard of DNS, only 59.9% had heard of encrypted DNS.

Individuals who had heard of DNS without necessarily fully understanding it may have encountered the term tangentially in other contexts not specific to encrypted DNS. Examples of when users have encountered DNS in the popular press may include: (1) when problems with DNS cause Internet outages and make popular websites and services inaccessible [43]; or (2) when widespread vulnerabilities are disclosed or a major security event occurs [42]. In these cases, people may be exposed to the terminology and a brief description of the DNS, yet we suspect they are likely focused on how DNS affects them, rather than internalizing technical details.

As Figure 3 demonstrates, most participants had heard of Google and Comcast but were less familiar with Cloudflare, NextDNS, and Quad 9. Further, Figure 4 shows that participants were ambivalent about their trust in NextDNS and Quad 9. Both of these factors may be due to participants' lack of knowledge about these providers. Participants were more divided on if they trusted the more well-known companies, Google and Comcast, that also operate recursive resolvers. More participants reported that they trusted their primary browser, mobile service provider, and Internet service provider, which may be related to their familiarity and previous interactions with them.

Because so few participants knew what the DNS was or what DNS queries do, it is unreasonable to expect users to understand the implications that their choices of setting could have on their security and general browsing experience. Thus, even a small description or a link to a more in-depth description of DNS and encrypted DNS could be useful when presenting these settings to users.

Browser	Successfully reached setting (% of participants)	With Current Service Provider	Google	Cloudflare	Disabled	Unsure
Brave	23 (88.5%)	**21**	0	1	1	0
Chrome	58 (81.7%)	**46**	2	0	10	0
Edge	24 (70.6%)	**18**	0	0	5	1
Firefox	43 (91.5%)	N/A	N/A	N/A	N/A	N/A
Opera	3 (75.0%)	-	2	1	**0**	0

default setting

Table 5: *Percentage of participants who reached the encrypted setting page and their subsequent resolver selections.*

5.2 What encrypted DNS settings do users have enabled in their browsers and mobile devices?

> Most participants had the default settings enabled in their browsers, which typically meant that participants' browsers were opportunistically encrypting their DNS queries. The only deviations from the defaults were to disable the setting, or to use Cloudflare or Google resolvers. In the mobile devices, to our surprise, there was a more even split between users that had the default "Automatic" (opportunistic) setting and the setting entirely disabled.

Although most participants were able to access the encrypted DNS settings menu, most still reported that they had the default options enabled, as Table 5 demonstrates. "With Current Service Provider" refers to the resolver that a user's device would use by default, indicating no changes made by the user. 108 participants reported that they could access one of the Brave, Chrome, Edge, and Opera interfaces.[4] One participant was unsure if the setting was enabled. Although the survey provided written instructions and a video describing how to access the encrypted DNS settings in each browser, it is possible that the participants who could not access the encrypted DNS settings menu were using older versions of the browser that did not provide support for these settings. Additionally, participants may have simply been unable to find the setting due to the complexity of browser settings menus. Of the remaining 107 participants, 85 (79.4%) had the default settings for their browser selected.

Only six participants had encrypted DNS configured in such a way that all of their queries went to a single resolver. All of those individuals were using either Cloudflare's resolver or Google Public DNS. No participants reported inputting a custom DNS resolver in their browser. This observation underscores not only the importance of good defaults, but also the careful selection of the suggested resolvers that are shown to users because those are more likely to be selected than a custom DNS resolver. Many of the participants that had a setting other than the default reported not remembering changing the setting. This observation could result in part

[4] Due to an error in the survey, we do not have the actual settings for individuals that looked at their settings in the Firefox browser.

from circumstances, such as not having the most updated browser or operating system, or perhaps having had settings modified by another user on a shared machine.

In the case of mobile devices, 109 participants reported having a phone that ran an Android operating system and 81 reported being able to navigate to the "Private DNS" settings page. Of these participants, 46 (56.7%) had the "Automatic" option selected, 34 (42.0%) had "Off" selected, and only one participant had "Private DNS Provider hostname" selected with the correct URL to send their queries to Cloudflare. "Automatic" is the current default, yet none of the participants that had the "Off" setting selected reported remembering changing this setting in the past. This suggests that perhaps the default of "Automatic" was somehow not applied to them, so while their phone supported the opportunistic mode, they were not taking advantage of the potential benefits of the setting. Participants who were unable to reach the Private DNS settings page may have had older operating systems installed on their phone, and thus might not be able to access the page.

5.3 When shown encrypted DNS settings for different browsers, which settings do users select, and why?

> Most participants chose the default settings in the interface shown to them. There were variations in the settings that users chose based on which interface they were shown. For example, no participants that saw a Chromium-based interface disabled the setting. No participants correctly entered a custom trusted recursive DNS resolver.

When shown the anonymized browser interfaces for encrypted DNS, 71.7% of participants continued to use the default settings shown to them. Participants seemed to trust the default, stating, "Because it is the default, so I feel it is recommended by the software developers." (P135). This percentage varied by browser, with Edge having the highest percentage of users continuing with the default setting (85.4%) and Opera having the lowest, with only 50% of the participants selecting the default. Opera is the only browser that has encrypted DNS disabled by default, which could have been a factor for many people modifying the setting. The predominant reasons participants gave for selecting the settings that they did included: (1) a perceived increase in security, simply because the setting was the default; or (2) because they just didn't know what the setting did. As one participant put it (P144), "It was the default setting and also helps prevent low level attacks from hackers." Participants' choices for the "Private DNS" setting show a similar pattern, with 83.7% of participants keeping the default "Automatic" setting. This finding illustrates the importance of how browsers and mobile service providers configure defaults.

No participants disabled the encrypted DNS setting when shown any of the interfaces for the Chromium-based browsers (Brave, Chrome, Edge); 86.7% of users who were shown the Firefox interface and 50% of participants shown the Opera interface enabled the setting. Chromium-based browsers have a small toggle that collapses the settings window, it is possible that discouraged people from disabling the setting. Furthermore, the option to use their current service provider might have been seen as a lower risk alternative since they already have a relationship with that company: "I chose my current service provider because I trust that it is a great choice since I am currently using it." was how one user expressed the sentiment (P31).

When participants enabled encrypted DNS but did not go with the default setting, they were much more likely to choose a resolver that was listed in the setting rather than specifying a custom resolver. Cloudflare was by far the most popular. Table 6 shows the initial choices of the users.

Although few participants chose to specify a custom resolver in any of the browser (2.7%) or mobile (9.8%) interfaces, the ones who did, entered text that would not function the way they might expect it to. **In fact, no participant entered a custom DNS resolver that would have resulted in their queries being encrypted.** For example "McAfee," "www.google.com," and "1.1.1.1" were entered by participants into the browser and mobile interfaces. In the case of "1.1.1.1", while it may seem correct, to actually use the Cloudflare DNS resolver through the custom resolver input field, the user would need to have entered "1dot1dot1dot1.cloudflare-dns.com" on android or "https://cloudflare-dns.com/dns-query" for any of the browsers. Some interfaces do check whether the text entered will function, but it is often possible to click away from the setting before the warnings are shown. It would be beneficial to users if all of the interfaces, rather than only some, would give users actionable feedback on the validity of their inputs before they exit the page.

When asked about the advantages and disadvantages of enabling encrypted DNS, many participants thought enabling the setting would result in general improvements to security, although they were often unable to go into any detail as to what those security benefits might be, stating "HTTPS has a major advantage of being more secure." (P44) and "I might have more security while using my computer" (P65). Based on survey responses, participants who saw interfaces that labeled DoH as "secure DNS" were more likely to mention security as a potential benefit of enabling DoH than people that saw the setting called "DNS over HTTPS" ($p < 0.05$).This connection between the name of the setting and the perceived impact emphasizes the importance of this subtle difference in wording.

There was confusion among participants about how their choice of encrypted DNS resolver might affect their browsing performance: 19.6% of participants mentioning that the setting could slow down Internet browsing, while 13.0% (not a significantly different number of participants) thought it

Browser	#	Off	With Current Service Provider	Cloudflare	Google (Public DNS)	Quad9	NextDNS	CleanBrowsing (Family Filter)	OpenDNS	Custom
Chrome/Brave	51	0	**37**	6	2	0	0	2	1	3
Edge	48	0	**41**	3	3	0	0	0	1	0
Firefox	45	6	-	**34**	-	-	3	-	-	2
Opera	40	**20**	-	17*	3	-	-	-	-	0
Android	184	12	**154**	-	-	-	-	-	-	18

default setting - indicates that the option is not available for that browser

* The Opera interface offers three versions of the Cloudflare resolver: the default (11), No Malware (2), and No Malware or Adult Content (4)

Table 6: *Users' choice of encrypted DNS setting in the anonymized browser interfaces with no additional information about DNS or encrypted DNS. With current service provider indicates that the resolver would default to the trusted resolver of their ISP.*

might improve performance. Such confusion is consistent with empirical studies, which have shown that the relative performance improvement (or degradation) of encrypted DNS depends quite a lot on the choice of encrypted DNS resolver and client [25].

Aside from the potential effects on speed, participants also mentioned concerns that enabling encrypted DNS might reduce their access to websites with one respondent stating, "If it is security-related, it may restrict access to certain domains." (P6). The desire to be able to access the Internet as they normally do was also mentioned by several participants as the reason they choose their respective settings. Participants overwhelmingly wanted an explanation of the settings to assist with making the decision. For example, one participant (P47) said, "I would have wanted to know what each setting represented in simple terms." Another participant (P14) said, "I would want to know what DNS stands for and what it does, as well as any non-obvious considerations I may want to think through before enabling it." More specific requests included wanting definitions of different relevant terms shown on the settings page, the pros and cons of different settings, and information on the security benefits of each setting.

Interfaces that labeled the setting with the technical name "DNS over HTTPS" caused additional confusion among some participants. **Instead of interpreting the name as meaning DNS *using* the HTTPS protocol they interpreted DoH as meaning use DNS *instead* of HTTPS.** Of the participants who saw the Firefox or Opera interfaces, that label the setting in this way, 10.6% mentioned an incorrect interpretation of the setting name as part of their reason for choosing the setting option that they did. There may have been more participants who misinterpreted the setting name, but they did not mention it in their reasoning for choosing their preferred setting option. One participant (P3) who saw the Firefox interface and chose to disable DoH stated, "I have no earthly idea what DNS is, while I at least have a passing familiarity with HTTPS." Another participant (P30) said "From the little I know I believe that HTTPS is more secure than DNS" and chose to disable the setting in the Opera interface. While most of the participants who misinterpreted the setting name in this way ended up opting to disable the setting, that decision was not universal. This observation highlights the importance of avoiding technical jargon that could be easily misinterpreted by average users.

5.4 When the technical aspects of these systems are explained to users, how do their choices of settings change?

> Almost 40% of the participants modified their settings in some way after being shown an explanation of DNS and encrypted DNS. The default settings remained popular, but much less so than when participants had made decisions without extra information about encrypted DNS. Although participants appeared to demonstrate a better qualitative understanding of encrypted DNS, they still had problems understanding the differences in functionality or privacy guarantees between the different resolvers.

When asked to look at the same anonymous interface they were shown earlier in the survey, after having been provided a description of what the DNS is used for and what encrypted DNS does, 37.0% of participants chose to modify their settings in some way. 30 (16.3%) participants reversed their choice: with an equal number choosing to disable the setting that they had previously enabled and enable the setting that they had previously disabled. Figure 5 shows the relationship between the two settings that users chose before and after receiving an explanation.

Table 7 shows all of the setting options chosen by participants after receiving additional information about each setting. The default settings were still the most selected option across all of the interfaces (58.2%), but the number of participants who selected the respective defaults for each browser decreased across every browser, which is significantly different than the (71.7%) of participants who chose the default before they were provided with additional information ($p < 0.05$).The largest change was seen among users of the Opera browser, with 47.5% of participants choosing to modify their setting in some way. Participants were still more

Browser	#	Off	With Current Service Provider	Cloudflare	Google (Public DNS)	Quad9	NextDNS	CleanBrowsing (Family Filter)	OpenDNS	Custom
Chrome/Brave	51	1	**33**	8	3	0	1	0	2	3
Edge	48	2	**29**	6	4	0	1	1	3	2
Firefox	45	6	-	**28**	-	-	7	-	-	4
Opera	40	**17**	-	19*	4	-	-	-	-	-

default setting - indicates that the option is not available for that browser

* The Opera interface offers three versions of the Cloudflare resolver: the default (11), No Malware (5), and No Malware or Adult Content (3)

Table 7: *Users' choice of encrypted DNS setting in the anonymized browser interfaces after DNS and encrypted DNS has been explained.*

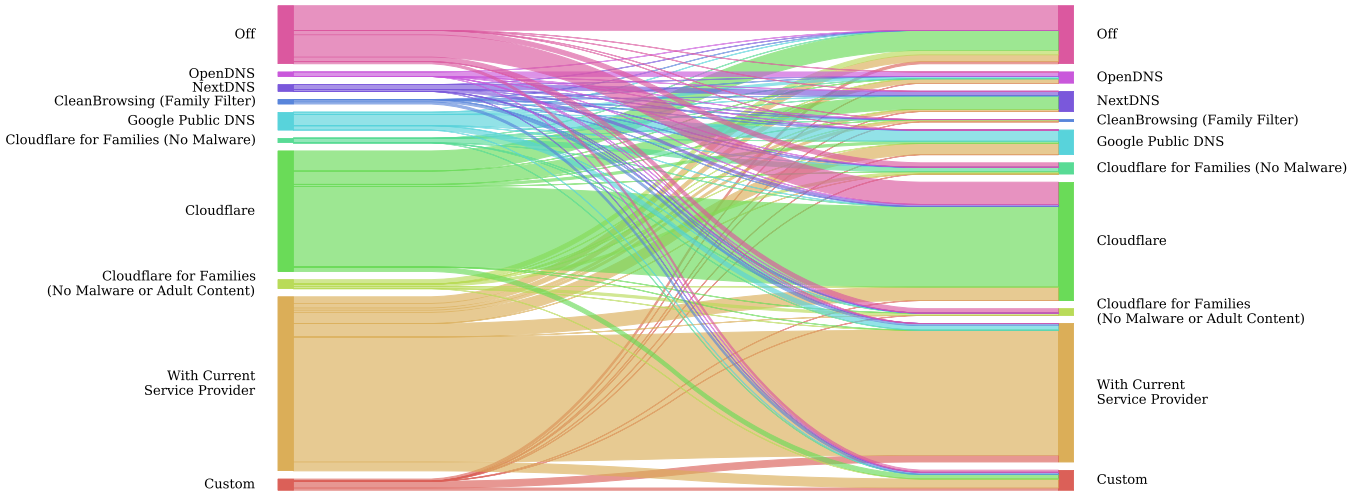


Figure 5: *How users' settings choices changed from their initial choice to their decision after DNS and encrypted DNS have been explained.*

likely to choose a resolver listed in their respective interfaces. Although more people opted to enter custom resolver hostnames again not a single participant added text that would have functioned properly. Because the descriptions we provided to participants did not provide instructions for how to select a resolver, but mainly talked about the settings on a high level, such errors could be expected and were consistent with how participants described their experience; for example, "I understand more about DNS now, but still don't know who else I'd use if not my current service provider" (P46).

Perceived benefits to security remained a predominant factor in many participants' decision-making process. Unlike with their initial choice of setting, privacy and encryption factored into participants' decision-making processes at the end of the survey. For example, when asked why they enabled DNS-over-HTTPS, a participant (P26) stated, "Private browsing and a faster and secure network." Others stated "Seems like it is the correct call for security" (P61) and "Because from what I understand, the DNS gives some privacy so Internet providers don't see your online activity" (P94). Because our descriptions of DNS and encrypted DNS discussed those topics, this result was expected to some degree. Finally, prior knowledge of and trust in a company was a factor users mentioned when explaining why they chose the setting options that they did. When asked why they chose a particular company, one participant stated, "because I already have a relationship with them." (P98). When participants reported having heard of encrypted DNS, they were significantly more likely to enable encrypted DNS as their initial choice when they were not provided with any additional information about the setting ($p < 0.05$). On the other hand, after everyone had been provided with information about DNS and a brief description of encrypted DNS the differences were no longer significant. Note that future work could explore these effects in more detail in a larger randomized controlled trial, as discussed in Section .

6 Discussion

The results from previous sections highlight several general takeaways and point to a variety of recommendations, both for designers and policymakers (e.g., standards bodies, or regulators who may wish to standardize how various protocol options are presented to users).

6.1 Takeaways from Results

Our results highlighted that, although many users have generally heard of DNS and that various configuration options are possible, most users do not change their browser or mobile OS settings from the defaults, and many users also do not understand either how DNS (or encrypted DNS) works, or the guarantees that encrypted DNS can provide which is consistent with research that looked at other privacy settings [20,36,40] Users generally want more information about the privacy benefits that encrypted DNS can provide, as well as information about their options in configuring it. These observations are consistent with Clark's discussions of "tussle spaces", which have noted that the choices that users have (and are aware of) can have significant consequences. As such, encrypted DNS (and interface) implementations should recognize these tussles and make choices available to users in ways that allow them to make appropriate tradeoffs between privacy and performance, according to their preferences.

Additionally, users were concerned that their attempts to customize encrypted DNS configurations could cause basic functionality to break, resulting in their inability to use the Internet. As it turns out, such concerns are not unfounded. For example, specifying a custom recursive resolver with incorrect syntax in the mobile OS configuration does result in a silent connectivity failure, with no error message to the user concerning the nature of the misconfiguration.

Based on these observations, we provide a set of recommendations for designers of encrypted DNS interfaces on user-facing devices (e.g., browsers, mobile OSes) that could allow users to make more informed choices concerning the configuration of encrypted DNS.

6.2 Design Recommendations

Provide a basic primer on DNS function (and privacy risks). Many users are not aware of the functions of DNS, as well as the privacy risks associated with the ability of a third party to observe DNS traffic. We thus recommend that application designers find interface-agnostic ways to provide information to users about DNS function, privacy risks, and the tradeoffs associated with each setting. In some cases, it may be useful to augment the *interface* itself in a way that indicates to the user which entities and organizations can see DNS traffic for different settings, in simple terms (e.g., "your ISP", "the coffee shop's provider", "the web site host"). The exact design of such an interface could be a ripe topic for future work, as we discuss in more detail below.

Provide privacy policies for the resolvers. In principle, users have many choices for trusted recursive resolvers, from major providers (i.e., Google, Cloudflare), to medium-sized operators (i.e., Quad9), to smaller independently operated recursive resolvers. A user's choice of trusted recursive resolver has significant implications for privacy, since the organization operating the trusted recursive resolver sees potentially all of the user's DNS traffic (and hence may be able to infer much about the user, from browsing patterns to other behavior). Our results indicated that while participants understood the setting after it was described to them, they still struggled to understand the differences between different choices of trusted resolvers. Because users have significantly different levels of trust for the respective operators of recursive resolvers, the privacy practices and policies of operators should be more transparent to users to ensure that users can make more informed choices.

Be thoughtful about the use of technical protocol terminology, which may not map to users' mental models. Some technical terminology to describe encrypted DNS protocols can be confusing to users: In particular, we found that many users misinterpreted the phrase "DNS-over-HTTPS", to mean that DNS would be used instead of HTTPS, *not* that HTTPS was the transport protocol over which DNS queries and responses were transmitted. In such cases, understanding the assumptions that users make about functionality based on language choice can help designers choose terminology and phrasing that better reflects the properties that a protocol provides. User studies and focus groups may be appropriate when deploying such protocols and variants, both now and in the future.

Provide users with resolver options. The large collection of data by one or a few mainstream resolvers raises privacy concerns. Per the suggestions of participants, browsers could also add more information about the advantages and drawbacks of different choices of encrypted DNS resolvers, which would allow them to make an educated decision about their browser settings.

Provide users with the necessary format to select a custom resolver and check that the user specification is correct and functional. Participants expressed concerns about experimenting with the settings, fearing that they would break elements of their browsers. Browsers could add more apparent instructions, warnings, or guidelines to their interfaces to provide more clarity for users. Many survey participants also maintained the default setting.

6.3 Future Research

Future work could replicate this study on a larger scale, and across a wider range of demographics. Because encrypted DNS is not limited to the United States, a larger study that captures a broader cross-section of users could deepen our understanding of user perceptions by including participants who live in other countries. Involving more participants could also provide data that may highlight broader themes, including how various attitudes and awareness might vary according to user demographics such as age, level of education, and geography. Future studies could further explore user behavior in the context of their own browsers and mobile operating systems, rather than in the context of a survey. Finally, another

avenue for future work could attempt to design new interfaces that incorporate background information users might need to make a more informed choice.

As opportunistic encrypted DNS becomes more widely adopted, default settings and their implications will become more important. For example, this study explored the extent to which users trust various service providers who offer encrypted DNS; given that opportunistic encrypted DNS is becoming more widespread, other risks, such as downgrade attacks whereby behavior reverts to unencrypted DNS, may become more prevalent, giving rise to the need to assess user understanding of these more subtle issues. We note that in many cases, given current interfaces, the fallback behaviors were unclear, even to us—suggesting the possibility for a more detailed study on encrypted DNS fallbacks and failure modes. Finally, future studies might evaluate the extent to which different phrasing and explanations of settings and options (including the privacy implications associated with different choices of trusted recursive resolver) might ultimately affect users' attitudes and behaviors concerning encrypted DNS settings.

7 Conclusion

The increasing deployment of encrypted DNS in browsers and mobile operating systems has significant consequences for privacy, performance, and reliability—particularly as vendors change default settings (often without direct notification to users). Previous research has observed that encrypted DNS is a tussle space among users, Internet service providers, and content providers because the parties who control DNS have more ability to optimize content and services and have access to potentially sensitive information about users' browsing behaviors and activities. Given the significant stakes of encrypted DNS deployment, users should be able to make informed choices about how it is configured. Interfaces should make it easy for users to be aware of how encrypted DNS is configured, as well as how to change default settings to match their preferences. Our findings in this research confirmed that work is needed in several areas, including: to improve user awareness about the privacy implications of DNS, to provide users with information to better understand the implications of how encrypted DNS is configured, and to design setting interfaces that make these options intuitive for users to customize. Although this paper does not offer the last word on user attitudes and awareness about encrypted DNS, our hope is that it lays the groundwork for more research in this area, to positively affect interfaces, standardization, and policymaking.

Acknowledgments. This work was funded by NSF Award SaTC-2155128 "Understanding Practical Deployment Considerations for Decentralized, Encrypted DNS". Ranya Sharma and Alexandra Nisenoff were supported by NSF Research Experiences for Undergraduates (REU) supplement awards under NSF Award TWC-1953513 "Towards a Science of Censorship Resistance". This material is based upon work supported by the National Science Foundation Graduate Research Fellowship under Grant No. DGE2140739. We thank Allison Mankin, the anonymous reviewers, and our shepherd for comments that helped improve this paper.

References

[1] R. Abu-Salma, K. Krol, S. Parkin, V. Koh, K. Kwan, J. Mahboob, Z. Traboulsi, and M. A. Sasse. The Security Blanket of the Chat World: An Analytic Evaluation and a User Study of Telegram. Internet Society, 2017.

[2] R. Abu-Salma, E. M. Redmiles, B. Ur, and M. Wei. Exploring user mental models of End-to-End encrypted communication tools. In *8th USENIX Workshop on Free and Open Communications on the Internet (FOCI 18)*, Baltimore, MD, Aug. 2018. USENIX Association.

[3] R. Abu-Salma, M. A. Sasse, J. Bonneau, A. Danilova, A. Naiakshina, and M. Smith. Obstacles to the Adoption of Secure Communication Tools. In *2017 IEEE Symposium on Security and Privacy (SP)*, pages 137–153, 2017.

[4] D. Akhawe and A. P. Felt. Alice in warningland: A Large-Scale field study of browser security warning effectiveness. In *22nd USENIX Security Symposium (USENIX Security 13)*, pages 257–272, Washington, D.C., Aug. 2013. USENIX Association.

[5] N. Apthorpe, D. Reisman, and N. Feamster. A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic. *arXiv preprint arXiv:1705.06805*, 2017.

[6] N. Apthorpe, D. Reisman, S. Sundaresan, A. Narayanan, and N. Feamster. Spying on the Smart Home: Privacy Attacks and Defenses on Encrypted IoT Traffic. 2017.

[7] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose. Protocol Modifications for the DNS Security Extensions. Technical report, RFC 4035, March, 2005.

[8] K. Borgolte, T. Chattopadhyay, N. Feamster, M. Kshirsagar, J. Holland, A. Hounsel, and P. Schmitt. How DNS over HTTPS is Reshaping Privacy, Performance, and Policy in the Internet Ecosystem. In *The 47th Research Conference on Communication, Information and Internet Policy*, 2019.

[9] S. Bortzmeyer. DNS Privacy Considerations. *RFC 7626*, 2015.

[10] S. Bortzmeyer. DNS Query Name Minimisation to Improve Privacy. *RFC7816*, 2016.

[11] D. D. Clark, J. Wroclawski, K. R. Sollins, and R. Braden. Tussle in cyberspace: defining tomorrow's Internet. In *ACM SIGCOMM*, pages 347–356, 2002.

[12] S. Dechand, A. Naiakshina, A. Danilova, and M. Smith. In Encryption We Don't Trust: The Effect of End-to-End Encryption to the Masses on User Perception. In *2019 IEEE European Symposium on Security and Privacy (EuroS P)*, pages 401–415, 2019.

[13] S. Deckelmann. What's next in making Encrypted DNS-over-HTTPS the Default.

[14] S. Dickinson. DNS Privacy - The Problem. https://dnsprivacy.org/the_problem/.

[15] D. Eastlake and C. Kaufman. Domain Name System Security Extensions. Technical report, rfc 2535, March, 1999.

[16] A. P. Felt, A. Ainslie, R. W. Reeder, S. Consolvo, S. Thyagaraja, A. Bettes, H. Harris, and J. Grimes. Improving SSL Warnings: Comprehension and Adherence. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, CHI '15, page 2893–2902, New York, NY, USA, 2015. Association for Computing Machinery.

[17] A. P. Felt, R. W. Reeder, A. Ainslie, H. Harris, M. Walker, C. Thompson, M. E. Acer, E. Morant, and S. Consolvo. Rethinking Connection Security Indicators. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 1–14, Denver, CO, June 2016. USENIX Association.

[18] X. Gao, Y. Yang, H. Fu, J. Lindqvist, and Y. Wang. Private Browsing: An Inquiry on Usability and Privacy Protection. In *Proceedings of the 13th Workshop on Privacy in the Electronic Society*, WPES '14, page 97–106, New York, NY, USA, 2014. Association for Computing Machinery.

[19] N. Gerber, V. Zimmermann, B. Henhapl, S. Emeröz, and M. Volkamer. Finally Johnny Can Encrypt: But Does This Make Him Feel More Secure? In *Proceedings of the 13th International Conference on Availability, Reliability and Security*, ARES 2018, New York, NY, USA, 2018. Association for Computing Machinery.

[20] H. Habib, M. Li, E. Young, and L. Cranor. "okay, whatever": An evaluation of cookie consent interfaces. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, CHI '22, New Orleans, LA, USA, 2022. Association for Computing Machinery.

[21] H. Habib, Y. Zou, Y. Yao, A. Acquisti, L. Cranor, J. Reidenberg, N. Sadeh, and F. Schaub. Toggles, Dollar Signs, and Triangles: How to (In)Effectively Convey Privacy Choices with Icons and Link Texts. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '21, New York, NY, USA, 2021. Association for Computing Machinery.

[22] D. Herrmann, C. Gerber, C. Banse, and H. Federrath. Analyzing Characteristic Host Access Patterns for Re-identification of Web User Sessions. In *Nordic Conference on Secure IT Systems*, page 136154. Springer, 2010.

[23] N. P. Hoang, I. Lin, S. Ghavamnia, and M. Polychronakis. K-resolver: Towards Decentralizing Encrypted DNS Resolution. In *MADWeb 2020*, 2020.

[24] P. Hoffman and P. McManus. DNS Queries over HTTPS (DoH). *Internet Requests for Comments, IETF, RFC*, 8484, 2018.

[25] A. Hounsel, P. Schmitt, K. Borgolte, and N. Feamster. Can Encrypted DNS Be Fast? In *International Conference on Passive and Active Network Measurement*, pages 444–459. Springer, 2021.

[26] A. Hounsel, P. Schmitt, K. Borgolte, and N. Feamster. Designing for Tussle in Encrypted DNS. In *Proceedings of the Twentieth ACM Workshop on Hot Topics in Networks*, pages 1–8, 2021.

[27] A. Hounsel, P. Schmitt, K. Borgolte, and N. Feamster. Designing for Tussle in Encrypted DNS. In *Proceedings of the Twentieth ACM Workshop on Hot Topics in Networks*, HotNets '21, page 1–8, New York, NY, USA, 2021. Association for Computing Machinery.

[28] A. Hounsel, P. Schmitt, K. Borgolte, and N. Feamster. Encryption without Centralization: Distributing DNS Queries across Recursive Resolvers. In *Proceedings of the Applied Networking Research Workshop*, ANRW '21, page 62–68, New York, NY, USA, 2021. Association for Computing Machinery.

[29] R. Houser, Z. Li, C. Cotton, and H. Wang. An investigation on information leakage of dns over tls. CoNEXT '19, New York, NY, USA, 2019. Association for Computing Machinery.

[30] Z. Hu, L. Zhu, J. Heidemann, A. Mankin, D. Wessels, and P. Hoffman. Specification for DNS over Transport Layer Security (TLS). *IETF RFC7858, May*, 2016.

[31] Q. Huang, D. Chang, and Z. Li. A comprehensive study of dns-over-https downgrade attack. In *10th USENIX Workshop on Free and Open Communications on the Internet (FOCI 20)*. USENIX Association, Aug. 2020.

[32] K. Hynek and T. Cejka. Privacy Illusion: Beware of Unpadded DoH. In *2020 11th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, pages 0621–0628, 2020.

[33] M. Knodel and S. K. Sahib. DNS privacy vs. In *Proc. USENIX PEPR*, Santa Clara, CA, June 2022. USENIX Association.

[34] F. Le, J. Ortiz, D. Verma, and D. Kandlur. Policy-based identification of iot devices' vendor and type by dns traffic analysis. In *Policy-Based Autonomic Data Governance*, pages 180–201. Springer, 2019.

[35] R. Lemos and D. Reading. Got malware? Three Signs revealed in DNS Traffic. *InformationWeek Dark Reading, May*, 2013.

[36] Y. Liu, K. P. Gummadi, B. Krishnamurthy, and A. Mislove. Analyzing Facebook Privacy Settings: User Expectations vs. Reality. In *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference*, IMC '11, page 61–70, New York, NY, USA, 2011. Association for Computing Machinery.

[37] M. Lyu, H. H. Gharakheili, and V. Sivaraman. A Survey on DNS Encryption: Current Development, Malware Misuse, and Inference Techniques, 2022.

[38] G. C. M. Moura, S. Castro, W. Hardaker, M. Wullink, and C. Hesselman. Clouding up the Internet: How Centralized is DNS Traffic Becoming? In *Proceedings of the ACM Internet Measurement Conference*, IMC '20, page 42–49, New York, NY, USA, 2020. Association for Computing Machinery.

[39] Mozilla. Dns over https (trusted recursive resolver)¶.

[40] A. Nisenoff, N. Feamster, M. A. Hoofnagle, and S. Zink. User Expectations and Understanding of Encrypted DNS Settings. In *NDSS DNS Privacy Workshop*, Virtual Event, Feb. 2021.

[41] P. Nohe. What is the Difference between DNS over TLS & DNS over HTTPS?

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

[43] Dozens of Websites Go Down in a Widespread Internet Outage. https://www.nytimes.com/2021/07/22/business/internet-outage.html, July 2021.

[44] P. Pearce, B. Jones, F. Li, R. Ensafi, N. Feamster, N. Weaver, and V. Paxson. Global Measurement of DNS Manipulation. In *26th USENIX Security Symposium (USENIX Security 17)*, pages 307–323, 2017.

[45] F. Y. Rashid. The Fight Over Encrypted DNS: Explained.

[46] F. Schaub, R. Balebako, A. L. Durity, and L. F. Cranor. A Design Space for Effective Privacy Notices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 1–17, Ottawa, July 2015. USENIX Association.

[47] P. Schmitt, A. Edmundson, A. Mankin, and N. Feamster. Oblivious DNS: Practical Privacy for DNS Queries. In *Proceedings of the Applied Networking Research Workshop*, ANRW '19, page 17–19, New York, NY, USA, 2019. Association for Computing Machinery.

[48] S. Siby, M. Juárez, C. Díaz, N. Vallina-Rodriguez, and C. Troncoso. Encrypted DNS -> privacy? A traffic analysis perspective. In *27th Annual Network and Distributed System Security Symposium, NDSS 2020, San Diego, California, USA, February 23-26, 2020*. The Internet Society, 2020.

[49] C. Stransky, D. Wermke, J. Schrader, N. Huaman, Y. Acar, A. L. Fehlhaber, M. Wei, B. Ur, and S. Fahl. On the Limited Impact of Visualizing Encryption: Perceptions of E2E Messaging Security. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*, pages 437–454. USENIX Association, Aug. 2021.

[50] J. Sunshine, S. Egelman, H. Almuhimedi, N. Atri, and L. F. Cranor. Crying Wolf: An Empirical Study of SSL Warning Effectiveness. In *Proceedings of the 18th Conference on USENIX Security Symposium*, SSYM'09, page 399–416, USA, 2009. USENIX Association.

[51] J. Y. Tsai, S. Egelman, L. Cranor, and A. Acquisti. The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. *Information systems research*, 22(2):254–268, 2011.

[52] Vannette, Dave. Why Including "Don't know" Responses is Hurting Your Survey Data, 2019. https://www.qualtrics.com/blog/why-including-dont-know-responses-is-hurting-your-sur

[53] D. Vekshin, K. Hynek, and T. Cejka. DoH Insight: Detecting DNS over HTTPS by Machine Learning. In *Proceedings of the 15th International Conference on Availability, Reliability and Security*, pages 1–8, 2020.

[54] T. Verma and S. Singanamalla. Improving DNS Privacy with Oblivious DoH in 1.1.1.1.

[55] S. Wang, K. MacMillan, B. Schaffner, N. Feamster, and M. Chetty. A First Look at the Consolidation of DNS and Web Hosting Providers, 2021.

[56] M. Weinmann, C. Schneider, and J. v. Brocke. Digital Nudging. *Business & Information Systems Engineering*, 58(6):433–436, 2016.

[57] S. Wilson, F. Schaub, R. Ramanath, N. Sadeh, F. Liu, N. A. Smith, and F. Liu. Crowdsourcing annotations for websites' privacy policies: Can it really work? In *Proceedings of the 25th International Conference on World Wide Web*, WWW '16, page 133–143, Republic and Canton of Geneva, CHE, 2016. International World Wide Web Conferences Steering Committee.

[58] J. Wu and D. Zappala. When is a Tree Really a Truck? Exploring Mental Models of Encryption. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, pages 395–409, Baltimore, MD, Aug. 2018. USENIX Association.

[59] Y. Wu, P. Gupta, M. Wei, Y. Acar, S. Fahl, and B. Ur. Your Secrets Are Safe: How Browsers' Explanations Impact Misconceptions About Private Browsing Mode. In *Proceedings of the 2018 World Wide Web Conference*, WWW '18, page 217–226, Republic and Canton of Geneva, CHE, 2018. International World Wide Web Conferences Steering Committee.