User Expectations and Understanding of Encrypted DNS Settings

Alexandra Nisenoff, Nick Feamster, Madeleine A Hoofnagle[†], Sydney Zink
University of Chicago and [†]Northwestern
{nisenoff, feamster}@uchicago.edu, madeleine.hoofnagle@northwestern.edu, sydney.zink@gmail.com

Abstract

Domain Name System (DNS) queries map domains that are readable by humans into their corresponding IP addresses. As a way of mitigating the privacy risks associated with DNS queries, protocols such as DNS over HTTPS (DoH) and DNS over TLS (DoT) have been adopted by many major browsers and operating systems. In this paper we present the results of a small-scale online survey with the goal of probing users' sentiments on Private DNS in Android 9 Pie as well as DoH in Firefox. As many users decide to stick with the default setting, it becomes paramount developers choose defaults that benefit users. While many users choose to stick with the default setting, even given additional information, there are users who would change their DNS settings when given information on what the specific settings actually do. We also see that users believe DNS settings accomplish one thing, but actually the settings do something else. Finally, the survey uncovered interesting trends in users' knowledge of and trust in DNS service providers.

1 Introduction

Domain Name System (DNS) queries play an important, but mostly invisible role in users' online interactions. These queries map human readable domains to IP addresses. DNS queries can be triggered in several different ways that may not be obvious to the user. Traditionally these queries are sent unencrypted over UDP, however protocols that encrypt DNS traffic such as DNS over HTTPS (DoH) and DNS over TLS (DoT) have been proposed. Specific implementations of DoH and DoT can result in significantly different privacy concerns that may not be apparent to users. It appears that the design and implementation of these new "safer" features may not always consider user preferences and needs.

Once these settings are enabled, often by default or by onetime opt in, the menus to modify the settings are generally hidden deep within the settings pages and don't provide users enough information to make an informed choice about them. The complicated nature of these settings also makes designing interfaces to clearly present them to users very difficult [21, 23, 35]. The way settings are explained and displayed to users can have a major impact on how users decide what setting to select and further influence their understanding of what the different settings options actually do. The lack of information given at the point of choice, for encrypted DNS settings, is also notable and investigation into how users make a decision is needed.

In this paper we present the findings of a small scale user study where we begin to explore how users interact with, understand and select encrypted DNS settings, particularly as they relate to the encrypted DNS settings in the Firefox web browser and the Android 9 Pie mobile operating system. With this in mind, we studied these questions and found the following trends:

- ***Do users understand what these DNS setting options do?*** We find that users have misconceptions about the different settings options, often believing the defaults are necessary for systems to work properly.
- ***Why do users choose the settings that they do?*** Findings suggest that users will most often leave the default settings in place when they lack information beyond what the settings pages provide.
- ***Does being provided with more information on DNS settings change the settings option that users choose?*** The study shows that information may cause some users to change settings while others choose to remain with their original choice.
- ***Do people know about the different DNS resolvers and do they trust them?*** Users studied here had limited knowledge about DNS resolvers available to them. Trust in the familiar DNS resolvers varied among participants as well.

2 Background

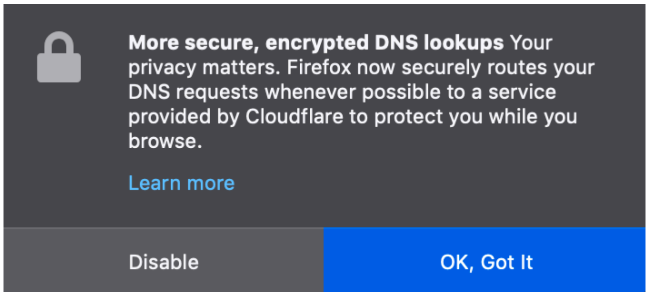
When the DNS system was being designed, the public nature of the DNS information itself led to design decisions that have privacy implications to this day. Given that DNS queries contain the user's IP address and the name of the site that their endpoint is communicating with (e.g., which website they are visiting), an operator of a DNS resolver and any entity who observes the traffic between the client and resolver can use this information to track users across the websites that they visit [7, 12, 25]. Previous research has also shown that an adversary can infer what IoT devices are present and some actions that are taking place within a home [2, 3, 22].

Another concern that can arise is having the IP address returned to the user spoofed, resulting in the user receiving the wrong IP address for a site. This provides an avenue for more active attacks that involve redirecting users' traffic with incorrect DNS responses, which can block access to the actual site, as is the case with censorship or can redirect users to a scam version of the site [7, 27].

2.1 Current Extensions and Improvements

DoT and DoH send DNS queries using encrypted protocols, preventing passive eavesdroppers from observing DNS queries. While DoT and DoH both encrypt DNS requests, there are some subtle differences in their implementation. DoT sends queries over a TLS connection using port 853 [15]. DoH works similarly, except that it uses HTTPS rather than TLS for the transportation protocol, using port 443 [13]. Since DoT has a dedicated port, it makes DoT easier to detect and more useful for network monitoring. Conversely, DoH blends in with the other HTTPS traffic which may have benefits for preventing DNS based censorship [26]. Although the queries are encrypted, these protocols are still susceptible to various attacks [14, 16, 17, 32, 33]. While DoH and DoT provide security for the queries while they are in transit, these protocols do not prevent the DNS resolvers from learning about users' queries. Oblivious DNS (ODNS) and Oblivious DNS over HTTPS (ODoH) mitigate the issue of exposing information to resolvers by hiding the query from the recursive resolver and the original IP address from Oblivious DNS server [30, 34].

While protocols such as DoH and DoT provide many benefits to users, they can also prevent some existing systems from functioning as intended or otherwise make network management difficult. DNS traffic is often used to enable parental filtering, safe search, or malware detection. Without access to the queries these methods might not work [8, 9, 24]. In some places, like in the UK, where ISPs are also required to block access to certain illegal content, implementation of encrypted DNS could prevent ISPs from complying with these laws [28]. Use of these protocols under certain conditions can result in the queries being sent to a smaller number of resolvers which then may have a greater ability to track users [6].



More secure, encrypted DNS lookups Your privacy matters. Firefox now securely routes your DNS requests whenever possible to a service provided by Cloudflare to protect you while you browse.

Figure 1: *DNS over HTTPS popup in Firefox Nightly*

In contrast to DoT and DoH, which are concerned with confidentiality of queries and responses, DNSSEC assures the authenticity and integrity of the DNS responses [4, 11]. To accomplish this, DNSSEC uses digital signatures and asymmetric cryptography. DNSSEC does not attempt to prevent an adversary from viewing the contents of query, as such, it is designed to solve an entirely different problem than DoH or DoT attempt to solve and both can be used simultaneously.

2.2 Implementations

Many browsers and mobile operating systems now provide support for DoH or DoT. In this paper we primarily study Private DNS and DoH in Firefox; additionally, Brave, Chrome, Edge, iOS, macOS, and Windows have all added support for encrypted DNS [1, 5, 10, 18, 37].

Although Firefox has supported DoH since version 62, the option had been turned off by default until early 2020 [8]. Users were notified of this change to the default settings with a one-time pop-up notification, shown in Figure1, allowing them to disable DoH. Users can also disable DoH in their settings menu or opt out ahead of time by setting the "network.trr.mode" to 5 in the Firefox settings page [29]. Because centralizing all of a user's DNS queries can create additional privacy risks, Mozilla devised policy requirements for their DoH Partners. The policies include rules on the data that can be collected or retained, rules about transparency and blocking, as well as technical requirements for operation. Currently the only three resolvers that have contractually agreed to these policies are Cloudflare, NextDNS, and Comcast, with Cloudflare being the default [36].

In Android 9 Pie, Google added in support for DoT through a “Private DNS” option. With Private DNS enabled (the default setting), if the DNS server you are trying to contact supports it, Android will use DoT. If the DNS server does not support DoT, the OS will fall back to not encrypting the DNS queries [20]. Private DNS also offers the option of inputting a Private DNS provider hostname. If this setting is selected, all queries are sent to the specified server. If the server can’t be reached then the network is marked as “No Internet access.” Private DNS secures all DNS queries even ones from apps [19].

3 Method

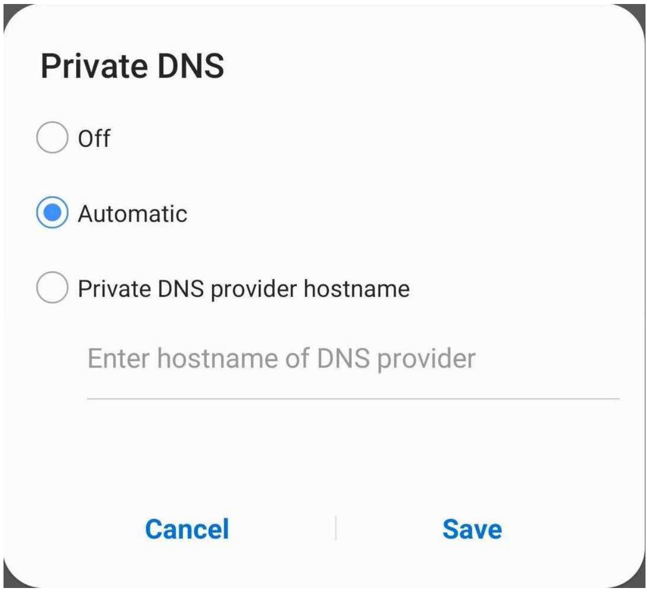
To explore participants’ understanding and opinions of these encrypted DNS implementations, we created a short online survey. The survey had four sections. The first two sections focused on Android Private DNS and DoH in Firefox. The order that they were shown to the participants was randomized. Following those sections, participants were asked about their knowledge of and trust in different DNS resolvers. The survey concluded with basic demographic questions.

3.1 Survey Design

In the section on DoH in Firefox, participants were shown the popup (Figure 1) that is displayed to users, after the update that enabled this feature. They were asked which of the two options from the popup they would select and whether they had seen the popup before taking the survey. To conclude this section, participants were shown screen shots of the Firefox settings menus and were asked questions about how likely they would be to modify the setting or be able to find this setting on their own.

If participants had a phone that supported Private DNS, they were asked to navigate to the Private DNS settings page. If they were able to get to the Private DNS settings page they were asked about their current settings. Users that were not able to navigate to the Private DNS settings page or had a phone that did not support Private DNS were shown images of the Private DNS settings page (Figure 2). All participants were then asked what Private DNS they would choose without any additional information about Private DNS.

After a brief description of DNS was given and a question to confirm that participants had understood the description, participants were asked what aspects of their DNS traffic they would expect to be protected by Private DNS. Following an explanation of Private DNS, participants were asked multiple-choice and open-ended questions regarding their opinions of this setting. Participants were then presented the original settings options for Private DNS and asked what option they would choose given what they had learned about DNS. Finally, participants were asked about their knowledge of and trust in various DNS providers.


Private DNS

○ Off

● Automatic

○ Private DNS provider hostname

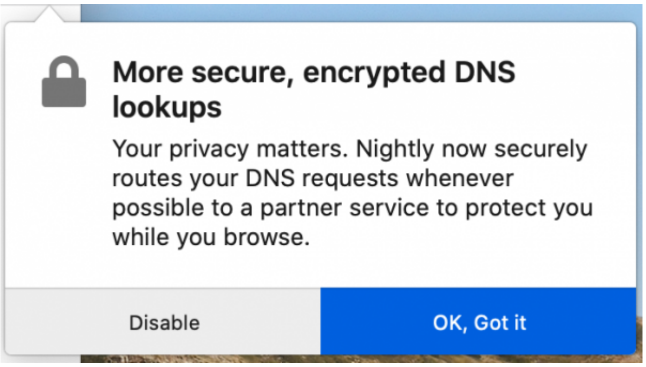
Figure 2: *Private DNS settings page*

3.2 Recruitment

In this survey, we recruited 15 participants via Prolific. To be eligible to take the survey participants needed to have completed 100 prior surveys with a 95% approval rating, be at least 18 years old, and live in the United States. The survey itself was designed to take approximately 15 minutes to minimize fatigue and participants were paid $3. 00 within 72 hours of completing the survey. Due to the formatting of our survey, we also required that the study not be taken on a mobile device.

3.3 Ethics

Before taking the survey, participants provided their consent to participate via a form, which informed them about the structure of the survey and their rights as a participant. Our study was approved by our institution’s IRB. In the course of the survey we did not collect any personally identifiable information beyond standard demographics. Participants potentially garnered some benefit from this survey by having the opportunity to learn more about the potential risks and benefits of Private DNS and DoH in Firefox, which might enable them to make more informed DNS settings choices in the future.



More secure, encrypted DNS lookups

Your privacy matters. Nightly now securely routes your DNS requests whenever possible to a partner service to protect you while you browse.

Figure 3: *Newer DNS over HTTPS popup in Firefox Nightly [31]*

4 Results

For the free response questions, we performed qualitative coding to identify themes that appeared in in users' answers. Due to our modest sample size, the percentages of responses for each theme may not generalize to a more general population.

4.1 Demographics

The participants in our pilot study tended to be young, educated, female, and lacking a technical background. These demographics are consistent with the demographics of Prolific participants as a whole. Of course, this participant demographic is not representative of the demographics of the entire United States (or any general population sample), our goal for this *preliminary* study was not to gather statistics that reflected a population sample but rather to gather evidence that could support a larger future study. In this regard, we believe that this preliminary work can still provide valuable insights into regular Internet users.

4.2 Firefox DNS over HTTPS

None of the participants remembered seeing the Firefox Nightly popup prior to the survey. This result is expected, as only a few participants reported that Firefox was their primary browser. When shown the DoH pop up from Firefox Nightly, most participants said that they would select the "Okay, Got it" option. If they were in their browser, this would result in all of their DNS queries being sent through Cloudflare. The ramifications of this choice may not have been clear to users at the point of choice. Furthermore, in newer iterations of the popup, shown in figure 3, the default resolver is not specified revealing even less information to the user at the point of choice.

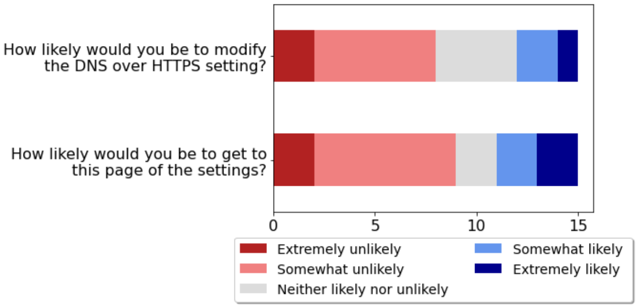


Figure 4: *User responses to questions about Firefox's DNS over HTTPS settings*

When shown the settings page in Firefox where the DoH settings were located, most participants reported that they probably wouldn't have found the settings page and that they wouldn't modify their settings even if they did. This makes it even more important to make the consequences of the initial choice more apparent.

4.3 Private DNS

About half of the participants had a phone that supported Private DNS. Of those seven participants, all but one were able to navigate to the Private DNS Settings page on their phone. Four of the participants had the setting in the default "Automatic" setting and the other two had Private DNS turned off. Most participants reported that they did not remember ever visiting this settings page prior to the survey. Of the three participants that did remember visiting the page, two did remember changing their settings. Further research could look into why users who changed their settings in the past made that particular decision.

When the participants were asked to choose a Private DNS setting without being given any extra information beyond what the settings page told them, most chose to leave it on the default option of "Automatic", while only a few chose to change it to the "Off" setting. Figure 5 shows the percentages of participants that chose each option.

Participants gave a variety of reasons for sticking with the default "Automatic" option. The most common reason was that users gave was that they didn't know what the setting was. Other reasons that people gave were that they thought their phone might not work if they changed the setting and that they stuck with "Automatic" specifically because it was the default option. One participant in particular stated that he trusted Google, and since they had decided that automatic should be the default, it was the best option for them. Reasons for not selecting the "Off" option included that users didn't think it was worth it or thought it might

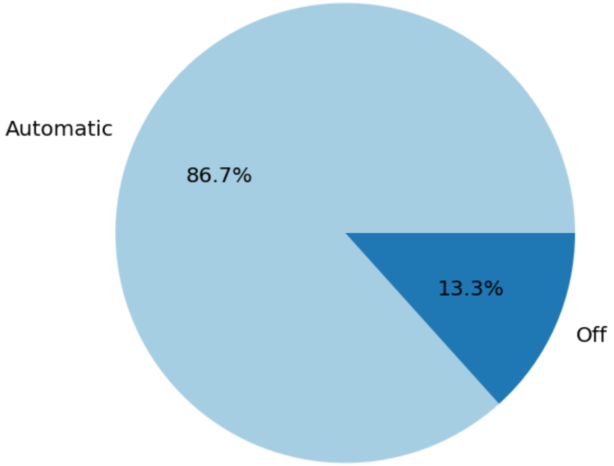


Figure 5: *Users' choice of Private DNS setting without any additional explanation of DNS or Private DNS*

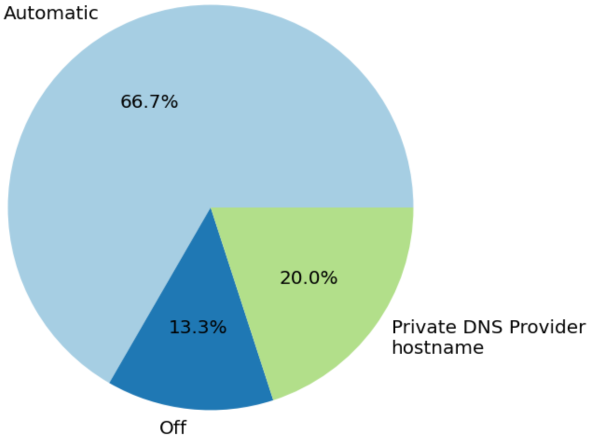


Figure 6: *Users' choice of Private DNS setting after an additional explanation of DNS and Private DNS*

be necessary for their phone to function properly. Unsurprisingly, the reasons people gave for not selecting the "Private DNS provider hostname" option was because they didn't know what to enter as the DNS provider hostname.

When asked what participants would have wanted to know while making a setting choice, many were interested in having more information on what the different options do and the ramifications of selecting each option. One participant was also interested in knowing what the most commonly selected option was.

While some participants were able to describe what DNS does prior to our explanation, far fewer had any concept of what Private DNS would do. Most, participants gave vague guesses about enhancements to security and privacy. However, some had more specific incorrect mental models of what the Private DNS would do, ranging from it speeding up internet access to keeping their phone "encrypted and safe". After having the Private DNS setting explained to them most participants were at least somewhat satisfied with what the setting currently does.

After having DNS and Private DNS explained there were several participants that said they would choose a different Private DNS setting option than they did when they were presented with the same options earlier in the survey. At this second point of choice, the same number of people chose the "Off" option, but fewer people chose "Automatic", instead opting for "Private DNS Provider hostname. " That being said, a couple people that did choose the "Private DNS Provider hostname" option still did not know what they would input as their hostname. A possible way to mitigate this issue would be to adopt a interface more similar to what is offered in Firefox, providing a drop down menu with the option of inputting a host name of their own choice. Figure 6 shows the breakdown of responses. Between the initial choice of Private DNS setting and the choice after participants were given additional information about Private DNS, both participants that had originally chosen "Off" setting switched to "Private DNS Provider hostname. " One person who had originally chosen "Automatic" also switched to "Private DNS Provider hostname," and two switched to "Off. "

The majority of people thought that a Private DNS setting should be on phones so that users could have the opportunity to modify the setting if they wanted to. Most people thought that the default setting should still be "Automatic. " The reasoning for this was that it would provide some benefits to users who might misconfigure the setting on their own. One of the reasons a participant gave for saying that "Off" should be the default was by selecting the "Automatic" setting people would not know where their DNS traffic is being sent.

4.4 Trust in DNS Providers

When asked about various DNS providers, unsurprisingly most participants hadn't heard of many of them with the exception of Google and their ISP. This trend becomes particularly important when you look at how few participants had heard of Cloudflare, where all of their DNS traffic would be

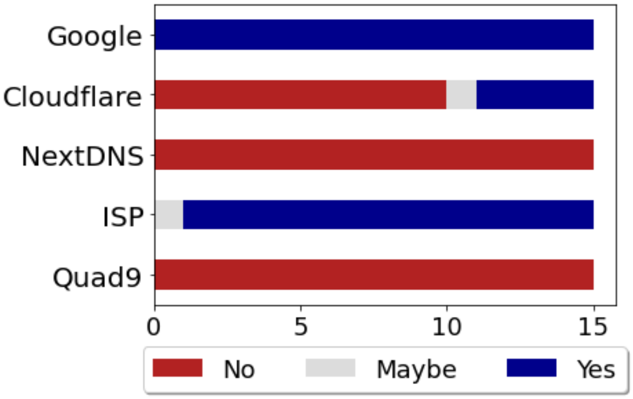


Figure 7: *If participants had heard of different DNS providers*

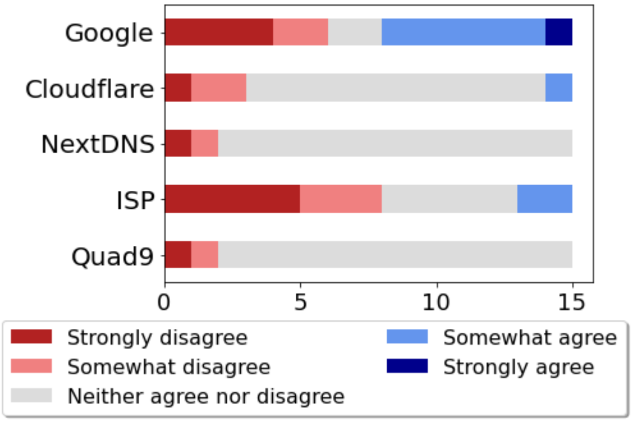


Figure 8: *If participants reported trusting different DNS providers*

directed if they used Firefox with DoH enabled. Based on figures 7 and 8, it appears that there is some connection between knowledge of the DNS provider and their trust in that DNS provider. When users hadn't heard of a DNS provider, they were more likely to have no opinion on or slightly distrust that DNS provider.

4.5 Limitations

The method and population sampled have several limitations. As mentioned earlier, our sample is representative of typical Prolific respondents and is skewed slightly younger, more female, and more educated than the general population of the United States. Since we used a convenience sample from Prolific our results are less generalizable to the general public although we still believe that the study provides useful insights for future research. Further, not all of the users who took part in our study were regular users of Firefox or devices that supported Private DNS. As such, the settings menus were shown to those users in the survey rather than in the context of their actual browser or mobile device. In this study only Private DNS and DoH in Firefox were investigated. Since this survey was distributed, other browsers and operating systems have added support for encrypted DNS protocols, which merits further investigation. As we have such a small sample size, these results should not be thought of as representative of the general public, but as a starting point to encourage future research into the subject.

5 Future Directions

Even with a small sample size, there are some interesting takeaways from our pilot study. What we found suggests a need for further investigation into encrypted DNS settings. Based on the responses that participants gave, it is apparent that users do not understand the implications of the different setting options that are currently provided. While many users remain okay with the default settings even after a thorough explanation of what Private DNS does, there are users who, when given more information, do want to choose a different setting. This suggests that there is a lot of room for improvement in how these settings are presented to users.

Since this pilot study was conducted, additional browsers and operating systems have added support for encrypted DNS. Incorporating these new platforms into the survey would allow for interesting comparisons between users' preferences and perceptions of the implementation choices. This could also allow more participants to interact with their own settings through the course of the survey. This would be particularly helpful as many of our participants did not use Firefox as their primary browsers or Android as their main mobile operating system. Creating anonymized versions of the different interfaces could be interesting since it would allow for a more objective analysis of the settings and interfaces that are separated from participants' opinions on the companies themselves.

Another possible direction for future research could look into specifically how users expect these settings to behave, what protection they expect the settings to offer, and their general satisfaction with the protection that the current implementations provide to them.

Additionally, future research could also focus on how these options could be presented to users in a way that would allow them to make a settings choice that corresponds with their privacy concerns. Using a much larger sample size would allow for more generalizable results and in-depth statistical analysis.

In conclusion, we found that while many people stick with the default encrypted DNS setting options, there are users who modify their choice of DNS setting when given when they have the options explained to them. There are also many misunderstandings and misconceptions regarding the different choices that are provided to users. We believe that this suggests that further research should find ways to empower users to make informed encrypted DNS settings choices.

References

[1] Ammar AlTahhan. "WWDC Notes: Enable encrypted DNS". 2020. URL: https://www.wwdcnotes.com/notes/wwdc20/10047/.

[2] Noah Apthorpe, Dillon Reisman, and Nick Feamster. "A smart home is no castle: Privacy vulnerabilities of encrypted iot traffic". In: *arXiv preprint arXiv:1705.06805* (2017).

[3] Noah Apthorpe, Dillon Reisman, Srikanth Sundaresan, Arvind Narayanan, and Nick Feamster. "Spying on the Smart Home: Privacy Attacks and Defenses on Encrypted IoT Traffic". In: (2017). arXiv: 1708.05044.

[4] Roy Arends, Rob Austein, Matt Larson, Dan Massey, and Scott Rose. *Protocol modifications for the DNS security extensions*. Tech. rep. RFC 4035, March, 2005.

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

[6] Kevin Borgolte, Tithi Chattopadhyay, Nick Feamster, Mihir Kshirsagar, Jordan Holland, Austin Hounsel, and Paul 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. URL: http://dx.doi.org/10.2139/ssrn.3427563.

[7] Stephane Bortzmeyer. "DNS privacy considerations". In: *Work in Progress, draft-ietf-dprive-problem-statement-06* 1 (2015).

[8] Selena Deckelmann. *What's next in making Encrypted DNS-over-HTTPS the Default*. URL: https://blog.mozilla.org/blog/2020/02/25/firefox-continues-push-to-bring-dns-over-https-by-default-for-us-users/.

[9] Sara Dickinson. *DNS Privacy - The Problem*. URL: https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+-+The+Problem.

[10] Cloudflare Docs. *Configure your browser to use DNS over HTTPS*. URL: https://developers.cloudflare.com/1.1.1.1/dns-over-https/web-browser.

[11] Donald Eastlake and C Kaufman. *Domain name system security extensions*. Tech. rep. rfc 2535, March, 1999.

[12] Dominik Herrmann, Christoph Gerber, Christian Banse, and Hannes Federrath. "Analyzing characteristic host access patterns for re-identification of web user sessions". In: *Nordic Conference on Secure IT Systems*. Springer. 2010, p. 136154.

[13] Paul Hoffman and Patrick McManus. "DNS queries over HTTPS (DoH)". In: *Internet Requests for Comments, IETF, RFC* 8484 (2018).

[14] Rebekah Houser, Zhou Li, Chase Cotton, and Haining Wang. "An Investigation on Information Leakage of DNS over TLS". In: CoNEXT '19. Orlando, Florida: Association for Computing Machinery, 2019. ISBN: 9781450369985. DOI: 10.1145/3359989.3365429. URL: https://doi.org/10.1145/3359989.3365429.

[15] Zi Hu, Liang Zhu, John Heidemann, Allison Mankin, Duane Wessels, and Paul Hoffman. "Specification for DNS over transport layer security (TLS)". In: *IETF RFC7858, May* (2016).

[16] Qing Huang, Deliang Chang, and Zhou 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. URL: https://www.usenix.org/conference/foci20/presentation/huang.

[17] K. Hynek and T. Cejka. "Privacy Illusion: Beware of Unpadded DoH". In: *2020 11th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*. 2020, pp. 0621–0628. DOI: 10.1109/IEMCON51383.2020.9284864.

[18] Tommy Jensen. *Windows Insiders can now test DNS over HTTPS*. 2020.

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

[20] Jon Knight. *Here's Why You Should Be Using Private DNS on Your Phone*. URL: https://android.gadgethacks.com/news/heres-why-you-should-be-using-private-dns-your-phone-0231554/.

[21] Katharina Krombholz, Karoline Busse, Katharina Pfeffer, Matthew Smith, and Emanuel von Zezschwitz. ""If HTTPS Were Secure, I Wouldn't Need 2FA"-End User and Administrator Mental Models of HTTPS". In: *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE. 2019, pp. 246–263.

[22] Franck Le, Jorge Ortiz, Dinesh Verma, and Dilip Kandlur. "Policy-Based Identification of IoT Devices' Vendor and Type by DNS Traffic Analysis". In: *Policy-Based Autonomic Data Governance*. Springer, 2019, pp. 180–201.

[23] Scott Lederer, Jason I Hong, Anind K Dey, and James A Landay. "Personal privacy through understanding and action: five pitfalls for designers". In: *Personal and ubiquitous computing* 8.6 (2004), pp. 440–454.

[24] Robert Lemos and Dark Reading. "Got malware? three signs revealed in dns traffic". In: *InformationWeek Dark Reading, May* (2013).

[25] Giovane C. M. Moura, Sebastian Castro, Wes Hardaker, Maarten Wullink, and Cristian Hesselman. "Clouding up the Internet: How Centralized is DNS Traffic Becoming?" In: *Proceedings of the ACM Internet Measurement Conference*. IMC '20. Virtual Event, USA: Association for Computing Machinery, 2020, pp. 42–49. URL: `https://doi.org/10.1145/3419394.3423625`.

[26] Patrick Nohe. *What is the difference between DNS over TLS & DNS over HTTPS?* URL: `https://www.thesslstore.com/blog/dns-over-tls-vs-dns-over-https/`.

[27] Paul Pearce, Ben Jones, Frank Li, Roya Ensafi, Nick Feamster, Nick Weaver, and Vern Paxson. "Global Measurement of DNS Manipulation". In: *26th USENIX Security Symposium (USENIX Security 17)*. 2017, pp. 307–323.

[28] Fahmida Y Rashid. *The Fight Over Encrypted DNS: Explained*. URL: `https://spectrum.ieee.org/tech-talk/telecom/security/the-fight-over-encrypted-dns-boils-over`.

[29] Michele Rodaro, Lamont Gardenhire, and Eve. *DNS-over-HTTPS (DoH) FAQs*. URL: `https://support.mozilla.org/en-US/kb/dns-over-https-doh-faqs`.

[30] Paul Schmitt, Anne Edmundson, Allison Mankin, and Nick Feamster. "Oblivious DNS: Practical Privacy for DNS Queries: Published in PoPETS 2019". In: *Proceedings of the Applied Networking Research Workshop*. ANRW '19. Montreal, Quebec, Canada: Association for Computing Machinery, 2019, pp. 17–19. URL: `https://doi.org/10.1145/3340301.3341128`.

[31] *Security/DNS Over HTTPS*. URL: `https://wiki.mozilla.org/Security/DNS_Over_HTTPS`.

[32] Sandra Siby, Marc Juárez, Claudia Díaz, Narseo Vallina-Rodriguez, and Carmela 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. URL: `https://www.ndss-symposium.org/ndss-paper/encrypted-dns-privacy-a-traffic-analysis-perspective/`.

[33] Dmitrii Vekshin, Karel Hynek, and Tomas Cejka. "DoH Insight: detecting DNS over HTTPS by machine learning". In: *Proceedings of the 15th International Conference on Availability, Reliability and Security*. 2020, pp. 1–8.

[34] Tanya Verma and Sudheesh Singanamalla. *Improving DNS Privacy with Oblivious DoH in 1.1.1.1*. URL: `https://blog.cloudflare.com/oblivious-dns/`.

[35] Alma Whitten and J Doug Tygar. "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0." In: *USENIX Security Symposium*. Vol. 348. 1999, pp. 169–184.

[36] Mozilla Wiki. *Security/DOH-resolver-policy*. URL: `https://wiki.mozilla.org/Security/DOH-resolver-policy#Conforming_Resolvers/`.

[37] Alice Wyman, Michele Rodaro, Wesley Branton, Joni, Lamont Gardenhire, and Angela Lazar. *Firefox DNS-over-HTTPS*. URL: `https://support.mozilla.org/en-US/kb/firefox-dns-over-https`.