Analyzing Real-World DoH and ECH Adoption Using Mozilla Telemetry

Matthias Kirstein, Lion Steger*, Christian Dietze*
*Chair of Network Architectures and Services
School of Computation, Information and Technology, Technical University of Munich, Germany
Email: kirm@net.in.tum.de, stegerl@net.in.tum.de, diec@net.in.tum.de

***Abstract*—DNS over HTTPS (DoH) and Encrypted Client Hello (ECH) are two of the most critical recent developments for closing remaining privacy gaps in Internet protocols. This paper analyzes the adoption of these technologies by leveraging Mozilla Firefox's public telemetry data. We find that global DoH usage has remained nearly constant throughout 2025, at around 13.91 % of handshakes. In regions where the protocol is rolled out, network heuristics leave DoH active for approximately 64 % of clients. A significant portion of the remaining share is attributed to enterprise-controlled browsers. Among users who manually configure their DoH settings, the choice of provider is notably distributed: custom resolvers (37 %) are the most frequent selection, surpassing both Cloudflare (34 %) and NextDNS (29 %). In contrast, ECH adoption remains at a marginal 0.17 % of handshakes. While only 38 % of ECH-enabled handshakes used DoH, this is primarily due to the limited regional rollout of DoH.**

***Index Terms*—DNS, DoH, ECH, measurement, evaluation**

1. Introduction

Modern Internet protocols have largely secured the confidentiality of payload data through encryption mechanisms. However, critical gaps remain regarding the privacy of metadata. Specifically, the domain names a user visits continue to be exposed during traditional cleartext Domain Name System (DNS) resolution and within the unencrypted Server Name Indication (SNI) of the Transport Layer Security (TLS) handshake. The plaintext visibility of these domains enables network observers to reconstruct sensitive user profiles and track activity, even when the application's content itself is encrypted. To address these vulnerabilities, the Internet Engineering Task Force (IETF) has standardized DoH [1] and is currently standardizing the TLS ECH extension [2].

While the theoretical benefits of these protocols are well-established, their real-world impact depends on widespread deployment and correct configuration. Mozilla has been an early adopter of these technologies, enabling DoH by default in specific regions and implementing support for the draft ECH specification in Firefox [3], [4]. However, the extent to which these features are successfully utilized by clients in the wild remains an open question.

In this paper, we analyze the deployment progress of these privacy technologies. By leveraging Mozilla's public telemetry data, we assess the adoption rates of DoH and ECH directly from the client's perspective. This approach allows us to quantify how frequently these protections are actually used in real-world connections.

2. DoH

Conventional DNS resolution was historically designed to prioritize speed, relying primarily on the connectionless User Datagram Protocol (UDP) for transport. While avoiding connection overhead makes this design lightweight and efficient, the reliance on cleartext transmission without cryptographic authentication provides no inherent security. Consequently, DNS traffic is fully visible to on-path observers, and the stateless nature of UDP allows responses to be easily spoofed or modified. This visibility allows a local network or Internet Service Provider (ISP) to track visited domains, while the lack of authentication enables active attacks, such as redirecting users to malicious destinations.

To mitigate these vulnerabilities, DoH, standardized in RFC 8484 [1], encapsulates DNS traffic within HTTPS. By leveraging the underlying TLS [5], [6], this approach replaces unauthenticated, cleartext exchanges with a secure channel that guarantees confidentiality, integrity, and authentication of all DNS queries. In addition to encrypting queries and responses to prevent eavesdropping, server authentication protects against active manipulation by on-path attackers. An additional benefit is traffic obfuscation: by encapsulating DNS queries within HTTPS packets sent on the default HTTPS port (port 443), DoH traffic can be nearly indistinguishable from standard web activity. This complicates traffic analysis and filtering.

Rather than treating HTTP as a mere transport tunnel, DoH can directly benefit from its application-layer features, including authentication mechanisms, compression, and caching. Moreover, by using HTTP as the protocol, DoH enables direct DNS access for web applications, bypassing the operating system's local resolver.

Encapsulating DNS in HTTPS introduces significant overhead compared to UDP, driven largely by TLS handshake delays and HTTP payload requirements. Nevertheless, the overhead introduced by DoH has been shown to have only a marginal impact on actual webpage load times [7]. Modern protocols like HTTP/2 or HTTP/3 offset these costs by reusing connections to amortize handshake delays and using header compression and multiplexing to reduce data footprints and eliminate head-of-line blocking.

While DoH resolvers are typically configured out-of-band using URI templates, RFC 9462 [8] enables the automated discovery of DoH endpoints via Service Binding (SVCB) records. These specialized DNS entries

 doi: 10.2313/NET-2026-05-1_12

supply clients with the necessary connection details, such as supported protocols and URIs. This allows clients to seamlessly and securely upgrade from unencrypted DNS to DoH.

Finally, DoH should not be confused with DNS Security Extensions (DNSSEC). While DoH secures the transport channel between the client and the resolver, DNSSEC provides cryptographic validation of the DNS data itself. These mechanisms address different threat models and are most effective when used together to provide comprehensive security.

3. ECH

Although TLS version 1.3 significantly enhances the protocol's privacy by encrypting the handshake immediately after the initial key parameters are exchanged, the initial `ClientHello` message remains partially visible. Critically, the SNI extension, which identifies the target domain, is transmitted in plaintext within the initial message. This allows on-path attackers to track user activity, even when the subsequent application data is encrypted. To close the remaining privacy gap, the IETF is currently standardizing the ECH extension [2].

ECH secures the TLS handshake by encrypting sensitive parameters, most notably the SNI. The encrypted payload is encapsulated within a standard, unencrypted `ClientHello`. Upon successful decryption, the server proceeds with the connection using the concealed parameters. Otherwise, if decryption fails, often due to stale ECH configurations, the server either safely falls back to the unencrypted message or triggers a connection retry to provide the client with updated cryptographic keys.

By encrypting the SNI, ECH prevents observers from distinguishing which specific site on a shared IP address is being requested. As a result, the architecture offers significant privacy advantages, particularly in environments where multiple sites are hosted behind a common reverse proxy or Content Delivery Network (CDN). To initiate an ECH-enabled connection, the client must first obtain the server's ECH configuration, typically distributed via DNS HTTPS resource records [9], [10]. Crucially, relying on conventional plaintext DNS to fetch these records, or to resolve the domain itself, exposes the target domain name and leaves the ECH configuration vulnerable to spoofing. Consequently, ECH achieves its full privacy potential only when paired with secure DNS transport like DoH, which protects the confidentiality of the domain query and the integrity of the retrieved ECH keys.

To prevent network middleboxes from targeting and filtering ECH traffic, the protocol introduces a GREASE mechanism. Even if the destination server lacks ECH support and no valid configuration is available, clients still include the extension using a randomized, non-functional payload. This ensures all modern TLS handshakes appear uniform, preventing genuine ECH connections from standing out and discouraging networks from selectively blocking privacy-enhancing technologies.

4. Related Work

The real-world impact of DoH and ECH depends on their deployment, which presents different challenges for each protocol. While DoH deployment primarily involves a client-side transition to a compatible resolver, ECH requires individual server operators to actively configure and maintain cryptographic keys. Previous research has primarily measured protocol adoption through active server-side scans and passive network monitoring, which contrasts with our client-centric, telemetry-based analysis.

Zirngibl *et al.* [11] scanned over 400 million domains and found that while 10.5 million had adopted DNS HTTPS records, deployment was almost entirely driven by Cloudflare. Additionally, they found that only a negligible 20 domains possessed active ECH configurations in 2023.

Dong *et al.* [12] conducted a longitudinal study of server-side DNS HTTPS record deployment using the Tranco top 1 million domains. They found that over 27 % of domains published HTTPS records by March 2024, a trend largely driven by Cloudflare's default configurations. However, active ECH adoption dropped to nearly zero in late 2023 after Cloudflare temporarily disabled the feature.

Merlach *et al.* [13] analyzed a month-long campus dataset to evaluate ECH adoption. They found that while 59 % of QUIC flows included an ECH extension, these extensions consisted almost entirely of randomized GREASE values. This discrepancy shows that while modern clients are actively trying to use ECH, server-side adoption has yet to catch up.

García *et al.* [14] conducted Internet-wide scans of the entire IPv4 address space to detect and verify public DoH resolvers. Their analysis revealed a rapid expansion of the ecosystem, reporting that between 2021 and 2022, the number of DoH resolvers increased by 4.8 times and the number of organizations providing DoH doubled.

5. Mozilla's Telemetry

To measure protocol adoption directly from the user's perspective, our analysis leverages public telemetry data from Mozilla Firefox. The browser's telemetry infrastructure collects performance and protocol-related metrics across its desktop and mobile platforms. This system is centered around a publicly documented registry of metrics and events that ensures data consistency between the different platforms [15], [16].

Telemetry data is transmitted in discrete packets called pings [17], which contain a primary payload of counters, histograms, and events, alongside environment metadata. These raw pings are processed and aggregated daily into derived datasets. Mozilla restricts raw telemetry access to protect user privacy, only sharing data after strict aggregation and review [18], [19]. Public access is provided through two primary channels: the Glean Aggregated Metrics (GLAM) dashboard and curated public datasets.

5.1. GLAM

The GLAM dashboard serves as Mozilla's primary high-level public analysis tool [20]. The dashboard visualizes heavily aggregated telemetry data, enabling the tracking of trends for Firefox Desktop and Firefox for Android across releases. However, not all metric types are available in the tool, and the strict aggregation of data into percentiles makes it impossible to perform precise analysis of certain metrics without the raw data.

5.2. Public Datasets

For more granular data than GLAM provides, researchers can request datasets through Mozilla's telemetry data publishing process [18], [19]. To prevent user reidentification, these requests undergo strict privacy and security reviews to enforce aggregation constraints, such as minimum bucket sizes. Approved datasets are published and regularly updated on Mozilla's public data HTTP endpoint [21], [22].

6. Adoption

We analyze the real-world adoption of both DoH and ECH using the Mozilla Firefox telemetry datasets introduced in section 5.2. The public availability of this data provides a practical, client-side perspective on the usage of these privacy-enhancing protocols. However, Firefox accounts for a relatively small share of the global browser market [23], [24], which must be considered when generalizing these metrics to the broader web ecosystem.

6.1. DoH Adoption

To date, Mozilla's default DoH rollout remains limited to the United States, Canada, Russia, and Ukraine [3]. Although Mozilla has expressed intentions to expand to additional regions, no further geographic deployments have occurred since March 2022.

We analyze DoH adoption within these specific regions using the public `doh_adoption_rate v1` dataset [22], [25]. This dataset provides the count of distinct clients reporting a given metric by country code, beginning January 1, 2025. Notably, this dataset is restricted to Firefox Desktop, meaning mobile telemetry falls outside the scope of this analysis.

6.1.1. DoH Heuristics. While DoH significantly improves user privacy, it bypasses local DNS resolvers, potentially disrupting split-horizon DNS and network-level security policies like enterprise filtering or parental controls [3]. Consequently, Firefox performs a series of heuristic checks to validate the network environment before enabling DoH by default [26], [27]. The primary metric for evaluating these checks is `networking.doh_heuristics_result`, which provides insight into both the proportion of clients with DoH enabled and disabled, and the specific reasons for each outcome. Notably, these heuristics are only executed and reported within the rollout regions.

An analysis of the 2025 data reveals that the distribution of heuristic results, as well as the total number of reporting clients, has remained stable throughout the year. This stability is expected, as reporting is limited to the few selected DoH rollout regions and no new geographic deployments occurred in 2025.

Table 1 details the distribution of the individual DoH heuristic results:

- Across the rollout regions, approximately 64 % of clients successfully pass the heuristics check, resulting in DoH being enabled by default.

TABLE 1: Aggregated DoH heuristic results for Firefox Desktop (release channel), January 1, 2025 – November 1, 2025. Based on the sum of daily unique client reports per result value for the `networking.doh_heuristics_result` event.

DoH Heuristic Result	DoH State	Reports (10^6)	Share
`pass`	✓	1363.12	64.08 %
`enterprise-present`	×	390.63	18.36 %
`canary`	×	235.61	11.08 %
`vpn`	×	89.54	4.21 %
`google`	×	20.82	0.98 %
`enterprise-disabled`	×	11.41	0.54 %
`nrpt`	×	5.82	0.27 %
`parental`	×	5.79	0.27 %
`youtube`	×	1.64	0.08 %
`manually-disabled`	×	1.25	0.06 %
`manually-enabled`	✓	0.96	0.05 %
`enterprise-enabled`	✓	0.54	0.03 %
`OTHER`	-	0.05	<0.01 %
Total		2127.18	100.00 %

- If Firefox has enterprise policies set, the decision whether DoH is enabled is determined by the `DNSOverHTTPS` policy rather than the DoH heuristics [26]. Approximately 18 % of heuristic runs detected enterprise policies but lacked an explicit `DNSOverHTTPS` configuration, resulting in DoH being disabled. When configured, results are categorized as `enterprise-enabled` or `enterprise-disabled`.
- Approximately 11 % of clients disable DoH upon resolving the `use-application-dns.net` canary domain. This domain enables network administrators to notify Firefox that the local DNS resolver offers special features, which make the network unsuitable for DoH [28].
- In 4 % of cases, Firefox detects an active VPN on Windows, which prevents the automatic use of DoH [27].
- The remaining results can be attributed to enabled parental controls (`parental`), forced SafeSearch (`google`, `youtube`), the presence of the Name Resolution Policy Table (NRPT) on Windows (`nrpt`), or manual DoH configurations (`manually-enabled`, `manually-disabled`) [27].

In summary, the heuristics successfully validate the network environment for the majority of users, allowing Firefox to enable DoH by default for approximately 64 % of client networks in the rollout regions.

6.1.2. Global DoH Usage. Because the DoH heuristic metric is only reported in the rollout regions, it cannot be used to assess global DoH adoption. However, the `ssl_handshake.privacy` metric provides a broader perspective. This metric tracks the usage of several privacy features for every handshake, including whether TLS 1.3 is negotiated, whether the connection's DNS records were fetched over DoH, and whether the server accepted an offered ECH configuration. As this metric is currently only available within the ECH dataset, detailed further in section 6.2, publicly accessible data is limited to the last six months.

TABLE 2: Aggregated DoH provider choices for Firefox Desktop (release channel), January 1, 2025 – November 1, 2025. Based on the sum of daily unique client reports per choice for the `security.doh.settings.provider_choice_value` event.

DoH Provider Choice	Reports (10^3)	Share
`custom`	274.61	37.12 %
`mozilla.cloudflare-dns.com`	250.64	33.88 %
`firefox.dns.nextdns.io`	211.67	28.61 %
`private.canadianshield.cira.ca`	2.86	0.39 %
`OTHER`	0.02	0.00 %
Total	739.80	100.00 %

The data indicates that the proportional usage of DoH remained stable over this six-month period. Of the 9.54×10^{12} handshakes recorded globally in Firefox Desktop, approximately 13.91 % utilized DoH.

When breaking down this figure on a per-country basis, the disparity between rollout and non-rollout regions becomes clearly evident. Across the four DoH rollout countries, 43.78 % of handshakes utilized DoH, whereas across all other countries, this figure drops to just 0.79 %.

6.1.3. DoH Provider Choice. Mozilla's Trusted Recursive Resolver (TRR) program allows resolver operators to become default or non-default DoH options in Firefox [29]. Participating resolvers must contractually meet strict data privacy, transparency, and operational standards. Mozilla categorizes TRR partners as follows:

- Regional default partners: Cloudflare (US, Russia, Ukraine) and CIRA (Canada).
- Global non-defaults: Cloudflare and NextDNS.
- ISP steering partners: Comcast (US) and Shaw (Canada), which take precedence in their networks unless manually overridden.

When a user modifies their DoH settings in Firefox, the `security.doh.settings.provider_choice_value` event records the DoH resolver selection. This event captures the URL for Mozilla's partner resolvers or reports `custom` for any other user-defined URL. An analysis of the telemetry data shows that the distribution of reported values has remained relatively stable throughout 2025. As shown in table 2, approximately 37.12 % of clients configuring their DoH provider opted for a `custom` resolver, followed by Cloudflare at 33.88 % and NextDNS at 28.61 %.

6.2. ECH Adoption

To analyze the ECH adoption, we use Mozilla's `ech_adoption_rate v1` dataset [22], [30], which at the time of research contained ECH-related telemetry for Firefox Desktop from May 1, 2025, to November 1, 2025.

As previously discussed in section 6.1.2, the `ssl_handshake.privacy` metric records the privacy features used during each handshake, including whether the server accepted an ECH configuration. The telemetry indicates that the percentage of handshakes using ECH is negligible and has not significantly changed over the observed six-month period. As shown in table 3, ECH accounts for only 0.17 % of total handshakes and 0.47 % of handshakes using DoH. This negligible adoption indicates that only a handful of servers currently have ECH configured.

TABLE 3: Aggregated ECH usage in Firefox Desktop (release channel) handshakes, May 1, 2025 – November 1, 2025. Based on the total number of handshakes reported in the `ssl_handshake.privacy` metric. Percentages are calculated relative to the total handshakes within each respective table section. Anomalies omitted.

ECH Usage	Handshakes (10^9)	Share
Without ECH	9519.60	99.83 %
With ECH	16.29	0.17 %
Using DoH, without ECH	1320.51	99.53 %
Using DoH, with ECH	6.19	0.47 %
Using ECH, without DoH	10.10	61.98 %
Using ECH, with DoH	6.19	38.02 %

ECH negotiation in Firefox was initially tied to the internal DoH implementation, as the privacy value of ECH is severely diminished if the browser uses unencrypted DNS to fetch the necessary configurations [31]. Since version 129, however, Firefox allows delegating these lookups to the native operating system DNS resolver to broaden ECH availability when DoH is disabled [4], [31]. This shift is reflected in the telemetry: only 38.02 % of ECH-enabled handshakes used Firefox's DoH, with the majority relying on native DNS infrastructure.

This observation is largely a consequence of Mozilla's geographically limited DoH rollout. A country-level analysis confirms the regional disparity: in all four DoH rollout countries, over 70 % of ECH handshakes used DoH. In contrast, in all other countries, the share remains below 30 %, with the majority falling well under 10 %.

7. Conclusion

While DoH and ECH represent critical advancements in closing the remaining privacy gaps in web communication, our analysis of Mozilla Firefox telemetry indicates that real-world deployment has stagnated. Although DoH is enabled by default in select regions, the rollout has seen no geographic expansion since March 2022, leaving global adoption at approximately 13.91 % of Firefox Desktop handshakes. Our findings show that users who manually configure their DoH provider frequently opt for custom resolvers, representing approximately 37 % of selections. Meanwhile, ECH adoption remains marginal, accounting for only 0.17 % of total handshakes with no significant upward trend observed in 2025.

The effectiveness of these protocols is interdependent, as ECH provides limited privacy if the preceding DNS query is unencrypted. We found that over 60 % of ECH handshakes in Firefox still rely on native DNS, potentially leaking domain names via cleartext queries. Furthermore, preventing domain leaks during the handshake relies on widespread ECH support from CDN and server operators. Therefore, these technologies will only provide robust privacy guarantees when the client-side transition to encrypted DNS is matched by broader ECH adoption across the server landscape.

References

[1] P. E. Hoffman and P. McManus, "DNS Queries over HTTPS (DoH)," RFC 8484, Oct. 2018. [Online]. Available: https://www.rfc-editor.org/info/rfc8484

[2] E. Rescorla, K. Oku, N. Sullivan, and C. A. Wood, "TLS Encrypted Client Hello," Internet Engineering Task Force, Internet-Draft draft-ietf-tls-esni-25, Jun. 2025, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-tls-esni/25/

[3] Mozilla, "DNS over HTTPS (DoH) FAQs," https://support.mozilla.org/en-US/kb/dns-over-https-doh-faqs, Feb. 2024, accessed: 2025-12-02.

[4] ——, "Encrypted Client Hello (ECH) - Frequently asked questions," https://support.mozilla.org/en-US/kb/faq-encrypted-client-hello, Aug. 2024, accessed: 2025-12-02.

[5] E. Rescorla, "HTTP Over TLS," RFC 2818, May 2000. [Online]. Available: https://www.rfc-editor.org/info/rfc2818

[6] ——, "The Transport Layer Security (TLS) Protocol Version 1.3," RFC 8446, Aug. 2018. [Online]. Available: https://www.rfc-editor.org/info/rfc8446

[7] Böttger, Timm and Cuadrado, Felix and Antichi, Gianni and Fernandes, Eder Leão and Tyson, Gareth and Castro, Ignacio and Uhlig, Steve, "An Empirical Study of the Cost of DNS-over-HTTPS," in *Proceedings of the Internet Measurement Conference*, ser. IMC '19. New York, NY, USA: Association for Computing Machinery, 2019, p. 15–21. [Online]. Available: https://doi.org/10.1145/3355369.3355575

[8] T. Pauly, E. Kinnear, C. A. Wood, P. McManus, and T. Jensen, "Discovery of Designated Resolvers," RFC 9462, Nov. 2023. [Online]. Available: https://www.rfc-editor.org/info/rfc9462

[9] B. M. Schwartz, M. Bishop, and E. Nygren, "Bootstrapping TLS Encrypted ClientHello with DNS Service Bindings," Internet Engineering Task Force, Internet-Draft draft-ietf-tls-svcb-ech-08, Jun. 2025, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-tls-svcb-ech/08/

[10] ——, "Service Binding and Parameter Specification via the DNS (SVCB and HTTPS Resource Records)," RFC 9460, Nov. 2023. [Online]. Available: https://www.rfc-editor.org/info/rfc9460

[11] J. Zirngibl, P. Sattler, and G. Carle, "A First Look at SVCB and HTTPS DNS Resource Records in the Wild," in *2023 IEEE European Symposium on Security and Privacy Workshops*, July 2023, pp. 470–474.

[12] H. Dong, Y. Zhang, H. Lee, S. Huque, and Y. Sun, "Exploring the Ecosystem of DNS HTTPS Resource Records: An End-to-End Perspective," in *Proceedings of the 2024 ACM on Internet Measurement Conference*, ser. IMC '24. New York, NY, USA: Association for Computing Machinery, 2024, p. 423–440. [Online]. Available: https://doi.org/10.1145/3646547.3688410

[13] G. Merlach, M. Trevisan, and D. Giordano, "Encrypted Client Hello Is Coming: A View from Passive Measurements," *Network*, vol. 5, no. 3, 2025. [Online]. Available: https://www.mdpi.com/2673-8732/5/3/29

[14] García, Sebastián and Bogado, Joaquín and Hynek, Karel and Vekshin, Dmitrii and Čejka, Tomáš and Wasicek, Armin, "Large Scale Analysis of DoH Deployment on the Internet," in *Computer Security – ESORICS 2022*, Atluri, Vijayalakshmi and Di Pietro, Roberto and Jensen, Christian D. and Meng, Weizhi, Ed. Cham: Springer Nature Switzerland, 2022, pp. 145–165.

[15] Mozilla, "Glean," https://docs.telemetry.mozilla.org/concepts/glean/glean, Oct. 2025, accessed: 2025-12-02.

[16] ——, "Glean Dictionary," https://dictionary.telemetry.mozilla.org/, accessed: 2025-12-02.

[17] ——, "What Data does Mozilla Collect?" https://docs.telemetry.mozilla.org/introduction/what_data, Aug. 2021, accessed: 2025-12-02.

[18] ——, "Data Publishing @ Mozilla," https://blog.mozilla.org/data/2020/09/25/data-publishing-mozilla/, Sep. 2020, accessed: 2025-12-02.

[19] ——, "Data Publishing - MozillaWiki," https://wiki.mozilla.org/Data_Publishing, Feb. 2021, accessed: 2025-12-02.

[20] ——, "GLAM: Glean Aggregated Metrics Explorer," https://glam.telemetry.mozilla.org/, accessed: 2025-12-02.

[21] ——, "Accessing Public Data," https://docs.telemetry.mozilla.org/cookbooks/public_data, Feb. 2021, accessed: 2025-12-02.

[22] ——, "Mozilla Public Datasets," https://public-data.telemetry.mozilla.org/all-datasets.json, accessed: 2025-12-02.

[23] StatCounter, "Browser Market Share Worldwide | Statcounter Global Stats," https://gs.statcounter.com/browser-market-share, accessed: 2025-12-20.

[24] Cloudflare, "Adoption and Usage Worldwide | Cloudflare Radar," https://radar.cloudflare.com/adoption-and-usage, accessed: 2025-12-20.

[25] Mozilla, "Bug 1982897 - Data Publishing Request," https://bugzilla.mozilla.org/show_bug.cgi?id=1982897, accessed: 2025-12-02.

[26] ——, "Security/DNS Over HTTPS - MozillaWiki," https://wiki.mozilla.org/Security/DNS_Over_HTTPS, accessed: 2025-12-02.

[27] ——, "Security/DNS Over HTTPS/Heuristics - MozillaWiki," https://wiki.mozilla.org/Security/DNS_Over_HTTPS/Heuristics, accessed: 2025-12-18.

[28] ——, "Canary domain - use-application-dns.net," https://support.mozilla.org/en-US/kb/canary-domain-use-application-dnsnet, accessed: 2025-12-02.

[29] ——, "Security/DOH-resolver-policy - MozillaWiki," https://wiki.mozilla.org/Security/DOH-resolver-policy, accessed: 2025-12-14.

[30] ——, "Bug 1957082 - Data Publishing Request," https://bugzilla.mozilla.org/show_bug.cgi?id=1957082, accessed: 2025-12-02.

[31] ——, "Security/Encrypted Client Hello - MozillaWiki," https://wiki.mozilla.org/Security/Encrypted_Client_Hello, accessed: 2025-12-20.