User Perceptions of the Privacy and Usability of Smart DNS

Rahel A. Fainchtein
Georgetown University

Adam J. Aviv
The George Washington University

Micah Sherr
Georgetown University

Abstract

Smart DNS (SDNS) services enable their users to avoid geographic restrictions to content (i.e., *geoblocking*) with minimal internet quality of service overhead. While previous research has shown that usage of SDNS has numerous associated privacy risks, the security and privacy perceptions of users of SDNS are unexplored. In this paper, we perform a survey of $n = 63$ SDNS users, finding that many have limited understandings both of how these systems work and their overall security/privacy properties. As a result, many users put undue trust in purveyors of SDNS services and in the security they provide.

CCS Concepts

• **Security and privacy → Usability in security and privacy**; *Web protocol security*.

ACM Reference Format:
Rahel A. Fainchtein, Adam J. Aviv, and Micah Sherr. 2022. User Perceptions of the Privacy and Usability of Smart DNS. In *Annual Computer Security Applications Conference (ACSAC '22), December 5–9, 2022, Austin, TX, USA.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3564625.3567978

1 Introduction

The Internet does not have a uniform vantage point. Instead, the information and content users can access often depends on their geographic locations, as estimated by the web servers they contact. In particular, many streaming media services (e.g., Netflix, Hulu, Disney+, YouTube, etc.) apply *geoblocking* (sometimes called geofiltering) to impose geographically-based access controls over their content. When implemented by media companies, geoblocking is frequently used to enforce geographically limited licensing agreements. In these agreements, the licenses granted only allow their licensees to distribute the copyrighted material (e.g., movies) within predetermined geographic regions. To comply with these restrictions, streaming services use IP-geolocation mapping services to ascertain requestors' physical locations based on their (respective) network addresses. If they are determined to be outside the region stipulated in the provider's content license, their requests are (geo)blocked by the provider [3].

Such geoblocking can frustrate both users who wish to access the content but either fall outside of the geofence—the geographic area in which users are permitted to access the content—or through faults in the geolocation service, are incorrectly perceived as being outside of it.

The desire to access otherwise unavailable geoblocked content has led to a growing market of online services geared towards bypassing these geography-based access controls. Perhaps most widely used and advertised are VPNs (virtual private networks), which market themselves not just as a security tool but also as mechanisms for disguising users' locations to bypass geoblocking [6, 25, 30]. However, using VPNs to avoid geoblocking has a number of limitations, including: (1) it requires a moderate amount of technical sophistication to configure [24]; (2) it incurs significant communication overhead, which often leads to poor streaming experience; and (3) it requires re-configuration whenever a new streaming service is used, since the VPN exit point must be located in an allowable geographic region as determined by the streaming service.

Frequently sold together with VPN products, *Smart DNS* (SDNS) services offer an alternative method for bypassing geoblocks. Unlike VPNs, SDNS services are exclusively marketed for their ability to "unblock" or enable user access to otherwise geo-restricted content or websites. To use SDNS, a customer configures their computer to use the SDNS resolver (i.e., a DNS resolver operated by the SDNS service). The SDNS resolver resolves hostname requests as expected for non-geoblocked domains. However, when requested to resolve hostnames corresponding to web services or content providers that geoblock, the SDNS resolver returns IP addresses of proxy servers located within their (respective) geofences. For example, when a user located outside the U.S. requests `US-content.netflix.com` when using SDNS, instead of resolving to an IP address managed by Netflix, the SDNS resolver may return an IP for a proxy server that is located in the U.S.; that proxy then relays the customer's traffic to (and from) Netflix, giving Netflix the impression that the request originated from within the U.S.

SDNS addresses many of the shortcomings of using VPNs to avoid geoblocking: it does not require the installation of specialized software, it incurs low communication overhead, and it eliminates the need for tunnel reconfiguration for each content service. However, prior work by Fainchtein et al. demonstrated a number of serious security and privacy shortcomings of SDNS such as a lack of encryption, susceptibility to client-enumeration attacks, and SDNS user identification [8].

Despite these flaws, SDNS has a significant and growing user base. Fainchtein et al. perform empirical measurements of SDNS providers' DNS resolvers, and using statistical tests, estimate that some SDNS resolvers handle hundreds of thousands of requests for a *single geoblocked domain*, per hour [8]. Since SDNS services employ dozens or more SDNS resolvers, this suggests that SDNS is an enormously popular service. At least one SDNS-affiliated site estimates that SDNS is used by "…millions of people …" [16].

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

ACSAC '22, December 5–9, 2022, Austin, TX, USA

© 2022 Copyright held by the owner/author(s). Publication rights licensed to ACM.

ACM ISBN 978-1-4503-9759-9/22/12…$15.00
https://doi.org/10.1145/3564625.3567978

Although SDNS usage appears to be widespread, the motivations and perceptions of SDNS by its users have not been studied. This paper examines how users perceive SDNS services by exploring four main research questions: (1) what motivates users to use SDNS?; (2) how do users select which SDNS provider to use?; (3) to what degree do SDNS users trust these services; and (4) how well do SDNS users actually understand SDNS functionality?

To answer these questions, we conducted an online survey of 63 SDNS users, recruiting participants from topical subreddits (Reddit discussion boards) and Prolific. Participants were asked about their histories and experiences with SDNS services, their understanding as to how these systems operated, and their perceptions of SDNS' trustworthiness and ethics.

We find that most of our study participants had misconceptions about how SDNS services function. Alarmingly, many conflated SDNS with VPNs, and considered the former to be a privacy-enhancing technology that provided additional layers of encryption and/or sender anonymity—in actuality, SDNS services do neither. Many were prone to put undue trust in the protections that SDNS services purport to offer.

Moreover, very few of the SDNS users who took our study considered the privacy and security risks of using SDNS. While many participants (incorrectly) understood that SDNS services would bolster their privacy, very few considered that using SDNS could diminish their security and privacy.

Interestingly, most participants viewed their use of SDNS services to bypass geofiltering as ethical. Several participants justified their use of SDNS by noting that the Internet should be open and free from geography-based discrimination, and SDNS was a technology that helped achieve this ideal. Most participants similarly believed that using SDNS was legal, although a large portion of participants were uncertain of its legality.

The main findings of our study—that participants often did not understand how SDNS services functioned, and that they overestimated its privacy protections while underestimating the risk that using these services posed—should be construed as a strong signal that these services deserve more study. Our survey suggests that SDNS users may be unknowingly risking their security and privacy, and that much more user education is needed.

2 Background on SDNS

Smart DNS services offer their customers the ability to bypass geoblocking by selectively proxying requests for geoblocked domains. However, unlike VPNs, SDNS neither requires the installation of special software nor incurs the same delay overheads. Instead, SDNS requires that customers (1) register their IP addresses on their SDNS provider's allow-list (and pay for the service) and (2) update their computers' DNS settings to route all DNS resolution requests to a DNS resolver controlled by the SDNS provider.

SDNS Workflow. Figure 1 reviews the workflow of SDNS. The SDNS resolver returns the correct DNS resolution for requested domains that either do not geoblock, or for which the requester's geographic location, as determined by IP-geolocation, is within the requested domain's *geofence*, or set of geographic regions from which the (geoblocking) domain's servers will accept incoming connections. However, if a customer requests a DNS resolution for a geoblocked domain they normally would be unable to access, the SDNS resolver "smartly" recognizes it and, in lieu of the correct DNS resolution, returns the IP address of an *proxy* located within the domain's geofence that is under the SDNS provider's control (hereinafter *SDNS proxy*). The proxy relays traffic between the customer and the destination, serving as a TCP endpoint for both. Because the proxy simply forwards TCP payloads and does not rewrite traffic, it does not break end-to-end guarantees and is compatible with TLS/HTTPS.

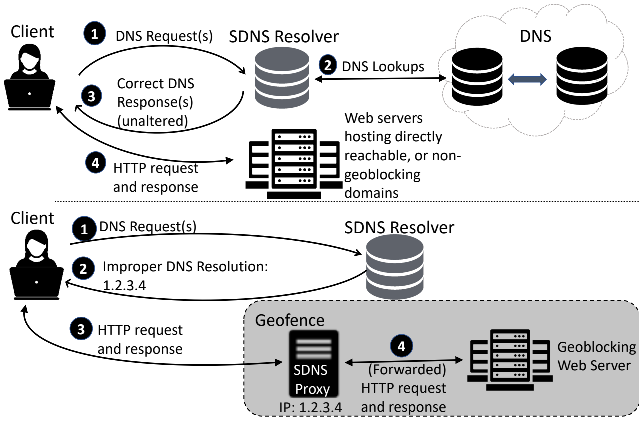
Client
1 DNS Request(s)
SDNS Resolver
2 DNS Lookups
DNS
3 Correct DNS Response(s) (unaltered)
4 HTTP request and response
Web servers hosting directly reachable, or non-geoblocking domains
Client
1 DNS Request(s)
SDNS Resolver
2 Improper DNS Resolution: 1.2.3.4
3 HTTP request and response
Geofence
SDNS Proxy
IP: 1.2.3.4
4 (Forwarded) HTTP request and response
Geoblocking Web Server

Figure 1: An overview of SDNS systems' workflow; When a client requests a domain whose web server either does not geoblock or allows direct incoming connections from the client's IP *(top)*, and when the client requests a *supported channel* or a domain that would otherwise reject connections originating from the client's IP *(bottom)*. As shown in steps (3) and (4) of the bottom diagram, when the client requests a geoblocking domain, the SDNS resolver returns the IP address of an SDNS proxy situated inside that domain's *geofence*. The SDNS proxy then transparently forwards traffic between the client and the geoblocking domain's web server.

SDNS Vulnerabilities. Fainchtein et al. describe several privacy and security vulnerabilities in both SDNS providers' architectures and implementations [8]. Among the identified vulnerabilities inherent to SDNS systems' construction, most stem from customers' exclusive use of SDNS resolvers for all of their DNS resolution requests. Fundamentally, by handling all DNS requests, SDNS providers maintain ultimate control over where their customers send their Internet traffic. Fainchtein et al. disclose instances in which SDNS providers return proxy IP addresses for domains for which they do not advertise support, indicating a potential mismatch between how users might expect their traffic to be handled and the realities of how their traffic transits the Internet. More generally, SDNS providers have the ability to observe *every* domain that their customers request (regardless of whether the domain is for a supported streaming service), and have the ability to decide at any time and without notice whether or not a given domain will be proxied. This is particularly problematic given that SDNS services operate within a "set-and-forget" framework; unlike with VPNs, once a user re-configures their computer to use an SDNS resolver, there are no overt signs that all DNS resolution requests are routed through SDNS resolvers and that some portion of non-DNS traffic is relayed through SDNS proxies. Fainchtein et al. posit that the complete lack of user interface means that users may be more likely to forget that SDNS is configured and may continuously and without realization transmit an enormous amount of privacy-sensitive information via SDNS providers.

Fainchtein et al. additionally argue that SDNS may increase exposure to third-party eavesdropping, since DNS resolution requests likely travel beyond customers' local ISPs.[1] That is, due to the increased length of their DNS traffic's Internet traversal path, a larger set of passive, on-path eavesdroppers can learn which domains they visit, and in so doing, track their online behavior. Similarly, traffic that is proxied via SDNS proxy servers also likely traverses a longer path than would occur via direct (non-proxied) connections. Unlike VPNs, SDNS does not add a layer of encryption and thus eavesdroppers who can intercept traffic can potentially learn a lot about customers' Internet browsing habits (for example, by inspecting unencrypted Source Name Indication headers [4]).[2]

Finally, Fainchtein et al. demonstrate that some SDNS customers face additional threats to their privacy due to their providers' improper system configurations. Among the most egregious of these vulnerabilities is the susceptibility to a client enumeration attack in which a third-party attacker can identify all of a vulnerable provider's customers by IP address. The attack requires only that the adversary register a domain name and operate its own authoritative name server [8].

SDNS Marketing and Packaging with VPNs. Despite having a distinct architecture and workflow from VPNs, SDNS services are frequently offered by VPN providers and sold together with their VPN services. For some VPN providers, it is difficult (if not impossible) to solely purchase SDNS; SDNS is sometimes only available as an add-on or as part of a VPN service subscription. This is true of many of the SDNS services that appear to be the most popular, and we note that this bundling has the potential to bring about or exacerbate user confusion about the distinctions between these two services. That is, a user who chooses to use SDNS for geoblock evasion may be at a notable risk of confusing it with a VPN service, especially when purchasing the VPN service (regardless of whether the actual VPN functionality is ever used) is required to gain access to SDNS functionality. We explore users' confusion between VPN and SDNS services in §5.4.

3 Related Work

IP-geolocation, which serves as the primary means of geoblocking, has been widely studied. Numerous methods of performing IP-geolocation have been identified and include both active [11, 21, 35] and passive [23] mechanisms for estimating a computer's geographic location given its IP address. Poese et al. note that the most widely used form of IP-geolocation relies on databases that map IP address blocks to geographic locations [26]. As a primary example of this, they point to commercial IP-geolocation services, while also showing that these services have high rates of inaccuracy.

Despite the large body of work on IP-geolocation, research on geoblocking has been more limited. While there has been significant study of server-side denial of connections in the context of anonymity networks (e.g., Tor [5]), existing approaches for blocking [19, 29] and blocking-circumvention [36, 37] are specific to anonymity networks and differ from those used for geoblocking.

Much of the existing work on geoblock evasion has focused on VPNs. Weinberg et al., who empirically measure the locations of VPN proxies, find that many proxies' advertised locations are inaccurate [34]. Khan et al., who independently study the VPN ecosystem, also find widespread misrepresentation of proxies' geographic locations [18]. However, both works find that, despite the inaccuracy of their claimed geographic locations, they are still successful at geoblock evasion as long as websites performing the associated IP-geolocation checks also misattribute their (respective) proxies' locations to places within the geofence [18, 34].

Namara et al. [24] examine the factors that contribute to users' adoption and abandonment of VPNs. They conduct an online survey of Reddit users and university students to determine how and why users decide to use (or not use) VPNs. A significant finding of their work is that users who are motivated by emotional factors (e.g., the need to protect their privacy) are less likely to abandon the use of VPNs as compared to users who use it for more practical purposes (e.g., to gain access to an otherwise inaccessible resource) [24]. Like Namara et al., we also investigate users' perceptions of a technology (in our case, SDNS service) and their reasons for choosing to use it. However, while Namara et al.'s focus is to determine what makes users continue to use or abandon VPNs, our goal is to better understand users' perceptions of the functionalities, trustworthiness, and security and privacy properties of these newer SDNS services.

In the context of geoblocking, Afroz et al. [1], who perform a large scale measurement of the practice, find that it appears to be ubiquitous. In particular, they note widespread blocking of IP addresses associated with developing countries by websites hosted in industrially advanced ones, such as the United States and other European nations [1]. McDonald et al. track CDN-based geoblocking by sending requests to different CDN-supported websites from hundreds of vantage points around the world [3]. They find that geoblocking occurs across a wide range of countries and websites, and is implemented for a wide range of reasons. These include (but are not limited to) compliance with legal or diplomatic restrictions such as economic sanctions, export control legislation, and copyright usage restrictions [3].

Though likely due to their also offering VPNs, we observe that many SDNS providers' websites appear to advertise more security than these services actually offer. This partially inspired our work, which seeks to increase our understanding of SDNS users' perceptions of their providers' trustworthiness and the extent to which they believe using SDNS offers them additional security or privacy. There is a substantial body of research on how Internet users ascertain an online source's authenticity, technical soundness, trustworthiness and overall security. Other papers have assessed users' mental models of online security and privacy, as well as their impact on users' security decisions [9, 15, 17, 27, 28].

In general, these papers' find that users do not assess the risks posed by system usage completely logically, and that their decisions to share or withhold sensitive information tend to be contextually

[1] The same is true for public resolvers (e.g., Google's 8.8.8.8). Although SDNS is not incompatible with encrypted DNS protocols such as DoT [14] and DoH [13] that could mitigate the increased risk of eavesdropping, we have not encountered an SDNS provider that supports the encryption of DNS requests and responses.

[2] In the case of connections over TLS, the SNI would allow the eavesdropper to learn the domain names of the websites visited rather than their full URL.

based. Acquisti and Grossklags, who study users' attitudes and decision making processes concerning their privacy, explain that users' notions of privacy are complex and multifaceted, and that Internet users face major limitations on their ability to logically assess the implications of their decisions to share or withhold sensitive information [2]. These include users' lack of access to contextual information about the full scope of their decisions' impacts, as well as their bounded rationality, or their limited ability to synthesize, recall and logically apply all of the available information when making a decision. To cope with these shortcomings, Acquisti and Grossklags note, users rely on a set of mental shortcuts or cognitive heuristics to try and qualitatively approximate the missing information and logic steps, and arrive at a decision more quickly. In addition, users' decisions are also influenced by their biases and other "psychological deviations from rationality" [2].

Gambino et al. [10] identify several cognitive heuristics that users often resort to when determining whether (or not) they are willing to share private information with a given website. Specifically, they note several positive heuristics that make users feel more at ease sharing more sensitive information, as well as negative heuristics that make users more wary of sharing this information [10]. Shyam notes that users tend to assess a site's trustworthiness based more on its appearance and visual presentation than on its content [31].

4 Methodology

To ascertain users' understandings and perceptions of SDNS services, we conducted an online study. In this section, we describe the study's recruitment and screening procedures, as well as its amended eligibility criteria, our ethical considerations when conducting this study, and the study's limitations. For completeness, all components of the survey are included in Appendix A.

4.1 Study Procedure

The main components of our study included a pre-screening phase, and a main survey:

Pre-screening Participants. To ensure familiarity with SDNS, we asked participants a series of screening questions. Respondents whose answers indicated they were not familiar with SDNS were not allowed to complete the main survey.

We initially required respondents to either have experience using SDNS, as a current or previous SDNS user, or to be seriously considering using the service within one month of completing the survey[3]. As described in more detail in §4.2, participants were recruited across two separate platforms (Reddit and Prolific), which necessitated two distinct presentations of screening questions (**S1** through **S7**)[4]. Despite this, both groups of participants were ultimately asked the same questions and were required to meet the same requirements to be eligible to complete the main survey.

Main Survey. The main survey consisted of questions covering the following topics:

(1) *SDNS impact on online security and privacy:* To ascertain how participants believed that SDNS services affected their security and privacy, we began by asking participants whether they thought the service made their Internet browsing more or less secure, and whether it provided additional protections or posed a risk to their online security and/or privacy (questions **M1**-**M4**).
(2) *SDNS functionality:* Participants were then asked a set of more specific questions about how SDNS systems operate. These questions were aimed at getting more detailed insights into participants' understandings and misconceptions. Participants were presented with two sets of Likert scale questions that asked whether they agreed or disagreed with statements describing SDNS's proxying behavior (**M5**) and ability to conceal customers' IP addresses from websites (**M6**).
(3) *Choice to use SDNS:* To gain context about participants' SDNS usage, we then inquired about their goals in using SDNS. We surveyed participants about their motivations to specifically use this service, and whether they thought it was worth the effort required to set it up (**M7**-**M11**).
(4) *Participant setup and usage of SDNS:* Next, respondents were asked about their setup and usage of SDNS services. These questions covered (1) whether their SDNS providers offered services in addition to SDNS (e.g., VPNs) and the extent to which participants used them (**M12**-**M15**); and (2) the types of devices on which participants set up SDNS and the extent to which they had SDNS enabled when browsing the web (**M16**-**M18**).
(5) *Trustworthiness of SDNS providers:* Participants were asked whether they thought their chosen SDNS provider was trustworthy in general, and the steps they trusted their SDNS provider to take to ensure that (1) the service functioned as advertised and (2) that users' security and privacy were safeguarded (**M19**-**M21**).
(6) *Success evading detection:* Given the ongoing cat-and-mouse dynamic between content providers and SDNS services, participants were then asked about their experience accessing geoblocked content using these services. These questions focused on whether participants had been blocked by a content provider due to their use of SDNS, how often they were caught, and how easy they thought it was for a content provider to detect that they were using SDNS (**M22**-**M26**).
(7) *Ethics and legality of using SDNS:* Finally, participants were asked whether they thought using SDNS to access geoblocked content was ethical and/or legal, and to explain their opinions (**M27**-**M28**).
(8) *Demographics (Reddit participants only)*: Participants who were recruited through Reddit were then asked demographic questions (**D1**-**D6**).[5]

Analysis of Responses. As we explain in more detail in §4.2 and §4.4, five participants' responses had to be removed from quantitative analysis, and one response had to be removed from qualitative analysis despite our initial screening for participant eligibility. Given our small sample size (n = 63 for qualitative analysis, n = 58

[3] Responses from participants who did not have experience using SDNS were later excluded from analysis. We explain our reasoning for this decision in §4.2

[4] Survey questions are referenced in bold typeface and can be found in Appendix A.

[5] Prolific participants were asked demographic questions (**D1**-**D6**) in the pre-screening. We describe this in more detail in §4.2.

participants in both qualitative and quantitative analysis), we perform a qualitative analysis of survey responses. Qualitative, or free-text responses were open-coded by a primary coder and were then evaluated by a secondary coder (Cohen’s $\kappa \geq 0.76$). Our code book is included in the paper’s artifact repository [7].

4.2 Recruitment and Eligibility Criteria

As noted in §4.1, participants were recruited across two groups: One group was recruited on Reddit through posts that advertised our study on r/samplesize, r/SurveyExchange, and r/TakeMySurvey between February 1, 2021 and March 25, 2021. Upon completion of the survey, participants were given the opportunity to enter a raffle to win a $50 USD Amazon gift card with minimum odds of winning of 1:20.

To determine eligibility, Reddit participants were screened using conditional navigation. That is, they were presented with a single survey that began with screening questions **S1** through **S7**. Before completing the survey, Reddit respondents were warned that the survey included screening questions and attention checks, and, if determined ineligible, they would be screened out of the survey and ineligible for remuneration. As such, Reddit respondents whose answers to screening question indicated that they neither had used SDNS as a current or previous user (**S2**), nor that they were not seriously considering using it within the next month (**S3**), were screened out mid-survey. Additionally, responses from Reddit participants that indicated familiarity with SDNS, but failed to identify the service’s main use—i.e., bypassing access restrictions to domains that performed geoblocking—were manually removed from consideration. As outlined in their informed consent, Reddit respondents who were screened out or submitted these removed entries were ineligible for remuneration.

The second group of participants was recruited using Prolific. Since Prolific does not allow participants to be screened out mid-survey, these respondents were given a screening survey in which they were asked these same screening questions, as well as demographic questions **D1** through **D6**. Although included in the Prolific group’s screening survey, we note that respondent answers to the demographic questions were not considered when determining their eligibility to participate in this study. Those who were qualified, as we determined from their answers to the screening questions, were able to return and take the main survey, which we described in more detail in §4.1 and whose complete contents can be found in Appendix A. Prolific participants were compensated $0.75 USD for completing the prescreen questionnaire and earned an additional $4.25 USD for completing the main survey. On average, Prolific participants took about 5 minutes to complete the prescreen, and 10 to 15 minutes to complete the main survey. Similarly, Reddit participants completed the combined survey in roughly 15 to 20 minutes.

Amended Eligibility Requirements. Using the initial eligibility criteria described above, we surveyed 72 respondents across both groups (Reddit: $n = 18$; Prolific: $n = 54$). However, upon further scrutiny of responses, we found that responses from participants who did not currently or previously use SDNS were often of lower quality. As such, once all participants had been compensated, these responses were excluded from analysis. Additionally, we found six responses that could not be included in our quantitative analysis; these consisted of four participants who indicated having used a service provider that provided VPN services but we discovered did not actually offer SDNS, and one participant whose answers reflected VPN usage but not that of SDNS. As we explain in more detail in §5 and §6, participant confusion over whether they had in fact used SDNS and not solely used a VPN was likely due to their general confusion about the differences between the two services. Since it is not uncommon for SDNS providers to also offer VPN services, and for VPNs to also be used to bypass geoblocks, we only removed these responses from quantitative analysis.

Metric	Reddit sample	Prolific sample
Total Participants	10	48
Gender: Male	7 (70%)	33 (69%)
Gender: Female	3 (30%)	14 (29%)
Gender: Prefer not to disclose	0	1 (2%)
Age: 18-24	3 (30%)	30 (63%)
Age: 25-44	6 (60%)	16 (33%)
Age: 45-74	1 (10%)	2 (4%)
Less than high school degree	0	2 (4%)
High school graduate, diploma, or equivalent	1 (10%)	15 (31%)
Trade/technical/vocational training/Associates’ Degree	1 (10%)	4 (8%)
Some college credit, no degree	2 (20%)	10 (21%)
Bachelor’s degree	3 (30%)	12 (25%)
Master’s, Professional (e.g J.D., M.D.), or Doctoral Degree	3 (30%)	6 (13%)
Annual income: Less than $10,000	2 (20%)	21 (44%)
Annual income: $10,000 - $49,999	2 (20%)	21 (44%)
Annual income: $50,000 - $79,999	2 (20%)	1 (2%)
Annual income: $80,000 - More than $150,000	2 (20%)	2 (4%)
Annual income: Prefer not to disclose:	1 (10%)	3 (6%)

Table 1: Demographics for Reddit and Prolific participants included in the quantitative and qualitative analyses. Prolific demographics exclude tallies from respondents who only completed the pre-survey.

In total, 63 responses (Reddit: $n = 11$; Prolific: $n = 52$) were included in qualitative analysis, and, of those 58 responses (Reddit: $n = 10$; Prolific: $n = 48$) were also included in quantitative analysis. The final groups of participants had the demographic makeup described in Table 1; the SDNS services they used is listed in Table 2 in Appendix B.

4.3 Ethical Considerations

This study protocol was approved by our Institutional Review Boards (IRBs). All data collected was deidentified such that all participants’ personally identifiable information (PII) was removed, and responses were associated with random identifiers.

Since we ask participants whether they believe using SDNS to bypass geoblocking is ethical and/or legal, we also consider whether their responses to these two questions could constitute a confession of wrongdoing. This is not straightforward since determining the legality of using SDNS to bypass geoblocking appears to be quite complicated [32, 33].[6] To this end we acknowledge that we would be required to comply if served with a court-ordered subpoena. While we believe the this would be unlikely to occur, we nonetheless provided the following warning to all participants in the study’s informed consent:

[6] Based solely on participant responses, we observe a general lack of clarity on the legality of using SDNS to bypass geoblocking, and that its legal status appears to vary across different regions’ regulations. However, we reiterate the caveat that we are neither lawyers, nor legal experts on this matter.

"If you are concerned with potentially revealing that you have used, currently use, or intend to use SmartDNS services, you should not participate in this study."

While we are neither lawyers nor legal experts, we believe that by deidentifying participant responses before analysis and not maintaining a link to persistent identifiers, we provide reasonable risk mitigation for participants.

4.4 Study Limitations

SDNS is a relatively new offering, and although there appear to be a large number of SDNS users [8, 16], there are fewer discussion forums devoted to SDNS than there are VPNs, making it challenging to identify populations of SDNS users to recruit as participants. It is also possible that our recruitment efforts are affected by users' wariness of sharing that they have used SDNS.

Due to the number of participants we were able to recruit, we cannot guarantee our participants make up a fully representative sample of SDNS users. As such, we can neither assess the prevalence of the themes identified across all SDNS users, nor perform more in-depth quantitative analysis (e.g., correlation or regression studies).

Additionally, as we describe in more detail in §5, participants often struggled to distinguish between SDNS and VPN. This in turn made it harder to determine which of them had actually used SDNS. As we note in §4.2, some (n = 6) participants claimed to have used SDNS, but upon further inspection were found not to have. Specifically, one participant failed attention checks, four participants listed providers that neither currently nor previously offered SDNS, and one respondent had free text responses indicating their exclusive use of their provider's VPN offerings. However, free text responses from participants in this subgroup who passed all attention checks were still included in qualitative analysis, since their responses still indicated participants' underlying confusion (see §5.4).

Despite these shortcomings, this study highlights many important themes amongst SDNS users' perceptions, many of which, we believe, add valuable insight to the broader study of geoblock evasion, and how usage of evasion tools impacts the online security and privacy of their users.

5 Results

In this section, we describe the results of our study. We denote participants whose responses were only included in qualitative analysis with the letter Q. Participants whose responses were included in both quantitative and qualitative analysis are identified with the letter P.

5.1 Motivation to Use SDNS

The vast majority (n = 52) of participants noted they mainly used SDNS to access websites or other content to which their access would otherwise be restricted (**M8**). For most of these respondents (n = 38), this meant bypassing server-side geoblocking, often (n = 18) to use a performance-sensitive service such as video streaming that required low latency and high bandwidth.

Interestingly, several (n = 12) participants sought to use SDNS for protection it did not offer. These participants used SDNS for Internet privacy (n = 7), online anonymity (n = 2) and online security (n = 3). Amongst those seeking online privacy, two participants specifically mentioned limiting online tracking by corporations and government agencies. For example, P18 notes they specifically felt SDNS would help "...to minimise the collection of my data by companies who like spamming individuals with personalised ads." In contrast, Q5, who sought to avoid government tracking, chose to use SDNS "...[to avoid] be[ing] tracked by the FBI," implying potentially more serious consequences in the event that SDNS failed to sufficiently protect their online privacy.

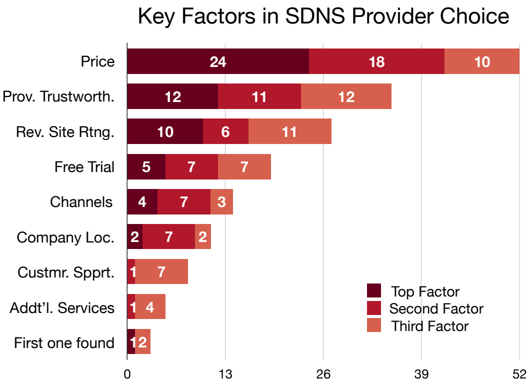

Figure 2: Top factors in choosing an SDNS provider (M11).

Given the frequency with which SDNS is offered alongside VPN services, we asked participants why they specifically decided to use SDNS (**M10**). For many (n = 21) participants, the answer lay in SDNS' lower latency overhead, and its improved Internet quality of service (QoS). Specifically, 18 participants noted experiencing lower latency in their Internet browsing with SDNS and three participants noted it being a more lightweight and efficient solution to avoid geoblocking than VPNs. As P38 notes, increased network latency is especially noticeable when using online streaming services: "What motivated me to specifically use Smart DNS was the fact that it does not slow down my Internet connection, more specifically, when using streaming services." Two participants also note an additional reason for SDNS' increased efficiency. As P43 explains, SDNS "...only forwards the necessary data for the geo unlock through the designated servers[.] ...[This prevents] speed issues when using the service."

For six participants the choice to specifically use SDNS was informed by its recommendation by someone they trusted. For most (n = 5) of these participants, that person was a friend. However, for one participant (P40), the recommendation came in the form of an "...advertise[ment] by one of the content creators on youtube I watch regularly." Among the remaining participants, other frequently cited reasons for choosing to use SDNS included it being less expensive to use than VPN services (n = 3) and participants' belief that it more effectively evaded detection by content providers (n = 3).

However, one group (n = 5) of participants indicated that they did not know the difference between SDNS and other offerings. For example, P49 stated, "Marketing probably, because I dont know how difefent [sic] work VPN and Smart DNS[.]" This lack of understanding of how SDNS services operated was a common theme in many participants' responses, as we describe in more detail in §5.4.

5.2 Selection of SDNS Provider

While most participants were able to distinguish between SDNS and VPN to some degree, we still observe a high overlap between the factors participants considered when choosing an SDNS provider, and those Khan et al. [18] note as VPN users' key motivations behind their choice of provider.

As shown in Figure 2, participants most strongly considered service price with 24 citing it as the top factor and 52 listing it as one of the top three factors considered overall. The next most considered factors were the provider's trustworthiness, with 12 citing it as the top factor and 35 citing it as one of the three factors, and provider's ratings on review sites, 10 noting it as the top factor and 27 listing it among the three most important factors (**M11**).

5.3 Trustworthiness of Selected Providers

Given that *trustworthiness of a provider* was a common criterion among our participants when selecting their SDNS service, we also consider how participants formed their assessment of trustworthiness. When asked to explain their view on SDNS's overall trustworthiness (**M20**), 16 participants spoke about positive factors that led them to believe their providers were trustworthy.[7] Among these participants, seven cited providers' projected image of security, six noted provider reviews, and four highlighted their provider's overall reputation.

Among the seven participants who mention their providers' projected image of security, most (n = 6) explain that their services provide anonymity and/or added security and privacy. Of those, two participants explicitly tout their provider's use of safeguards such as data encryption, and "no logging" policies to protect their online security and privacy. As P13 (erroneously) states, "[a]ll of Smart DNS proxy servers are encrypted and secured. There are no logs, so all your traffic and data remains anonoymous [sic]..." However, for P51, this image stems in part from SDNS providers' general orientation towards security, noting "[t]he companies involved do seem to be primarily based around online security, so being trustworthy is fundamental to their businesses..."

For the four participants who considered their providers' reputation, checking providers against additional criteria was generally necessary to convince them of their reputability. As other participants explained (n = 3), not all SDNS providers can be trusted. Some providers, as P22 and P45 note, are scams that either "[claim] to offer a smart DNS [but] just charge you for nothing" (P45), or use the rouse of providing SDNS as a means to "...take your info" (P22). Among the criteria these four participants used to determine reputation were user reviews and recommendations (n = 1), providers' years of experience offering their services (n = 1), and their overall track record (n = 1).

As shown in Figure 3, once participants had chosen an SDNS provider, most of them (n = 48) found it trustworthy overall (**M18**).

Breaking Down Trust. We next consider to what degree participants who use SDNS services trust their providers to do certain actions (**M21**). Unsurprisingly, far more participants (n = 54) indicated that they trusted their provider to bypass geoblocking—one of the primary functions of SDNS services—while only four indicated that they did not.

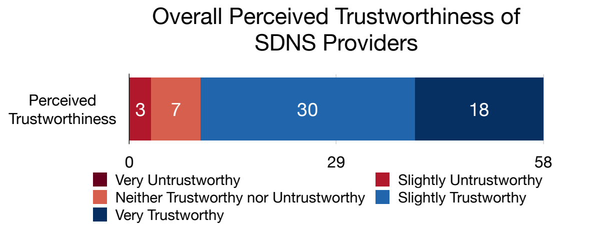

Figure 3: Participants' overall trust of SDNS providers (M19).

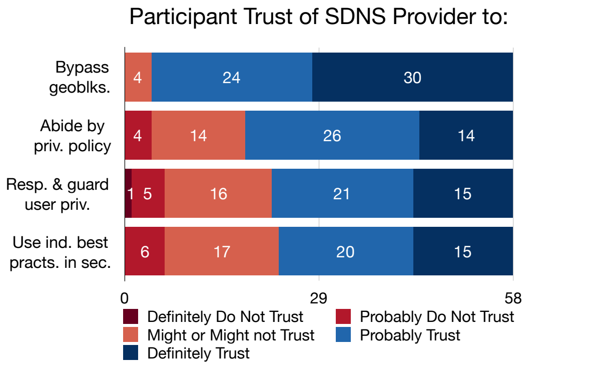

Figure 4: Participants' trust of SDNS providers, broken down by actions (M21).

However, when asked about their willingness to trust their chosen provider to respect and protect their privacy, more participants indicated hesitancy to do so. Specifically, when asked if they trusted their SDNS providers to abide by their privacy policy, fewer participants (n = 40) indicated that they did (relative to the 54 who trusted their ability to bypass geoblocks).

While the majority of participants still trusted their SDNS provider to respect and safeguard their privacy and to use industry best practices in security, many (but not most) participants were hesitant to do so. As Figure 4 further illustrates, only 36 participants trust their provider to respect and safeguard their privacy while 35 trust them to use industry best practices in security (**M21**).

When asked to explain why they trusted these services (**M20**), participants mainly cited that the service reliably worked well (n = 10) and that nothing bad had happened, or that they lacked a reason to distrust their providers (n = 7). That is, many participants acknowledged that by choosing to use SDNS, they were likely taking a risk with their online security and/or privacy. Despite this, these respondents indicated not noticing any evidence of their SDNS service providers harming them.

The remaining respondents (n = 27) implied they still had (varying degrees of) lingering reservations about their providers. Chief among their concerns were how SDNS providers used their personal data (n = 9). As P31 notes, many SDNS providers lack transparency about how they handle their users' data: "I think i [sic] can trust they service, but I'm not so sure how my personal information is

[7] We exclude the ten participants who cited that their service worked reliably, and the seven participants who did not observe any indication of something bad happening when using SDNS, as it is unlikely these participants made these observations before they had chosen a provider.

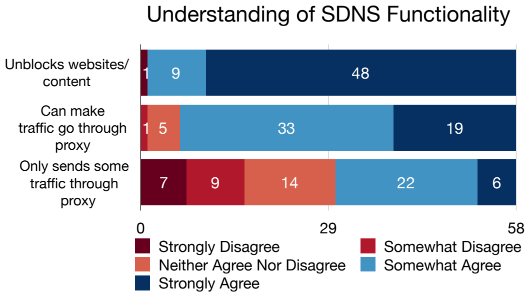

Figure 5: Overall, participants understand SDNS's functionality on a high level. However, many incorrectly attribute VPN functionality to SDNS. This is specifically pronounced in their responses on the frequency with which SDNS sends their Internet traffic through a proxy (M5).

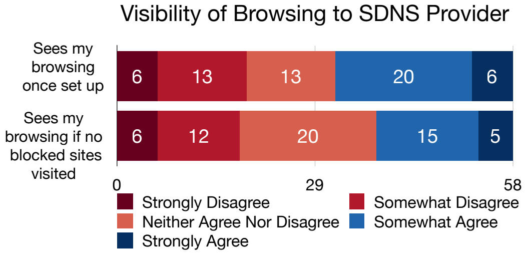

Figure 6: Participant beliefs about the visibility of their browsing to their SDNS provider (M6).

used." Similarly, Q1 notes, "Some may very well make significant money exchanging your data."

5.4 Understanding of SDNS Functionality

As indicated by their motivations to use SDNS (see §5.1), most participants understood that SDNS providers enabled the bypassing of geoblocks. However, many participants struggled to distinguish between SDNS and VPN. In particular, participants largely mis-attributed VPN functionality to SDNS. When asked why they specifically chose to use SDNS rather than a VPN or any other tool capable of bypassing geoblocks (**M10**), four respondents explicitly remarked that they did not know the differences between SDNS and VPNs, and one participant stated that they were unfamiliar with other circumvention options.

Confusion over Prior SDNS Use. Many participants were not able to accurately distinguish their usage of VPNs from that of SDNS. Specifically, five participants who stated they had experience using SDNS (either as a current SDNS user or as a previous one) had in fact confused their usage of a VPN for that of SDNS. Among these respondents, four stated they had used SDNS provided by providers that only offered VPN services, and one provided open responses that strongly indicated they had exclusively used the VPN. We posit that a potential source of this confusion is the marketing and product packaging practices of VPN providers (see §2), especially those that require the purchase of VPN services in order to use their SDNS functionality.

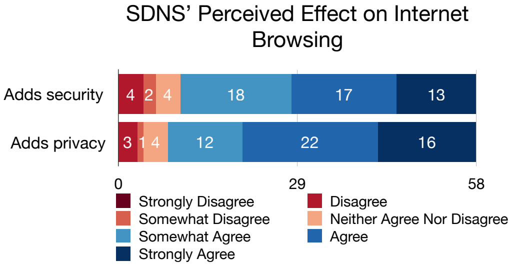

Figure 7: Participant beliefs on SDNS's overall impact on the security and privacy of their Internet browsing (M1, M2).

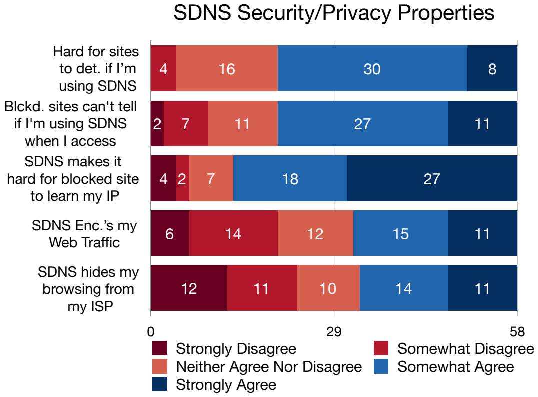

Figure 8: Participant beliefs on SDNS security and privacy qualities (M5, M6).

Among participants who did distinguish between SDNS and VPNs (and other circumvention options), many still showed confusion, or misconceptions about how SDNS works. As shown in Figure 5, much of this disconnect concentrated around the services' routing and proxying behaviors. Specifically, participants' conceptualizations of SDNS systems did not seem to encompass how and when SDNS routes their traffic to proxies.

5.5 Understanding of SDNS' Impacts on Security and Privacy

We found that for many participants, there was a major disconnect between their conceptions of how SDNS operates and actual SDNS functionality. For example, when asked about how SDNS proxies their Internet traffic (**M5**), less than half ($n = 28$) of participants stated (correctly) that SDNS proxied only some of their Internet traffic rather than all of it.

More troubling, participants also tended to underestimate SDNS services' ability to observe which websites are accessed by their users. Because all DNS requests are routed through SDNS services' DNS resolvers, SDNS services have access to the domain names requested by users' browsers. However, when asked whether their SDNS provider could determine which websites they visited (**M6**), less than half of the participants ($n = 26$) correctly indicated that their SDNS provider could see their Internet browsing behavior, as shown in Figure 6. Even fewer participants ($n = 20$) understood that SDNS services can observe the domains to which their users navigate online even if users never visit blocked websites.

More broadly, participants by and large appeared to put undue confidence in the security and privacy offered by SDNS services. As shown in Figure 7, the vast majority of participants (n = 48) at least somewhat agreed that SDNS improved their online security when browsing the Internet (**M1**). Even more participants (n = 50) indicated that SDNS helped protect their privacy when browsing the Internet (**M2**).

When asked about SDNS's security and privacy properties in more detail (see Figure 8), slightly less than half of participants (n = 26) indicated that SDNS encrypts web traffic (in actuality, it does not). Slightly fewer (n = 25) indicated that SDNS hides their browsing behavior from their Internet service provider (ISP); this too is false, since (1) SDNS services do not encrypt traffic and (2) ISPs can observe unencrypted DNS requests to SDNS resolvers.

Additionally, through participants' free text responses (**M4**, **M8**, **M10**, **M20**), we observe several pervasive misconceptions about the security provided by SDNS services. Chief among these were SDNS gives its users (some degree of) anonymity online (n = 11), and using SDNS helps prevent tracking of one's online behavior (n = 9). Amongst the parties from whom respondents claimed SDNS protected against tracking, were advertisers or corporations (n = 3), governments (n = 2), any third party (n = 2), malicious entities (n = 1), and participants' ISPs (n = 1). For P36, the perception that using SDNS would offer anonymity and privacy also served as a large motivation for their decision to use SDNS and not a different service (**M10**): "The ability to feel free knowing that barely noone [sic] can identify me. Obviously this isn't as secure as using .onion, but it narrows down the possibilities for people and organisations to know who I am."

Although not nearly as pervasive, we observe two other noteworthy misconceptions about the security and privacy provided by SDNS. These include perceptions that SDNS was more safe or secure than a VPN (n = 3) and that using SDNS helps mitigate the risks of hacking or malware infection (n = 2).

5.6 Impact of Familiarity with DNS

In addition to determining users' general perceptions of SDNS, we sought to determine whether participants who understood how DNS functions (as a proxy for gauging technical sophistication) tended to show any differences in their conceptions of SDNS.

We first asked participants to estimate their own familiarity with DNS (**S6**) and knowledge of how it worked (**S7**). Here we found that most participants (n = 54) indicated having some familiarity with DNS, and that a smaller majority (n = 38) indicating they at least somewhat knew how DNS works. We then asked them to describe the step-by-step process taken by a computer to navigate to a website (**S8**). Responses to question **S8** were then open-coded to capture what knowledge and possible misconceptions about DNS (and how it works) participants demonstrated in their answers. We provide a list of the codes used for **S8** and a more detailed descriptions/definitions of the meaning assigned to the primary codes used in the artifacts release that accompanies this paper.[8]

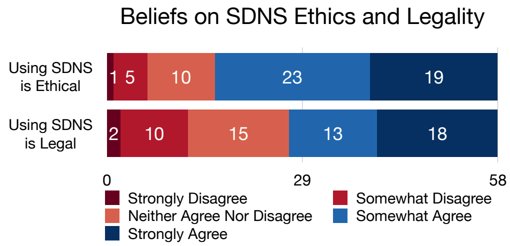

Figure 9: Participant beliefs on the ethics (M27) and legality (M29) of using SDNS.

Based on the initial codes they were assigned, participants' knowledge of DNS was then categorized as being *low*, *medium*, *medium-high* and *high* according to the criteria described in the paper's artifacts. To validate our classification, we then compared participants' estimates (**S7**) of their knowledge with our assessment results, and found the two were highly correlated (Spearman Rank ρ = 0.54).

We then qualitatively assessed the extent to which participants' knowledge of DNS functionality appeared to be correlated with their conceptions of SDNS by creating alluvial plots between participants' answers about the security (**M1**) and privacy (**M2**) implications of using SDNS (**M3**), their beliefs on providers' overall trustworthiness (**M19**), and the level of knowledge they each demonstrated when describing DNS' functionality (**S8**). As illustrated in Figure 10 in Appendix C, we did not find any meaningful indication that participants who were more familiar with DNS held different views about SDNS impact on their security and privacy, or on providers' trustworthiness when compared to participants whose responses indicated lower familiarity with DNS.

5.7 Ethics and Legality of Using SDNS

Ethics of using SDNS. As shown in Figure 9, most participants (n = 42) agreed that using SDNS is ethical. In their reasoning, they cited several factors including the belief that geoblocking is unethical (n = 27), and that they were still paying the content providers whose content they accessed (n = 5).

Amongst the 27 participants who justified using SDNS, eight cited beliefs in a free and open Internet. P32 explained that "the internet has evolved as a virtual world without borders, and it is right that it remains so." Some of these participants (n = 3) described geoblocking as a form of discrimination. For example, P11 stated:

> I believe in free use and free access i [sic] believe it to be unfair and bordering racism if you don't provide users with the same content that you would other if there is no legitimate reason otherwise. (P11)

Others (n = 5) noted that they were still paying to access content.

And finally, four participants stressed little concern from evading geoblocks. P57 said "Why would something like this be unethical. I'm not doing any harm to anyone. I'm just watching Netflix."

[8] See our artifacts repository [7] for the full codebook and https://github.com/GUSecLab/smartdns-study/blob/main/analysis/qualitative_analysis/dns_knowledge_explanation.md for descriptions/definitions of the codes assigned to **S8** responses.

Among the participants whose answers indicated they did not believe bypassing geoblocks using SDNS was ethical, one participant (P49) noted regional copyright and usage rights issues:

> This is hard to explain, its [sic] just comes to tv rights. Maybe netflix has bought the rights for a series, lets say game of thrones but only for america, because in other countries another company has the rights. Well if you are entering and watching game of thrones in that other country u should do it through the company that has the rights who is paying for them.

Given SDNS is used frequently (primarily) to access streaming services, this is noteworthy, as compliance with licensing restrictions is likely the main reaso streaming services perform geoblocking.

Legality of using SDNS. A majority of participants ($n = 31$) believe that using SDNS is legal but slimmer than that for the ethics of using the service. This seems to reflect participants' widespread confusion and lack of awareness of how their local laws address geoblock bypassing, if at all. When asked to explain their reasoning, participants' answers varied. Several participants ($n = 17$) stated that they do not know whether or not it is legal, and another four respondents indicated that its legal status depends on the user's local laws ($n = 3$) or on the purpose of use ($n = 1$). In more detail, 12 participants point out that there is a wide regional variance in local laws governing the usage of tools such as SDNS to bypass geoblocking. In fact, most ($n = 7$) of these respondents state that there likely is no local law prohibiting them from using SDNS.

Other participants ($n = 2$) point out that if geoblock bypass via SDNS is illegal, the laws banning it are not enforced. As Q2 notes, "I think it is legal, but if its not noone is going to come to your house, 'cause a lot of people do worst things in the internet ... "

As P1 describes, this lack of clarity is only magnified by the prevalence of mainstream ads that serve to normalize SDNS usage: "I'm not sure but I would guess it has to be legal for them to be so popular, and advertised on mainstream media (like YouTube)." In some cases, this normalization is also reflected on the information published on various SDNS provider websites. For example, in at least three SDNS providers' FAQ pages, the services argue that their services are legal since it is lawful to both change one's DNS settings and use a proxy server [12, 20, 22]; we lack the expertise to authoritatively assess the legal persuasiveness of these arguments.

6 Discussion and Conclusion

A troubling finding of our study is that most of our participants did not consider the consequences to their security and privacy of using SDNS services. As illustrated by participants' responses, many were not cognizant of the types of vulnerabilities to which they are susceptible when using SDNS. Worse still, many participants were prone to putting undue trust in the protections their SDNS providers purported to offer.

Given the nature of the privacy vulnerabilities identified by Fainchtein et al. [8], SDNS users are unlikely to recognize whether their privacy has been breached. Specifically, the attacks Fainchtein et al. identify do not give their victims any indications that anything went awry. As such, participants' widespread belief that nothing nefarious has happened due to their SDNS usage may be inaccurate.

Since many of the privacy vulnerabilities associated with SDNS usage are inherent to these systems' architecture [8], there is no straightforward means to adequately remedy them or mitigate the risks they pose while using SDNS. As such, the best way a user could protect themselves against these threats to their privacy would be to stop using SDNS altogether. To continue evading geoblocking, users could switch to a geoblock evasion tool with more robust security such as a VPN, or Tor. For participants who indicated using SDNS because they (1) were unfamiliar with other geoblock evasion tools, (2) did not know the difference between SDNS and other options for bypassing geoblocks, or (3) had misconceptions about SDNS' impact on their online security and privacy, user education may be beneficial. This education would need to explain the security and privacy risks of using SDNS, and to address common user misconceptions about these systems. In particular, educators would need to address common user misconceptions about SDNS' impact on their online security and privacy, and to stress that (1) SDNS usage inherently opens users up to privacy risks to which they would not otherwise be vulnerable; and (2) that a user whose privacy has been breached often receives no indication that this occurred.

One means by which this could be achieved is through the publication of accurate and easily accessible information about SDNS systems, how using them impacts users' online security and privacy. In the case of selecting a trustworthy VPN provider, Khan et al. recommend providing easy access to unbiased, thorough and peer-reviewed information about the most prominent service providers [18]. They argue that doing so would help inform VPN users' decisions and encourage them to make more secure choices of provider. Such advice may also be applicable to SDNS users. As such, we recommend the publication of online guides or articles describing the risks associated with using SDNS, written to be accessible to individuals lacking technical backgrounds.

To redirect willing SDNS users to a more secure means of geoblock evasion, education would also need to provide guidance on how to select a trustworthy and secure alternative to SDNS. Such guidance would need to either include basic descriptions of these options including their respective capabilities and limitations, or link to existing sources with this information.

However, while education is likely to be beneficial to many SDNS users, it would not be reasonable to expect it to consistently empower/influence users to stop using SDNS. As noted in §5.4, many participants chose to use SDNS in lieu of VPN due to its increased usability. Previous research by Kang et al. finds that Internet users are often deterred from taking actions to protect their privacy when they perceive they would have to sacrifice convenience do so, or that the software tools aimed at protecting their privacy have poor usability [17]. Ruoti et al. expand on this further, noting that, when determining which security and privacy measures to adopt, users opt for measures that will not impede their ability to use the Internet [28]. Given our findings indicating many SDNS users view geoblocking as an unethical practice, a form of censorship and discrimination, and as being directly in conflict with (their belief in) the open Internet, these users may see successful geoblock evasion as a prerequisite for (or core component of) their ability to use the Internet. Therefore, persuading these SDNS users to adopt VPNs instead would likely require a VPN service that boasted similar, if not better, usability than the SDNS services that are currently available. In the case where these SDNS users find the VPN falls short of offering comparable usability to SDNS, they may decide to continue using SDNS services despite the risks they pose.

Acknowledgments

We are grateful to the anonymous reviewers for their feedback, and especially to our shepherd, Phani Vadrevu, for the many suggestions that helped us improve this paper. We also would like to thank Darika Shaibekova for her extensive work as second coder on free-text responses. This paper is partially supported by the National Science Foundation under grants CNS-2138078 and CNS-2138654 and the Georgetown University Callahan Family Chair Fund. The opinions and findings expressed in this paper are strictly those of the authors and do not necessarily those of any employer or funding agency.

References

[1] Sadia Afroz, Michael Carl Tschantz, Shaarif Sajid, Shoaib Asif Qazi, Mobin Javed, and Vern Paxson. 2018. Exploring Server-side Blocking of Regions. *arXiv preprint arXiv:1805.11606* (2018).

[2] Alessandro Acquisti and Jens Grossklags. 2005. Privacy and rationality in individual decision making. *IEEE Security Privacy* 3, 1 (2005), 26–33.

[3] Allison McDonald, Matthew Bernhardand Luke Valenta, Benjamin VanderSloot, Will Scott, Nick Sullivan, J. Alex Halderman, and Roya Ensafi. 2018. 403 Forbidden: A Global View of CDN Geoblocking. In *Proceedings of the Internet Measurement Conference (IMC).*

[4] S. Blake-Wilson, M. Nystrom, D. Hopwood, J. Mikkelsen, and T. Wright. 2003. *Transport Layer Security (TLS) Extensions.* RFC 3546. Internet Engineering Task Force.

[5] Roger Dingledine, Nick Mathewson, and Paul Syverson. 2004. Tor: The Second-Generation Onion Router. In *USENIX Security Symposium (USENIX).*

[6] ExpressVPN. 2022. Get Started with 5 Awesome Ways to Use ExpressVPN. https://www.expressvpn.com/get-started.

[7] Rahel A. Fainchtein, Adam J. Aviv, and Micah Sherr. 2022. User Perceptions of the Privacy and Usability of Smart DNS: Codebook and Other Artifacts. https://github.com/GUSecLab/smartdns-study/blob/main/analysis/qualitative_analysis/codebook.pdf.

[8] Rahel A. Fainchtein, Adam J. Aviv, Micah Sherr, Stephen Ribaudo, and Armaan Khullar. 2021. Holes in the Geofence: Privacy Vulnerabilities in "Smart" DNS Services. *Proceedings on Privacy Enhancing Technologies (PoPETS)* (2021).

[9] Kevin Gallagher, Sameer Patil, and Nasir Memon. 2017. New Me: Understanding Expert and Non-Expert Perceptions and Usage of the Tor Anonymity Network. In *Symposium on Usable Privacy and Security (SOUPS).*

[10] Gambino, Andrew and Kim, Jinyoung and Sundar, S. Shyam and Ge, Jun and Rosson, Mary Beth. 2016. User Disbelief in Privacy Paradox: Heuristics That Determine Disclosure. In *Conference Extended Abstracts on Human Factors in Computing (CHI).*

[11] Gueye Bamba, Arthur Zivani, Mark Crovella, and Serge Fdida. 2004. Constraint based Geolocation of Internet Hosts. In *Internet Measurement Conference (IMC).*

[12] HideIPVPN. 2021. What Is Smart DNS? (How Does Smart DNS Work?). https://www.hideipvpn.com/learning-center/what-is-smart-dns-how-does-smart-dns-work/.

[13] P. Hoffman and P. McManus. 2018. *DNS Queries over HTTPS (DoH).* RFC 8484. Internet Engineering Task Force.

[14] Z. Hu, L. Zhu, J. Heidemann, A. Mankin, D. Wessels, and P. Hoffman. 2016. *Specification for DNS over Transport Layer Security (TLS).* RFC 7858. Internet Engineering Task Force.

[15] Iulia Ion, Rob Reeder, and Sunny Consolvo. 2015. "...no one can hack my mind": Comparing Expert and Non-Expert Security Practices. In *Symposium On Usable Privacy and Security (SOUPS).*

[16] Josh. 2022. SmartDNS | What Is It and How do You Set it Up? (2022 Guide). All Things Secured. Available at https://www.allthingssecured.com/vpn/faq/what-is-smartdns/.

[17] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. 2015. "My Data Just Goes Everywhere": User Mental Models of the Internet and Implications for Privacy and Security. In *Symposium On Usable Privacy and Security (SOUPS).*

[18] Mohammad Taha Khan, Joe DeBlasio, Chris Kanich, Geoffrey M. Voelker, Alex C. Snoeren, and Narseo Vallina-Rodriguez. 2018. An Empirical Analysis of the Commercial VPN Ecosystem. In *ACM SIGCOMM Conference on Internet Measurement (IMC).*

[19] Sheharbano Khattak, David Fifield, Sadia Afroz, Mobin Javed, Srikanth Sundaresan, Damon McCoy, Vern Paxson, and Steven J Murdoch. 2016. Do You See What I See? Differential Treatment of Anonymous Users. In *Network and Distributed System Security Symposium (NDSS).*

[20] Martynas Klimas. 2021. https://surfshark.com/blog/smart-dns-vs-vpn.

[21] Laki, Sándor and Mátray, Péter and Hága, Péter and Sebők, Tamás and Csabai, István and Vattay, Gábor. 2011. Spotter: A Model Based Active Geolocation Service. In *International Conference on Computer Communications (INFOCOM).*

[22] Tim Morcan. 2019. What Is Smart DNS Tech & How Does Smart DNS Work? https://www.cactusvpn.com/beginners-guide-to-smart-dns/what-is-smart-dns/#legality.

[23] Muir, James A. and Oorschot, Paul C. Van. 2009. Internet Geolocation: Evasion and Counterevasion. *Comput. Surveys* 42, 1 (December 2009).

[24] Moses Namara, Daricia Wilkinson, Kelly Caine, and Bart P Knijnenburg. 2020. Emotional and Practical Considerations Towards the Adoption and Abandonment of VPNs as a Privacy-Enhancing Technology. *Proceedings on Privacy Enhancing Technologies (PoPETS)* 2020, 1 (2020), 83–102.

[25] NordVPN. 2022. NordVPN. https://nordvpn.com/.

[26] Ingmar Poese, Steve Uhlig, Mohamed Ali Kaafar, Benoit Donnet, and Bamba Gueye. 2011. IP Geolocation Databases: Unreliable? *ACM SIGCOMM Computer Communication Review* 41, 2 (April 2011), 53–56.

[27] Rick Wash and Emilee Rader. 2015. Too Much Knowledge? Security Beliefs and Protective Behaviors Among United States Internet Users. In *Symposium on Usable Privacy and Security (SOUPS).*

[28] Scott Ruoti and Tyler Monson and Justin Wu and Daniel Zappala and Kent Seamons. 2017. Weighing Context and Trade-offs: How Suburban Adults Selected Their Online Security Posture. In *Symposium on Usable Privacy and Security (SOUPS).*

[29] Rachee Singh, Rishab Nithyanand, Sadia Afroz, Paul Pearce, Michael Carl Tschantz, Phillipa Gill, and Vern Paxson. 2017. Characterizing the Nature and Dynamics of Exit Blocking. In *USENIX Security Symposium (USENIX).*

[30] StrongVPN. 2022. Why Do I Need a VPN? | StrongVPN. https://strongvpn.com/vpn-uses/.

[31] S. Shyam Sundar. 2008. *The MAIN Model: A Heuristic Approach to Understanding Technology Effects on Credibility.* The MIT Press, 72—-100.

[32] Marketa Trimble. 2012. The Future of Cybertravel: Legal Implications of the Evasion of Geolocation. *Fordham Intellectual Property, Media & Entertainment Law Journal* 22 (April 2012).

[33] Marketa Trimble. 2021. A New CJEU Judgment on Copyright-Related Geoblocking – One Step Forward or One Step Back in the EU Commission's Fight Against Geoblocking? (Guest Blog Post) in *Technology & Marketing Law Blog*. https://blog.ericgoldman.org/archives/2021/01/a-new-cjeu-judgment-on-copyright-related-geoblocking-one-step-forward-or-one-step-back-in-the-eu-commissions-fight-against-geoblocking-guest-blog-post.htm.

[34] Zachary Weinberg, Shinyoung Cho, Nicolas Christin, Vyas Sekar, and Phillipa Gill. 2018. How to Catch when Proxies Lie: Verifying the Physical Locations of Network Proxies with Active Geolocation. In *ACM SIGCOMM Conference on Internet Measurement (IMC).*

[35] Bernard Wong, Ivan Stoyanov, and Emin Gün Sirer. 2007. Octant: A Comprehensive Framework for the Geolocalization of Internet Hosts. In *USENIX Symposium on Networked Systems Design and Implementation (NSDI).*

[36] Zhao Zhang, Tavish Vaidya, Kartik Subramanian, Wenchao Zhou, and Micah Sherr. 2020. Ephemeral Exit Bridges for. In *IEEE/IFIP International Conference on Dependable Systems and Networks (DSN).*

[37] Zhao Zhang, Wenchao Zhou, and Micah Sherr. 2020. Bypassing Exit Blocking with Exit Bridge Onion Services. In *ACM Conference on Computer and Communications Security (CCS).*

A Survey Instruments

The following question ordering reflects how this survey was presented to Reddit participants. Participants who took the survey through Prolific were given questions S1 through S9, and D1 through D6 as a screening survey, and completed M1 through M31 as the main survey.

S1 How familiar are you with Smart DNS services?

- ○ Not at all familiar
- ○ Slightly familiar
- ○ Somewhat familiar
- ○ Moderately familiar
- ○ Extremely familiar

S2 What are Smart DNS services primarily used for?
Answer: ________

S2 Do you currently use Smart DNS, or have you done so in the past?

- ○ Yes
- ○ No
- ○ I'm not sure

S3 Are you seriously considering using Smart DNS within the near future?

- ○ Yes
- ○ No
- ○ I prefer not to answer

S4 only shown if answer to S3 is not "Yes"

S4 Which SmartDNS services have you used before or are you seriously considered using? (Select all that apply)

- ○ AceVPN
- ○ Blockless
- ○ BulletVPN
- ○ CactusVPN
- ○ DNSFlex
- ○ GetFlix
- ○ HideIPVPN
- ○ Invisible Browsing (IB-VPN/IBDNS)
- ○ IronSocket
- ○ KeepSolid
- ○ Le-VPN
- ○ NordVPN
- ○ Overplay
- ○ PureVPN
- ○ SimpleTelly
- ○ SmartDNSProxy
- ○ SmartyDNS
- ○ StrongDNS
- ○ SurfShark
- ○ TrickByte
- ○ TVWhenAway
- ○ Uflix
- ○ Unblock-Us
- ○ Unlocator
- ○ VPNSecure
- ○ VPNUK
- ○ Other: ________
- ○ I do not recall *

** denotes an exclusive answer.*

S5 only shown if "Yes" answered to S3 or "Yes" answered to S4.

S5 Which of the following types of Smart DNS accounts have you had or used (including any accounts you currently have/use)? (Select all that apply.)

- ○ Free Trial
- ○ Paid Subscription
- ○ I Used Someone else's account
- ○ I am unsure*
- ○ I have never had nor used a Smart DNS account*

** denotes an exclusive answer.*

Now we are going to ask you questions about the **Domain Name System (DNS)** which is *different from Smart DNS.*

S6 How familiar are you with the Domain Name System (DNS)?

- ○ Extremely Familiar
- ○ Very Familiar
- ○ Moderately Familiar
- ○ Slightly Familiar
- ○ Not Familiar at all

S7 Do you know how the Domain Name System (DNS) works?

- ○ I definitely know
- ○ I somewhat know
- ○ I'm not sure I know
- ○ I definitely do not know

S8 To the best of your knowledge, explain how DNS works by describing the steps taken by your computer when you navigate to a website like http://www.example.com
Answer: ________

M1 Smart DNS provides additional security when browsing the Internet.

- ○ Strongly agree
- ○ Agree
- ○ Somewhat agree
- ○ Neither agree nor disagree
- ○ Somewhat disagree
- ○ Disagree
- ○ Strongly disagree

M2 Smart DNS provides additional privacy when browsing the Internet.

- ○ Strongly agree
- ○ Agree
- ○ Somewhat agree
- ○ Neither agree nor disagree
- ○ Somewhat disagree
- ○ Disagree
- ○ Strongly disagree

M3 Using Smart DNS is a risk to my security and privacy.

- ○ Strongly agree
- ○ Agree
- ○ Somewhat agree
- ○ Neither agree nor disagree
- ○ Somewhat disagree
- ○ Disagree
- ○ Strongly disagree

M4 Please explain why you think Smart DNS can affect your security and privacy in the way(s) you indicated. ________

M5 Note whether you agree or disagree with each of the following statements about Smart DNS.

	Stgly. Agr.	Swhat. Agr.	Neit. Agr. nor Disgr.	Swhat. Disgr.	Stgly. Disgr.
(i) Smart DNS encrypts my web traffic.	○	○	○	○	○
(ii) Smart DNS slows down my Internet connection.	○	○	○	○	○
(iii) Smart DNS Can make my Internet traffic go through a proxy server.	○	○	○	○	○
(iv) Smart DNS lets me access websites and/or content that I otherwise couldn't access.	○	○	○	○	○
(v) Smart DNS speeds up my Internet connection.	○	○	○	○	○
(vi) It is difficult for a website to determine if I am using Smart DNS to access it.	○	○	○	○	○
(vii) When I use Smart DNS, some sites are accessed via Smart DNS' proxies, while others are not.	○	○	○	○	○

M6 Note whether you agree or disagree with each of the following statements about Smart DNS.

	Stgly. Agr.	Swhat. Agr.	Neit. Agr. nor Disgr.	Swhat. Disgr.	Stgly. Disgr.
(i) Using Smart DNS hides my browsing activity from my Internet Service Provider.	○	○	○	○	○
(ii) Once I have set up Smart DNS on my computer, my Smart DNS provider can see which websites my computer visits.	○	○	○	○	○
(iii) Once I have set up Smart DNS on my computer, my Smart DNS provider can see which websites my computer visits even if I never use it to visit blocked websites.	○	○	○	○	○
(iv) Smart DNS makes it more difficult for a blocked website to determine my IP address.	○	○	○	○	○
(v) If I access a blocked website using Smart DNS, the website will not be able to tell I am using Smart DNS.	○	○	○	○	○

M7 It is worthwhile to put in the effort to use Smart DNS.

- ○ Strongly agree
- ○ Agree
- ○ Somewhat agree
- ○ Neither agree nor disagree
- ○ Somewhat disagree
- ○ Disagree
- ○ Strongly disagree

M8 What was your main goal in using a Smart DNS service?

Answer: __________

M9 Which countries' websites do/did you most often access using Smart DNS services? To select multiple options hold down the Control (Command on Mac) and click the answers you would like to select. To deselect a single answer hold down the Control key (Command on Mac) and click the option you would like to deselect.
Dropdown list of countries

M10 Like other services, Smart DNS services come with a specific set of strengths and weaknesses. Given that Smart DNS services are not the only offerings capable of unblocking geo-fenced websites (for example, some VPN services can do this as well), what motivated you to specifically use Smart DNS?
Answer: __________

M11 When you chose a Smart DNS service, which of the following factors did you consider most relevant? (If you plan to use Smart DNS in the near future, which of the factors are you most strongly considering?) Select up to three factors, and rank them by entering 1-3 in the text box to their left, where 1 is the most relevant item selected.
○ Price
○ Service's rating on a review site
○ Offered channels
○ Additional service offerings
○ Provider's Trustworthiness
○ Customer support
○ Company location (e.g., based in US, UK, etc.)
○ They offered a free trial
○ I just used the first one I found
○ Other (please specify):__________

M12 Does the Smart DNS provider you use, used, or plan to use, offer any services in addition to Smart DNS?
○ Yes
○ No
○ I'm Unsure

M13 and M14 are only displayed if participant answered "Yes" to M12.

M13 When you signed up for your provider's service(s) were you primarily looking to use their Smart DNS?
○ Yes
○ No
○ I'm Unsure

M14 Which other services does/did your Smart DNS provider offer? (Select all that apply)
○ I'm not sure*
○ VPN
○ P2P Torrent Support
○ Ad Blocking
○ Firewalls
○ Other (please specify):__________

** denotes exclusive answer*

M15 is only displayed if participant answers "Yes" to M12 and does not select "I'm not sure" on M14.

M15 Which, if any, of these services have you used, or do you plan on using? (Select all that apply)
[Selected choices from M14]
○ I did not use, nor plan on using any other services*
** denotes exclusive answer.*

M16 When was the last time you set Smart DNS on a device?
○ in the past few months
○ in the past few days
○ in the past few hours
○ I have not set up Smart DNS on a device

M17 Have you set up Smart DNS on the device you are using to complete this survey?

○ Definitely yes
○ Probably yes
○ Might or might not
○ Probably not
○ Definitely not

M18 Is Smart DNS currently enabled on the device you are using to complete this survey?
○ Yes
○ No
○ I'm Unsure

M19 How trustworthy do you find these services overall?
○ Very Trustworthy
○ Slightly Trustworthy
○ Neither Trustworthy nor Untrustworthy
○ Slightly Untrustworthy
○ Very Untrustworthy

M20 Please describe your view on the overall trustworthiness of Smart DNS.
Answer: __________

M21 To what extent do you trust your Smart DNS provider to:

	Definitely Trust	Probably Trust	Might or Might Not Trust	Probably Do Not Trust	Definitely Do Not Trust
(i) Allow you to bypass blocking as advertised?	○	○	○	○	○
(ii) Abide by its privacy policy?	○	○	○	○	○
(iii) Respect your personal data and keep it private?	○	○	○	○	○
(iv) Use industry best practices in security?	○	○	○	○	○

M22 Based on your experience, how often does Smart DNS successfully allow access to blocked content?
○ Always
○ Most of the Time
○ About Half of the time
○ Sometimes
○ Never

M23 Have you ever been blocked by a content provider because you were using Smart DNS?
○ Yes
○ No
○ I'm Unsure

M25 and M26 only displayed if participant answered "Yes" to M24

M24 How do you think they determined you were using Smart DNS?
Answer: __________

M25 How frequently are you blocked for this reason?
○ Always
○ Most of the Time
○ About Half of the time
○ Sometimes
○ Never

M27 only displayed if participant answered "No" or "I'm Unsure" to M24

M26 How easy do you think it would be for content providers to determine if you were using Smart DNS?
○ Extremely easy
○ Moderately easy
○ Slightly easy
○ Neither easy nor difficult
○ Slightly difficult
○ Moderately difficult
○ Extremely difficult

Ethics and Legality Because Smart DNS allows you to access content that would normally be unavailable in your geographic region, there may be disagreement among users regarding the ethics and legality of using Smart DNS. Based on your opinions, state how much you agree, or disagree with each of the following statements. After each statement, you will be asked to explain your response.

M27 Using Smart DNS to access content outside my geographic region is ethical.
○ Strongly agree
○ Agree
○ Somewhat agree
○ Neither agree nor disagree
○ Somewhat disagree
○ Disagree
○ Strongly disagree

M28 Please explain your prior response:
Answer: __________

M29 Using Smart DNS to access content outside my geographic region is legal.
○ Strongly agree
○ Agree
○ Somewhat agree
○ Neither agree nor disagree
○ Somewhat disagree
○ Disagree
○ Strongly disagree

M30 Please explain your prior response:
Answer: __________

D1 What is your age?
○ 18 – 24
○ 25 – 34
○ 35 – 44
○ 45 – 54
○ 55 – 64
○ 65 – 74
○ 75 – 84
○ 85 or older
○ I prefer not to disclose

D2 What is the gender to which you most closely identify?
○ Male
○ Female
○ Non-binary
○ I prefer to self-describe
○ I prefer not to answer

D3 What is the highest level of school you have completed or the highest degree you have received?
○ Less than a High School Degree
○ High school graduate (high school diploma or equivalent including GED)
○ Some college but no degree
○ 2 year degree (e/g Associate degree in college or trade degree)
○ Bachelor's degree in college (4-year)
○ Master's degree
○ Professional degree (e. g., J.D., M.D.)
○ Doctoral degree (PhD)
○ I Prefer not to answer

D4 In which country do you currently reside?

D5 What is your nationality?

D6 What is your annual income in US Dollars?
○ Less than $10, 000
○ $10, 000 – $19, 999
○ $20, 000 – $29, 999
○ $30, 000 – $39, 999
○ $40, 000 – $49, 999
○ $50, 000 – $59, 999
○ $60, 000 – $69, 999
○ $70, 000 – $79, 999
○ $80, 000 – $89, 999
○ $90, 000 – $99, 999
○ $100, 000 – $149, 999
○ More than $150, 000
○ I prefer not to disclose

B SDNS Service Providers

Service Provider	Total Used	SDNS	VPN
NordVPN	42	Yes	Yes
SmartDNSProxy	10	Yes	Yes
PureVPN	9	Yes	Yes
SurfShark	9	Yes	Yes
VPNSecure	6	Yes	Yes
ExpressVPN	4	Yes*	Yes
Unblock-Us**	4	Yes	Yes
HolaVPN	3	Yes	Yes
BulletVPN	2	Yes	Yes
DNSFlex	2	Yes	Yes
SmartyDNS	2	Yes	Yes
Windscribe	2	Yes	Yes
Blockless**	1	Yes	Yes
CactusVPN	1	Yes	Yes
GetFlix	1	Yes	Yes
IBVPN/IBDNS**	1	Yes	Yes
KutoVPN	1	**No**	Yes
Mullvad	1	**No**	Yes
OperaVPN	1	**No**	Yes
ProtonVPN	1	**No**	Yes
SimpleTelly	1	Yes	No
StrongDNS	1	Yes	Yes
VPNUK	1	Yes	Yes

Table 2: Service providers that participants indicated they had used, the total participants who indicated using them, and whether they respectively offered SDNS and/or VPN services. Demarcation with Yes* indicates that the provider previously offered this service, but no longer appeared to do so based on their website. Service providers demarcated with two asterisks (**) appear to no longer be in business.

C Impact of Knowledge of DNS Functionality

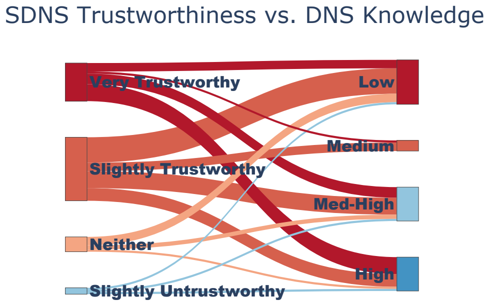

Figure 10: Participants' beliefs of SDNS providers' trustworthiness (M18) and their assessed knowledge of DNS based on responses to S8. As illustrated above, the two did not appear to be correlated.