Two Sides of the Shield: Understanding Protective DNS adoption factors

Elsa Rodríguez, Radu Anghel, Simon Parkin, Michel van Eeten, and Carlos Gañán, *Delft University of Technology*

https://www.usenix.org/conference/usenixsecurity23/presentation/rodriguez

This paper is included in the Proceedings of the 32nd USENIX Security Symposium.

August 9–11, 2023 • Anaheim, CA, USA

978-1-939133-37-3

Two Sides of the Shield: Understanding Protective DNS Adoption Factors

Elsa Rodríguez, Radu Anghel, Simon Parkin, Michel van Eeten, Carlos Gañán
Delft University of Technology

Abstract

Protective DNS (PDNS) filters out DNS requests leading to harmful resources. PDNS is currently being promoted by various governments and industry players – some global public DNS providers offer it, as do some government-sponsored DNS resolvers. Yet, are end users even interested in adopting it? The extent of current PDNS usage, as well as the factors that encourage or discourage end-users' adoption, have not been studied. We found that overall PDNS adoption is minimal, though in some countries over 20% of the DNS queries are being answered by these types of resolvers. Four human-subjects studies were undertaken to understand end-user adoption factors: a survey with 295 consumers; 24 interviews with ISP customers offered a free PDNS after a malware infection; 12 interviews with public and private enterprise professionals, and 9 interviews with DNS technology specialists. We found that users are more likely to use PDNS if operated by their own ISP rather than the government. For enterprises, we uncovered that access to global threat intelligence, a layered security strategy, and compliance with regulations were the main factors for PDNS adoption. The DNS technical specialists highlighted broader challenges of PDNS adoption such as transparency and centralization.

1 Introduction

To access most Internet-connected services, the Domain Name System (DNS) is a crucial component [1]. The resolution of domain names to IP addresses has traditionally been provided by the recursive DNS resolvers of Internet Service Providers [2]. Since 2006, alternative recursive DNS resolvers, also called public DNS resolvers (a.k.a. open resolvers) have emerged [2, 3]. Companies such as Google, Cloudflare, Yandex and Cisco, and non-profits such as Quad9, have positioned their services as alternatives.

Every day, millions of new domain names are registered, some of which attackers use to redirect end users to harmful resources [4]. Hence, some of the public DNS resolvers offer services that aim to protect users by preventing the resolution of domains that lead to known malicious resources, like phishing or malware sites [5–8]. This type of DNS filtering is called Protective DNS (PDNS) [9, 10].

Recently, some governments have started advocating that their citizens and enterprises should adopt PDNS as a security measure. The United Kingdom requires public sector organizations to use PDNS [10] and encourages adoption by private organizations. In the United States, the National Security Agency (NSA) and Cybersecurity and Infrastructure Security Agency (CISA) suggest that organizations use protective DNS as a best practice for their security strategy [9].

Some governments are actually backing specific PDNS services. Canada supports the CIRA Canadian Shield [11]. In January 2022, the European Commission announced plans to introduce DNS4EU [12], a recursive European DNS resolver service to protect citizens from malware, phishing, and other threats. The commission selected a public-private consortium to run the service and onboard 100 million users [13]. Australia has an initiative to encourage public sector entities that provide critical services to use AUPDNS, a DNS resolver that blocks cyber threats [14].

Although many governments and industry actors are pushing for PDNS services, their adoption critically depends on acceptance by consumers and enterprises. So far, solutions backed by a government have been imposed within government infrastructure itself, but not outside of it. The success of PDNS initiatives is based on voluntary adoption by users or their service providers. Service providers, in turn, have little incentive to adopt PDNS and provide it by default if there is no demand for it from their customers, since it also means losing a crucial data source for monitoring security threats on their network (e.g., observing customer DNS queries to botnet command-and-control servers). Even though adoption is critical to success, no research has examined whether citizens and enterprises have currently adopted PDNS and what factors drive or discourage adoption. Our research aims to fill this gap.

The closest related work asked home users about DNS over HTTPS (DoH) settings in Brave, Chrome, Edge, Firefox, Opera, and Android mobile operating system [15, 16]. These studies examined whether users changed their DNS settings after being told about encrypted DNS. DoH concerns user privacy, specifically which DNS provider can see queries. Our work explores user perceptions of DNS filtering by the resolver, which is previously unexplored and has implications for both the growing market in PDNS products and nation-level strategies for the uptake and utility of PDNS.

Our first research question is: what is the extent of adoption of public DNS and, in particular, PDNS? We estimate adoption by analyzing a dataset from the Asia Pacific Network Information Centre (APNIC) Labs [17]. From data from over 240 countries and territories on DNS recursive resolver usage and more than 15M average daily DNS queries over six months, we identify which portion went to PDNS providers. Earlier work underlined the importance of examining adoption factors for user-facing security and privacy technologies [18]. Hence, the main contribution of our study is focused on our second research question: what factors encourage or discourage the adoption of Protective DNS by users and organizations? For this question, we conducted four complementary human-subject studies. First, we carried out a survey in Prolific [19] with 295 participants to understand users' views on a PDNS service and what factors they would consider for adopting it. Where the survey captures the intention to adopt, we complement it with an interview study with data on actual adoption, with 24 customers of an Internet Service Provider who were offered to opt-in for a 'malware protection service' based on PDNS. Next, we interviewed 12 professionals in public and private organizations to understand factors to consider for adopting a PDNS resolver in an enterprise context. Finally, we interviewed 9 DNS technology experts who provided their reasoning on broader challenges before adopting PDNS resolvers. The main contributions of this paper are:

- By analyzing DNS recursive resolver usage of over 240 countries and territories and 15M average daily DNS queries, we determine the adoption of commercial PDNS resolvers in different regions (Asia, Africa, America, Oceania, and Europe) and countries.
- This research is the first to examine, across a variety of vantage points – namely users, ISP customers, enterprises, and experts – the factors that influence the adoption of PDNS as a security countermeasure.
- We find an adoption intention for 58% of users, but signal might overestimate demand, as only 9% of users signed up when the ISP we partnered with offered them PDNS after they had suffered a malware infection.

2 Methodology

Given the recent push for PDNS, we first analyze a DNS resolution dataset for evidence on PDNS adoption. Next, we survey end users to learn about adoption factors. To complement the survey, we interviewed ISP customers who were offered a free PDNS service by their ISP. Then, we analyze interviews with professionals about why their organizations might adopt or not PDNS. Finally, we interview experts on the relevant factors for or against PDNS adoption.

2.1 Recursive DNS resolvers measurement

APNIC dataset description. Asia Pacific Network Information Centre (APNIC) Labs performs a daily DNS resolver measurement to record users' sets of resolvers in DNS logs using a Google advertisement campaign [20, 21].

APNIC links the DNS resolver's Internet Protocol (IP) address and the user IP address to their autonomous system (AS) to identify the resolver type. If the resolver IP and user IP belong to the same AS, the resolver operator is most likely the user's ISP. This is counted as the resolver being in the 'same AS'. This omits public DNS resolvers. If the resolver IP address and the user IP address are in the same country, they increase the 'in country' count or 'out country' if the IP address of the operator of the resolver is not in the same country as the user IP. Public DNS resolver counts are excluded from 'in country' and 'out country' counts. Finally, if the resolver's IP address is associated with an AS of a public DNS resolver, they add the count to that resolver.

Processing and analysis of APNIC dataset. We employed the 'first use' resolvers – which is the first resolver seen for the user query in the DNS logs from January to June 2022 – to estimate which portion of DNS queries show PDNS usage. The data we obtained contains only the daily counts of DNS requests answered by each APNIC-labeled DNS resolver.

To determine if each public DNS resolver was a PDNS or not, we thoroughly examined their websites and service descriptions. We classified public DNS resolvers as 'Protective DNS (PDNS)' if they advertise themselves as protecting against botnets, malware, phishing, and spam. If not, they were categorized as 'No Protective DNS'. Cloudflare, Yandex, and Quad9 offer PDNS-enabled and PDNS-disabled services. Since we can only have access to counts, it is hard to determine which one the user is using, so we classify them as 'Possible Protective DNS'. Finally, we came across three cases -— Free DNS, Level 3, and puntCAT —- where we could not find information to determine whether they offer PDNS or not, so we categorized them as 'No information'. See Appendix A for summary of the classification of the public DNS resolvers.

Next, the penetration of each DNS resolver category was computed as a percentage. We divided the sum of the average daily unique queries per resolver type by the total average daily DNS queries. We calculated the percentage per country and aggregated different regions (Asia, Africa, America, Oceania, and Europe). China was undersampled compared to its Internet users, thus we removed it from our analysis.

2.2 Prolific survey

In August 2022, we ran a survey on Prolific [19] to gauge users' PDNS adoption intentions. The survey was created with Qualtrics. We paid proportional to the participants' completion time using the equivalent to the minimum wage from where the authors are based. PDNS was described to participants based on a literature review of the UK government's existing description [10] and the European Union tender for DNS4EU [12]. The survey design was informed by Fogg's behavior adoption model [22], which posits that motivation (M), ability (A), and trigger (T) (now 'prompt' [23]) affect how likely a behavior is to occur (in this case, opting in for PDNS).

Motivation focuses on the users' reasons for opting into PDNS. We asked participants about their 'perceived vulnerability' and 'perceived severity' to operationalize their motivations. Two questions concerned privacy, and a third examined the service's effectiveness against common threats. We also asked participants about what they regarded as significant threats, and whether they believed the service would be useful against them.

Users' skills determine the ability to perform a behavior. Time, effort, money, and pondering are elements of simplicity that increase ability [22]. We added questions about participants' ability to configure security on their devices, if they had other security methods, and use parental controls. Also, participants were asked if they would pay for the service. Finally, participants' awareness of comparable services was questioned, as a user may know about PDNS (i.e., have the ability), but not have the motivation to enable it.

Finally, according to Fogg's model [22, 23], triggers/prompts can be 'facilitators' that make the behavior easier, 'sparks' that inspire behavior, or 'signals' that remind the person to perform a behavior. A facilitator here could ease the adoption of PDNS or indicate its benefits – ISPs, DNS providers, and governments can facilitate DNS-blocking. Participants were asked which provider they preferred (Government, ISP, or commercial organization), but could add another.

Participants were also asked basic questions about their Internet usage and their computing devices. Open-ended questions let respondents explain their answers; some of these answers will be described in the results (See section Section 4). Demographic questions concluded the survey.

We added two attention-check questions, which all participants answered correctly. Before launching the survey, we ran two focus groups and a pilot (see appendix Appendix B for more details). The survey included a measurement to record participants' resolvers' IP addresses to determine if they were using PDNS or not (see Appendix C for more details). Appendix D contains the whole survey protocol.

Participants. We calculated the number of survey participants using power analysis [24]. We included countries where more than 25 users were active in the last three months to calculate the total population. With a conservative estimate of 25% of the population proportion using PDNS and a 95% confidence level, 288 or more participants were required to answer the survey. Then we used a proportionate stratified sample of the same countries to collect our sample size. We collected data from 295 participants from 29 different countries. The participants' ages range from 18 to 66, with a mean age of 34. The stated genders of the respondents were 155 men, 135 women, and five who identified as another gender. 103 participants were located in America, 144 in Europe, 21 in Africa, 22 Asia, and 5 in Australia. The survey was only open to Prolific members who had approval rates of 90% or higher and had previously completed at least five studies.

Variables coding and ordinal logistic regression. All Fogg suggested variables namely motivation, ability, and trigger were included in an ordinal logistic regression model [25] (we performed two by two correlations, and the independent variables were not correlated). Stepwise, we extended the model to include additional variables – gender, age, and education – to produce a second, third, and fourth model respectively. In a final model, we added regions. We use the lowest Akaike information criterion (AIC) to choose the best model, considering that if an uninformative parameter does not explain enough variation, it should be removed [26]. We used as baseline the first model to compare the rest of the models. See Appendix I for a summary of the variables of the final model with the lowest AIC value (model 2). The model aimed to predict which of these variables predict participants' PDNS adoption. The ordinal Likert scale responses to 'How likely are you to subscribe to Protective DNS if it were available today?' (slightly modified for home users willing to pay for the service) was the model's dependent variable.

We performed a factor analysis on Likert scale items measuring perceived vulnerability, perceived severity, and users' concerns (See Appendix D, questions 6–12,24–26). All items loaded in their respective factor, so we computed their means for the regression model. The only continuous variable was perceived usefulness; the rest were categorical.

2.3 ISP customers interviews

We partnered with a Dutch ISP from February to August 2021. 292 malware-infected clients were offered free PDNS by the ISP. Registering and consenting for the ISP service took about 2 minutes on the ISP website. 284 consumers received the invitation since 8 had email delivery difficulties. Of the 284, 259 (91%) did not enable the service, and 25 (9%) activated it. After a month, consumers were asked to participate in a phone interview (See Appendix E for the complete interview protocol). They were contacted via their subscription email address. 24 (8%) of 284 consumers consented to interviews. No compensation was offered for participating.

Nine of the 24 participants (37.5%) activated the service and 15 (62.5%) did not. Only 5 customers identified as female, the rest as men. The participants' ages ranged from 24 to 60 years old. We asked about their current security measures, how severe they perceive the possibility of someone abusing their internet-connected devices, why they enabled or did not enable the service, and if they saw any drawbacks in using PDNS. The interviews were conducted in the participant's native language and recorded with their consent. The sessions lasted 10 minutes on average.

Two researchers independently coded the transcripts in Atlas.ti for thematic analysis [27]. The two coders utilized a sample of transcripts to generate initial codes for the themes. Informal discussions were used to ensure the reliability of findings as suggested by [28]. Over the course of twenty-three interviews saturation was reached (no new codes emerged from the interview). Five themes were found and they are presented in Section 4.3. The frequency of each topic among participants is shown in Appendix H along with code examples that helped group them into themes.

2.4 Enterprise interviews

Between April and July 2022, we conducted virtual meeting interviews with twelve professionals in charge of managing threats from malicious domains in enterprises. Except for one product manager, all were IT experts such as Chief Information Security Officers, security architects, and risk and IT security managers. The interviewees were not compensated for their time.

Via various social media accounts, we set out to recruit participants. Out of the total number of participants, 5 were employed by the government, 2 by banks, 2 by universities, 1 by a cable business, and 2 by Internet Service Providers (ISPs). One of the enterprises has its primary operation in America, one in Asia, and two have global operations; the rest were based in Europe. One of the ISPs serves 30,000 customers and the other 2 million The rest of the enterprises are in charge of managing somewhere between 200 and 40.000 endpoints.

The interview questions asked if the practitioners were aware of PDNS, the pros and cons of implementing this security solution in their enterprises, and the factors to consider in using it. If necessary, participants were provided a definition of PDNS. Appendix F contains the interview protocol.

For the interviews, English was the language of choice. The recordings lasted 43 minutes on average. Recordings were transcribed and anonymized, leaving out participants' names and affiliations. Two researchers independently coded the transcripts in Atlas.ti for thematic analysis [27]. The two coders utilized a sample of transcripts to generate initial codes for the themes. Informal discussions were used to ensure the reliability of findings as suggested by [28]. Over the course of seven interviews saturation was reached (no new codes emerged from the interviews). Five themes highlighted the key subjects discussed by enterprise participants, and they are presented in Section 4.4. The frequency of each topic among participants is shown in Appendix H.

2.5 Expert interviews

Nine DNS technology experts participated in semi-structured virtual meetings interviews (one interview was in person) over the period between March and May 2022. The interviewees were not compensated in any form. From the RIPE DNS working group's open mailing list, we collected the email address of 28 DNS specialists debating DNS4EU. Nine agreed to the interview. DNS experts were from a range of countries, including the European Union. They have a variety of DNS-related experience, including building open source DNS resolver software, working with country-code top-level domain registries and participating in the development of Request for Comments (RFCs) related to DNS. Five experts describe they had global experience in DNS and four at the European Union level.

The interview questions focused mostly on learning what the DNS technology experts describe as 'PDNS', their opinions on this security countermeasure, how PDNS differs from other security countermeasures, its benefits and drawbacks, and their thoughts on governments' initiatives (see Appendix G for the complete interview protocol).

For the interviews, English was the language of choice. The recordings lasted 51 minutes on average, and transcripts were anonymized. Two researchers independently coded the transcripts in Atlas.ti for thematic analysis [27]. The two coders utilized a sample of transcripts to generate initial codes for the themes. Informal discussions were used to ensure the reliability of findings as suggested by [28]. Over the course of six interviews saturation was reached (no new codes emerged from the interviews). Eight themes highlighted the key subjects experts discussed, as presented in Section 4.5. The frequency of topics among participants is shown in Appendix H, along with example codes for how they were grouped into themes.

3 Ethics

The protocol of this research was approved by the human research ethics committee of our institution (Reference number: 1920). Prolific participants provided their consent to participate in the survey. We informed them that we were collecting their IP addresses and their DNS provider (who responds to DNS queries). Participants were reminded that they could stop at any time. In exchange for the time spent completing the survey, we paid proportional to the participants' completion time using the equivalent to the minimum wage from where the authors are based. All interviewees in the three interview studies gave consent for the interviews and recording. They were reminded that they could stop the interview at any time. For the ISP customer interviews, customers' personal information never left the ISP's premises. In accordance with the terms of service and in agreement with the ISP's privacy team, we obtained an anonymized dataset for our data analysis.

APNIC collects users' DNS resolvers through advertisements. Users arriving at these websites have agreed to their

Table 1: DNS Resolvers Usage (Period: January to June 2022)

		Non Public DNS resolvers			Public DNS resolvers				
Region	**avg daily queries**	**% Same AS**	**% In country**	**% Out country**	**% PDNS**	**% Possible PDNS**	**% No PDNS**	**% No Info**	Total
Africa	1,671,192	58.2%	9.3%	1.2%	2.0%	2.0%	26.0%	1.3%	100%
Oceania	73,443	83.0%	5.3%	1.3%	1.0%	2.3%	7.0%	0.1%	100%
America	2,804,980	65.0%	9.2%	1.3%	0.9%	3.1%	20.2%	0.3%	100%
Europe	1,758,927	75.2%	7.6%	1.0%	0.9%	3.2%	12.0%	0.1%	100%
Asia	9,023,027	59.0%	20.0%	1.0%	0.8%	2.0%	17.0%	0.2%	100%

Note: **% Same AS:** Percentage of average daily queries which resolvers ARE in the same AS as the users and NOT known public DNS resolvers. **% In country:** Percentage of average daily queries which resolvers are NOT known public DNS resolvers and NOT in the same AS as the users, but ARE geolocated in the same country as the user. **% Out country:** Percentage of average daily queries in which resolvers are NOT known public DNS resolvers and NOT in the same AS as the users but, and NOT geolocated in the same country as the user. **% Public DNS resolvers:** percentage of average daily queries which are answered by resolvers as categorized in Appendix A.

terms and conditions, including the use of adverts. The APNIC data we obtained was anonymized and cannot be traced to individuals.

4 Findings

4.1 Protective DNS adoption

We analyze what percentage of average daily DNS queries is answered by different DNS resolvers. In Table 1, we split non-public and public DNS queries, and we present the regional distribution. PDNS resolver adoption is low in all regions compared to resolvers in the user's Autonomous System (AS), which are normally operated by their ISP. We note that Africa is the region that uses PDNS the most, with 2% of all queries answered by this type of resolver. Oceania follows with 1%, America and Europe with 0.9% each, and Asia last with 0.8%. In all regions, OpenDNS is the most popular PDNS resolver.

When looking at the country level, a small number of countries – with Israel (IL) in the lead – have more than 20% of the average daily requests answered by a PDNS resolver (see Appendix J). The APNIC data does, of course, not show who took the action to set up PDNS: the end users themselves or others, such as the network provider. This high adoption in some countries does underline the importance of comprehending end-user opinions about this service, since so many queries are already routed through them.

4.2 Prolific survey

Out of 295 participants, 13 were extremely unlikely to use the PDNS service presented to them, 34 were somewhat unlikely, 76 were neither likely nor unlikely, 120 were somewhat likely, and 52 were extremely likely to use the service. When the last two groups are added, the intention to adopt is 58%.

Participants' PDNS Awareness, first impression, and comparison to similar services. During the survey, participants were introduced to a 'Protective DNS service' (See appendix D) that safeguards their devices against untrustworthy websites and malicious software which uses DNS to perform this task; we balance this explanation with clarification that, for instance, the service cannot stop all threats.

Participants were asked if they had heard of a similar service to 'Protective DNS service' before filling out the rest of the survey. 102 (34,6%) participants said they had heard of similar services, 121 (41%) did not hear about it, and 72 (24,4%) participants were unsure.

Participants were asked to describe the service using adjectives from a list; they could add more. Examining the responses of the 121 participants who had never heard of a service like this, 71 of these participants said the service would be helpful; 66 said it would be useful; 52 said it would be secure; 21 said it would be easy to use; 24 said it was confusing. 7 out of 121 participants thought the service was unnecessary for them, while 2 thought it was unclear. The service was viewed as useless by 1 participant. Anxiety was one participant's first reaction to describing the service. Additionally, we looked at whether these participants perceive the PDNS service useful for the top security threats they face. Among the 121 participants that stated having never heard of a service like this, 59 (49%) considered the service very useful, and 27 (22%) participants considered it extremely useful.

We followed up with the 102 participants who had heard of similar services by asking if they were using a service similar to the 'Protective DNS service' described. Out of the 102 participants, 29 acknowledged using a comparable service. Therefore, we asked what the service's name was. Compared to the presented service, 11 out of 29 participants cited other public DNS resolvers. Four participants mentioned Cloudflare, two OpenDNS, one Adguard secure, one Comodo secure, one DNS filter, one Next DNS, and one mentioned a DNS filter for ads on their phone. Fourteen out of these 29 participants compared the service to other security countermeasures, such as antivirus, Internet browsers such as Chrome and Opera, cloud security providers like Sophos, and using Pihole. Remaining participants could not recall the name of the service they were using.

We further investigated the 11 participants who claimed to use public DNS resolvers against our DNS data. All participants' DNS resolvers were in broadband ISPs in the same AS as where the participants' IPs were located, except for one participant who mentioned using OpenDNS but was actually using Yandex. We did not gather DNS measurements for the two participants who mentioned using Cloudflare and one participant who mentioned using Comodo Secure. These could be possibly explained by different factors: two respondents used their phones (which may not use the PDNS service), and respondents may have taken the survey from a different network than where they set up PDNS. We also cannot rule out socially-desirable answers [29], but mentioning DNS providers implies respondents were aware of the service.

DNS measurement results. As described in Section 2.2, we included a measurement to capture the DNS resolvers of participants. We collected measurements from 285 of the 295 participants. Of those 285 participants, 208 (73%) had resolvers' IP addresses from broadband ISPs in the same AS as the participants' IPs. 28 (10%) participants had resolvers in a different AS than their IP address, but that AS belonged to the same ISP as the participants' AS. 22 (8%) participants had Google as DNS resolver. 19 (7%) participants out of the 285 were using a PDNS or possible PDNS resolver. Remaining participants used security vendors such as Akamai or Fortinet.

PDNS resolver users have never heard of or used a similar service, with one exception. This could mean another household member set up the service or that their network provider is re-routing DNS requests to PDNS resolvers. These findings highlight the need of measuring a phenomenon rather than depending merely on participant responses.

Who should provide PDNS? We checked all participants' responses about which provider they wanted for 'Protective DNS'. 156 (53%) participants chose their ISP, 100 (34%) a commercial provider, 24 (8%) their government, and 15 (5%) participants chose others (referring to non-profits and independent organizations that focused on privacy).

Internet Service Provider. We looked into why 156 participants chose their ISP to provide this service. 49 of 156 participants stated that ISPs were the most logical provider, as ISPs have the most understanding of current threats, can benefit from enhanced network security, and already provide their Internet connection. 37 out of these 156 participants mentioned trust. Twenty-three of 156 participants described that they have a contract with the ISP and that such a service can be bundled with it. 18 other participants who selected their ISP provided privacy-related justifications, with one remarking *'They can already access my internet history, so it would make no difference to my privacy'*.

Another group of 11 participants said they chose their ISPs due to their role in Internet connectivity. Eight participants were unsure or simply opposed to another option, so they did not consider a different party. Seven participants said the ISP's proximity and ease of communication made this party appealing. Three respondents mentioned PDNS's affordability if their ISPs implemented it.

Commercial company We looked into why 100 participants chose a commercial provider. 41 participants mentioned that they would trust a commercial company more than their ISP or government. A participant stated *'I don't trust the government. A commercial company will be more transparent in what it does than the government or my internet provider'*. Twenty-three of the 100 participants also expressed that commercial companies would have better know-how, better resources, and staff than their ISPs or governments to carry out this task. Another group of eight participants mentioned reasons related to the incentive of profit that commercial companies have, with this leading to better service, as highlighted by one participant, *'There is room for competition among companies, you have options to change if the service doesn't meet expectations or doesn't align with what you think is important when it comes to your data, privacy or safety online'*.

The remaining participant's reasons to choose a commercial included simply preferring a commercial company (6 participants), having a good experience dealing with a commercial company rather than their government or ISP (5), they handle personal data better (4), the service will be cost-efficient (3), no other choice was appealing (2), easier to switch (2), commercial companies care about their reputation, so the service will be good (2), and the rest of participants did not state a reason for their choice.

Government Only 24 participants chose the government as their preferred provider. Fourteen of these 24 participants stated that they trust their government. Four participants stated reasons related to the government not having any economic incentive to offer the service, so they would not use their data to make a profit. A participant stated *'I feel the others [ISPs and commercial companies] would focus on making money - [I] feel like the government wouldn't use it [PDNS] as profit-making scheme'*. Of the remaining participants, reasons were raised that the government should be responsible for protecting its citizens (2 participants); government has access to their data (so it would not matter to them if the government offers the service) (2), and; government would have more resources for providing PDNS (1).

Least preferred provider We questioned participants about which provider they would not choose for Protective DNS. One hundred and ninety-one (65%) would not choose their government, 51 (17%) would not choose a commercial company, 31 (11%) participants would not choose other parties (mainly companies they do not know or trust and with low reputation), and 20 (7%) would not choose their ISPs.

Participants provided different explanations of why the government was their least preferred provider. Ninety-six out of the 191 participants mentioned distrust. Another group of 34 participants, expressed privacy concerns. As mentioned by one participant *'It would be like Big Brother watching you'*. Nineteen participants expressed concerns about the ability of the government to deliver a quality, efficient or effective service. Fifteen participants mentioned that they would not choose the government because they might use this service for censorship. A participant said *'..No government should have full access to everything their citizens do online. I don't want to be in a bootleg China/North Korea/Russia'*. Other groups mentioned they could block websites for political or personal reasons. Some said this gives the government too much power.

Twelve participants said this was not the government's role. One participant stated *'Doesn't seem like it's something in their wheelhouse'*. Two participants said it would be hard to complain if the service went wrong since the government is hard to reach. The other participants did not explain their choice.

Explaining adoption. We used ordinal logistic regression to predict PDNS adoption. As mentioned in Section 2.2, we incorporated all Fogg's model variables and evaluated models with gender, age, education, and regions. These models have no significant variables, except for the one including gender. The model including gender as a control variable has a slightly lower AIC value (800.70) than the one with Foggs' factors only (800.85). Thus, we report that model (see Appendix K for a summary of the significant predictor variables).

Concern, perceived severity, self-installing security in devices, use of parental control, and PDNS awareness were not significant. To understand the significant model coefficients intuitively, we calculated the odds ratio [30].

As perceived vulnerability to malicious software and data theft increases ($\beta = 0.234, OR = 1.264, p < 0.1$), the odds of adopting Protective DNS increase 1.264 times. Fear, to use Fogg's terminology [22], could motivate adopting PDNS to avoid threats.

As the perceived usefulness of the service to address threats participants recognize as important to them increases, the likelihood of adopting a PDNS service increases by 2.539 times ($\beta = 0.932, OR = 2.539, p < 0.1$). This suggests that users who perceive value in PDNS are more likely to use it.

For participants who already have security measures (Antivirus, Firewall, Ad blockers) ($\beta = 0.774, OR = 2.167, p < 0.1$), the odds of adopting PDNS are 2.167 times higher than for those without any security measures.

For participants willing to pay for the PDNS service (β =-$0.545, OR = 0.567, p < 0.1$), the odds of adopting it are 0.567 times lower than for those who did not want to pay. This outcome was somewhat unexpected, so we looked at qualitative responses. One hundred twenty-two (41%) were willing to pay, whereas 173 (59%) were not. Out of 122 people willing to pay, 103 (85%) considered the service 'very useful' or 'extremely useful'. Why participants wanted to pay but indicated they did not want to use the service is puzzling. This could imply, as Fogg [22] suggests, that cost in itself can reduce the Ability to adopt a new behavior (even if it does not completely diminish the possibility of change in behavior).

For participants in the group who chose their ISP as the preferred provider ($\beta = 1.091, OR = 2.976, p < 0.1$) the odds of being more likely to adopt PDNS increased 2.976 times compared to participants who chose the government. For participants who chose a commercial company as the preferred provider ($\beta = 0.965, OR = 2.626, p < 0.1$) the odds of being more likely to adopt PDNS increased 2.626 times compared to participants who chose the government. Interestingly, the ISPs and commercial companies acting as 'facilitators' rather than the government had a bigger effect size to predict the likelihood of PDNS adoption.

The control variable gender was significant. Females were more likely to adopt PDNS than men. As our instrument was not meant to measure gender differences and this was a control variable [31], we refrain from strong claims.

Additional information to decide to opt-in to the service. Participants were asked what information would help them subscribe to PDNS. Privacy policies and data use were popular subjects. Another topic was the service's cost and effectiveness against intended threats. Participants also mentioned cancellation policies, expert reviews, reports on what the service protects, whether the service can be turned off, whether the service affects network speed or device operation, general terms and conditions of the service, customer reviews of the service, reputation and trustworthiness of the provider, how simple it is to use, and why the service is needed in addition to other security measures. Additionally, the time to set up the service may be significant to communicate to users, since 212 (71.9%) participants were willing to devote only one to twenty minutes to subscribe.

All in all, from the Prolific survey, we learned that the motivation elements for users to adopt the service were the perceived vulnerability and perceived usefulness of the service. From the ability construct, the cost was a significant factor. However, who is the provider of the service, the trigger/prompt [22, 23], plays the most important role.

4.3 ISP customers interviews

Unlike the Prolific survey, we interviewed 24 ISP customers who were offered PDNS and suffered a malware infection three months prior to the interview. Nine of the customers we interviewed adopted the service provided by the ISP, while 15 did not.

According to Foggs' concepts fear of something bad happening can act as a motivator to enact a behavior [22], in this case, the perceived vulnerability (malware infection) could motivate choosing the ISP PDNS. In the Prolific survey we observed that as perceived vulnerability to malicious software and data theft increased, the likelihood of adoption increased. In reality, this did not happen. Surprisingly, just 25 (9%) of 284 customers opt-in to the service. This may be because the survey measures intention, not actual behavior, benefits were not communicated clearly, or users did not want the service even after suffering a malware infection.

Concerns about the service. Twenty-one customers voiced concerns about the service. 16 customers worried about privacy or data use. *C15* expressed *'Naturally it [PDNS] might have some implications for your privacy. I think that if you want to be sufficiently protected that necessarily comes at some cost to your privacy. I think that is something you have to take for granted; it is something that is inevitably linked'*. Two consumers expressed concern over their lack of understanding of how the service operates. Two participants were concerned about the service's effectiveness and the ISP's responsiveness in the event of a problem.

Reasons for non-adoption. 15 customers declined to use the ISP PDNS for different reasons. One person opted to control his own security, and another did not need the service. Another participant said that he was using work-provided equipment, so he did not enable it. Since the service requires no installation on any device, the customer may not have understood how the service operates.

Four users stated that they already had other software installed, namely antivirus, that protected their machines. To illustrate *C19* said *'Well, I have an antivirus program on my laptop that then stops everything that comes in from viruses, I think that is enough actually'*.

Three participants reported that they tried to follow the instructions but were unsuccessful in turning on the service. Additional justifications from two customers were that they didn't understand how the service operated.

A customer mentioned the possibility that the service may prevent accessing something he needed. Another client expressed that he did not enable it because the service could be billed later, and one customer forgot to activate the service.

Reasons for adoption. The nine consumers who enabled the service also provided a range of justifications for doing so. According to two customers, they enabled the service on their ISP's recommendation. One of these participants also expressed his fear of viruses. One customer stated that he considers the service useful as long as there is no payment involved. Another customer said that he thought an ISP could adopt security measures more quickly than an individual customer could.

One customer, *C1* said that he enabled the service because *'[it] automatically protects all devices that are connected to your router, that saves a lot of hassle'*. Three customers stated that they enabled it for a 'feeling of safety'. One client claimed that he enable the service to prevent malware from spreading.

Beliefs on abuse. Fifteen of 24 customers discussed various consequences of the misuse of their devices. Given that all participants have suffered a malware infection prior to the interview, it seems that not all customers perceived it as a major event. Five out of these 15 customers enable the service. Two customers worry about data theft. One user claimed that his devices could spread malware, another said identity fraud could occur, and another said his network could be made accessible to the public.

Ten consumers who chose not to use the service still thought that device misuse would have consequences. Data theft was cited as the primary impact by six consumers. The remaining customers mentioned phishing, viruses, and the rise of hacking as consequences. Even though they believe malicious software is dangerous, they did not activate the service. The ISP sent a message inviting them to use the service for free but failed. The 'spark' [22] for motivating behavior may not have resonated with all of the customers.

Trust. Trust was also a topic mentioned by 11 customers. Six users that enabled the service trusted their ISP to do this job. Three individuals who did not enable the service expressed trust in the ISP, but they were the ones that tried to enable the service but failed. One participant believed that the ISP was a reputable party, but still chose not to enable the service since they had other measures in place. Conversely, one participant expressed distrust in the ISP.

Apart from 'perceived vulnerability' (which some customers cited as a reason to adopt the service and this study demonstrates that a smaller proportion of participants actually adopts the free ISP PDNS service), and 'use of other security countermeasures' (which actually lead participants to not adopt the service and perhaps think the service was not useful), these results support the findings of our survey.

Customers adopted the ISP PDNS because their ISP offered it, showing how important the trigger was. The service's perceived usefulness also drove adoption. On the other hand, participants who did not use the service did not consider it useful for their circumstances (e.g. I have a device that is managed by my employer). Also, fear of future costs was listed as a reason for not opting in. Participants' concerns correspond with the survey, being privacy a predominant topic. According to the instructions, some participants attempted to enable the service, but they were unsuccessful. Hence, there is space for improvement since as Fogg [22] suggests, effort and time spent can influence the Ability to conduct a behavior.

4.4 Enterprise interviews

We interviewed twelve professionals, as described in Section 2.4. Two practitioners acknowledged that their organizations made use of a PDNS resolver. In addition, *P9* admitted that his organization had used a PDNS resolver, but no longer does because of the cost.

Two participants stated that their organizations run their own DNS resolvers and that they were filtering domain names at that level. One mentioned filtering Domain Generation Algorithms and the other a list of malicious domains. This shows that some enterprises can deploy PDNS internally, and they also mentioned that would not use an external provider.

Two practitioners were unaware of PDNS , while the other participants knew about PDNS but did not use them for a variety of reasons. *P4* stated that their organization values do not align with this measure, *P6* said cost was an issue, and *P7* mentioned that they consider that DNS filtering is not always a viable security countermeasure. The two participants who work for Internet Service Providers were implementing services that offer DNS protection as an opt-in service.

Reasons to implement PDNS. The two participants who confirmed utilizing PDNS, mentioned the global threat intelligence as justification. The service gathers data from many businesses around the world, offers visibility on attacks, and prevents them.

P8 said that as no security solution is perfect, they added this extra layer of security. *P10* said that they chose PDNS service because it was straightforward to implement globally and because safeguarding their reputation was vital *'We have a big name provider that it is in charge of filtering our DNS queries outside the organization. We use it because of the capability of the provider to deliver the service around the world since we have a lot of countries… it is not only cost.. for all organizations cost is important... Also, our reputation is important, so we take all the security measures that are possible'*. Also, *P9* indicated that their organization used PDNS in the past due to the value of global threat intelligence.

There were two organizations that added filtering to their own DNS resolvers, *P5* and *P1* cited having an in-depth defense strategy as the primary justification. P1 stated, *'we do filtering because of an in-depth strategy of protecting different layers... I think our organization and my colleagues tend to gravitate to just blocking stuffs'*. *P1*, however, claimed that the blocking that is now occurring in their resolver was out of date and was done with a static list.

P11 described that the main reason for offering this service to its ISP customers was that they believed that security was important. *P12*, on the other hand, said that the ISP implemented PDNS because its government mandated to block Child Sexual Abuse Material (CSAM) and they had to comply quickly. Since the solution was already in place, they saw the opportunity to offer businesses other types of blocking.

Factors to consider for adoption. We questioned participants who weren't currently utilizing PDNS about what they would consider before implementing the service. Many factors were mentioned.

P9, claimed that cost and service efficacy were the two most important factors to take into account. He said that the fact that they ceased using the service was due to their inability to afford this security countermeasure. Two other participants , also identified cost as the primary determinant. *P6* said they depend on public funding to invest in their security infrastructure. The same participant noted the need to examine this solution relative to their existing infrastructure.

P2 said that to evaluate the service's added value, they must consider its effectiveness. *P7*, on the other hand, who thinks DNS blocking might not always be a viable security countermeasure, said efficiency was the most crucial consideration. *P3* mentioned they would consider the organization's threat model and red teaming advice.

P4 stated that organization's values must be considered. When openness and transparency are desired, it may not be good to restrict domain names for the staff. Although not questioned, *P11* mentioned that the main consideration in adopting PDNS for the ISP where he works was consent. They had to consider all legal factors and build a way to obtain customers' consent to provide the service.

Concerns. Participants from adopters and non-adopters organizations raised different concerns, thus we separated them from adoption factors (See Section 2.4).

Five participants expressed concern about false positives. However, none of the participants who were using a third-party PDNS said that a false positive had caused a disruption in their daily operations. P10 stated, *'We experience it [false positives], but no frequently, but there were some hits. They have mechanisms to report it and the provider has excellent SLAs and we have ways where we can just make changes'*.

Additionally, *P3*, expressed concern about the time they would need to spend troubleshooting false positives. The trust a company places in a third party to manipulate the DNS responses was also brought up by *P5*. The service's transparency on what is being blocked was the main concern of *P6*. *P1* also stated that privacy was an issue since they are a privacy-conscious organization. *'When talking about blocklisting there are some concerns… because we have a lot of employees and all their traffic is passing within our network… even when they are working at home…. As there is security consciousness, there is also very much a privacy consciousness on the end of our users…'*.

Because DNS blocking may not be successful in all circumstances, *P7* expressed that his main worry would be that the organization would experience a false sense of security.

P11 was concerned that the service only protected devices linked to the ISP's router. If customers' phones are connected to a separate provider, they may get infected and customers might doubt the service. Second, the participant noted customers may not know the added value of the service because it does not provide reports of what is being blocked.

Government PDNS. Participants were asked if they would adopt a government PDNS. According to *P8* and *P10*, commercial PDNS services are global, while government initiatives are country or region-specific. For instance, DNS4EU will cover Europe. Commercial PDNS solutions provide them with improved threat coverage as a result. Both participants said their organizations would use PDNS if required by the government, as they comply with other regulations.

P1 and *P5* indicated that it would be preferable if the government shared block lists that businesses could use on their own. P1 highlighted *'If it would be a list that I could implement myself, then I would be interested … because then you can just also weed out filters that you may find too intrusive … and [have] more control of the actual blocking taking place'*. *P9*, whose organization discontinued using a PDNS resolver for financial reasons, believed that these initiatives are a good concept and that they would explore adopting them. Both *P3* and *P6* agreed with *P9* that these projects are beneficial, and *P6* added that they are beneficial as long as organizations are free to set them up any way they see fit.

It comes down to who consumers trust, according to *P11*, and personally, he would put more faith in his ISP than government PDNS initiatives. *P12*, on the other hand, stated that he had contradictory opinions; on one hand, he dislikes government PDNS initiatives, yet the more security the better.

The majority of enterprise participants stated that their organizations employ PDNS because of the additional layer of security and global threat intelligence it provides. In addition, several other considerations for PDNS adoption were brought up, including PDNS efficiency, the organization's threat model, the organization's values, and cost. Consistent with the Prolific survey, these mentioned factors suggest that some sort of perceived usefulness depending on the characteristics of the organization as well as perceived vulnerability (threat model) might play an important role in PDNS adoption for enterprises. The Prolific survey results demonstrated that the cost reduced the likelihood of PDNS adoption (as with the Fogg model [22]). We have evidence of one enterprise stopping using PDNS due to the inability to pay for it. Across our studies, this indicates that the cost of the service is a concern for individuals and enterprise customers alike. Some of the enterprise participants' concerns were transparency and privacy even though they might be adopting PDNS on behalf of their users. These concerns overlap with the concerns expressed by ISP customers. Trust in the provider was also mentioned by one enterprise's participant as an important factor. This topic was discussed by ISP customers as well as it stood out in the survey as one of the reasons to decide to opt for a certain provider of the service.

4.5 Experts interviews

Factors for adoption. For users to adopt PDNS, *E1, E2, E3, E4* and *E7* emphasized the importance of awareness. One expert said DNS is beyond the understanding 'common Internet users'. *E4* said that users usually stick with the default DNS settings offered to them, and it is hard to educate them on changing those settings, Thus, how easy it is to set up a PDNS resolver may affect its adoption. As part of awareness, experts described that it is critical that users grasp PDNS policies, what they are signing up for, and what is blocked, what they are protected against, and how their data is used. E2 highlighted *They [users] should check who is providing it [PDNS]... will be an entity they trust?... if there is filtering what are the policies to turn it on and off... in general what users do is just to buy security ... someone is selling a security tool, they turn it on, and then they forget about this... so this is, unfortunately, the average degree of awareness'.*

Most enterprises prohibit access to particular internet resources using next-generation firewalls or proxy servers, according to *E1,E2, E4* and *E6*. *E4, E6* and *E9* emphasized that the organization's size, security strategy, or network requirements may drive the adoption of PDNS. *'The level of filtering that can take place in DNS and especially in enterprise environments...well depends on the jurisdiction, will depend on the nature and strategy of the organization, size of the organization, will depend on the way that they're patronizing their employees or trusting them ... '* E4 said. *E1, E7, E9* mentioned it is vital to know where an organization's DNS data goes when employing third-party resolvers. Service level agreements, according to two experts , are crucial because the functioning of the organization will depend on an outside party. *E5* suggested that enterprises should consider performance, ease of deployment, and maintenance when implementing a PDNS service.

The key issue raised by experts in regard to ISPs is their lack of incentives as they have nothing to gain from DNS blocking. ISPs may have DNS systems that enable PDNS, however, filtering in resolvers brings maintenance costs and no revenue. *E3* suggested ISPs might adopt DNS filtering to offer to their customers if they could generate money by protecting users from DNS abuse.

According to five experts the main reason why governments should provide PDNS services to society is that doing so is in the public interest and for the benefit of society. *E7* noted that some governments are interested in supplying PDNS, citing the DNS4EU initiative, as an attempt to dispel the notion that important infrastructure like DNS is run by unrelated commercial organizations with distinct objectives, and not adhering to the same European Union regulations.

Provider. PDNS is offered by numerous commercial public DNS resolvers. The majority of experts, however, concurred that the government should play some role. As it is in the public interest to prevent DNS misuse, the government is the appropriate party to provide DNS alternatives. They do not have a corporate reason to protect DNS requests above the interests of society. However, *E6* questioned if the government could compete with private companies. *E2,E3* suggested that ISPs should provide PDNS because most customers' Internet connections go through them. According to *E1*, any private organization can provide it. *E9* recommended a federated effort, so no single entity would control DNS queries.

Limitations of PDNS. Six experts agree that PDNS's main drawback is that it is not a perfect solution and 'will not catch it all'. E1 stated, *'If you were to rely solely on DNS base security solution, you are going to run into problems because not everything will rely on DNS lookups in order to get the payload in, and if you will assume that you are protected, then you are not'*. Due to the dynamic nature of DNS, where attackers may use domain names briefly before a PDNS provider loses sight of them, the solution's success will depend on how accurate the threat intelligence is, according to *E6*. Experts also warned against using PDNS as their single security measure.

Another drawback of PDNS, according to *E1*, is false positives. *E7* stated that users could get around using standard methods like virtual private networks.

Types of blocking. Despite the limitations of PDNS services, preventing abuse was mentioned by five experts. Most experts agreed that restricting domains for security is an unambiguous strategy. However, *E1, E4* raised that a resolver could block categories based on keywords that could lead to blocking benign content. *E1* mentioned, *'The EU Commission decided to force the .eu registry to use a list of keywords,* *and any domain name that contains those keywords has to be sent for extra examination, the list of keywords include words like virus, corona, covid, covid-19, vaccination, vax, anti-vax, there was a whole list, so perfectly innocent websites saying let's say: help covid-19 victims or whatever... completely innocuous, would have been blocked, so it is crazy'*.

E5 noted that legal grounds filtering should be included as a category because it essentially involves listening to court orders. Contrarily, *E8* emphasizes that depending on where their business is headquartered, some resolvers may simply choose not to abide by court rulings. Intellectual property filtering was highlighted as contentious by three experts because it can be avoided in any case, just like legal filtering. While *E4* recommended using several lists to filter domains to check for overlap and avoid mistakes.

PDNS vs other security measures. Four experts described the main difference between PDNS and other countermeasures as that with DNS is possible to block the source of the problem and once the DNS path is broken DNS abuse will be stopped. For instance, one of these experts claimed that while DNS cannot be bypassed, encrypted network traffic can totally flow through firewalls. *E6* added that with this countermeasure is possible to detect patterns of malicious queries without any indicator of compromise. For instance, a system or user device may be investigated if it increases DNS requests to a domain, even if it's not immediately evident that this is harmful. *E4* added that PDNS is a protection mechanism for passive users who want protection.

Two experts, mentioned that PDNS is a solution easy to deploy and that can protect any device connected to a network without installing anything in each particular device, even if a device does not have any other tool to protect itself, for instance, Internet of Things devices. *'Homes are filled with IoT stuffs, they are WIFI connected, there are heating controllers, in these devices, there is no way you can install an antivirus or to do checks. They have limited hardware. It is important to look at this at the network level and Internet connection, if you install it [PDNS] there, then it works for any possible device that you connect to your network. This is why the filtering is very different than many other applications'*, E2 mentioned.

E8 compared PDNS with the browser, highlighting that it's unusual for DNS to prevent something the browser didn't. However, for devices that do not use the browser, such as the Internet of Things, this might be the only solution available. *E8* also mentioned that this is the cheapest solution to deploy.

Privacy. Seven experts talked about how a system like PDNS can affect privacy. According to *E1*, *E2*, and *E5* the General Data Protection Regulation (GDPR) may apply to these services if they operate under European Union (EU) privacy rules. Other services outside the EU are exempt. *E1* said that DNS information might potentially be sold for marketing purposes *'In the EU, you got GDPR, so you got some level of protection if actually, companies are complying, but theoretically it should not be a problem, it should be a non-issue, I don't know if in practice or not, but in theory. Outside the EU, good luck! There are services that are offered in the West, if you are in marketing, there are places where you can buy DNS data'*. Two experts, noted that there is a privacy issue because some public resolvers are even open about sharing DNS information with outside parties. *E3* pointed out that while DNS protection is hard to monetize, providers may turn to data collection as a revenue stream. Another expert (*E8*) stated that even device vendors redirect DNS traffic to them in order to 'guard users' privacy', which really means that they have access to the data.

Transparency. Given the implications that PDNS services have regarding privacy and blocking content, transparency was a topic that experts brought up. Six experts discussed the need for some level of disclosure. *'There must be an understanding of what you are blocking and why you are blocking'* E1 said.

Centralization. Six experts agreed DNS centralization is a problem. Many users relying on one resolver create single points of failure. E4 stated "*'I think it [DNS centralization] is creating single points of failure, for me both in professional and personal perspective is a significant reason not to do it ...than the ideological reasons that you will have people arguing on both sides ... '*. *E4* also said customers need a variety of options. According to *E3* if ISPs provided PDNS to their clients, centralization might be avoided while yet reaping the benefits. *E8* stated that there are no security observations that can be made if all DNS traffic goes to the same party.

Overall, experts emphasized that users must have a thorough understanding of PDNS policies, including what is blocked, how their data is handled, and what they are safeguarded against. Users, ISP customers, enterprises, and experts appear to agree that privacy and transparency must be taken into account in PDNS adoption. Experts suggest that enterprises should think about PDNS performance, the size of the enterprise, the organization's strategy, and network requirements. This implies that some perceived usefulness is important and can vary depending on the type of enterprise. This is consistent with the views of enterprises' participants. Participants in all our previous studies mentioned trust in the provider as critical, and some experts agree.

5 Discussion

Our four human subjects studies show how diverse factors can hinder or encourage PDNS adoption. Even though some participants in the ISP interviews said they had extra security measures and did not find PDNS useful, those who used their ISP's PDNS found it useful. This correlates with the survey results, which show that as the perceived usefulness of the service to handle the most important threats for participants increases, so does its adoption. Consistent with [18], secure tools must be useful to be accepted. Also, the trigger – who provides the service – played an important role. Experts emphasized the importance of user awareness. If users are not aware of the conditions of the service and how different it is from other security countermeasures, it is likely that they cannot perceive its utility.

Enterprises' PDNS adoption motivations vary. Enterprises that adopted PDNS did so because of global threat intelligence or an in-depth defense strategy. ISPs offering PDNS to their customers believed security was important and monetize the service after complying with government regulations. Costs and time to handle false positives were elements of simplicity [22] mentioned by participants. To consider adoption other factors such as organizational values, service effectiveness, and how PDNS complements its current infrastructure were mentioned by enterprises' participants. Experts concurred with all these factors adding that knowing where the data of the enterprise is going is important to consider. Some experts also shared the same opinions as users about PDNS providers, including ISPs as potential providers, although highlighting the lack of incentives for this actor to offer PDNS.

5.1 Intention vs behavior

According to [32], there is a chasm between intention and behavior, and we observe discrepancies between the Prolific survey and ISP customer interviews. Perceived vulnerability and data being stolen made PDNS adoption more likely for the survey participants. Yet only 9% of ISP customers opted in for the ISP PDNS, even though they had suffered a malware infection three months prior to the interview. A possible explanation is that the ISP's message lacked the 'spark' that would have motivated customers to adopt the service. Trigger moments at the correct time can encourage behavior [33], and interventions that encourage progress monitoring may be more successful [32]. However, the ISP did not follow up with a reminder to customers to enable the service.

The Prolific survey found that users who had additional countermeasures in place, namely antivirus, firewall, and ad blockers were more likely to adopt PDNS. However, using these security countermeasures was cited by 27% of ISP customers who did not sign up for the ISP PDNS. We explained how DNS worked, so survey participants may have understood that this was a different countermeasure. In the ISP customer interviews, consumers may not have understood the main value of PDNS because the ISP did not distinguish it from other solutions. Seeing PDNS as a different security countermeasure may have influenced the decision to adopt the service [34].

5.2 Pros and Cons of PDNS by default

Like every other technology, PDNS offers both benefits and drawbacks, necessitating moral reflection on their use [35]. A PDNS service can detect threats which individual users may never be aware of. This advantage was recognized by some of the survey respondents which stated that ISP as the provider would have the most understanding of current threats, (49 participants), though a few of the ISP interviewees did not immediately recognize this distinction. By enabling PDNS by default users won't have to worry about protecting their devices from dangers that are, for the most part, invisible to them. Our results indicate that defaulting to PDNS may be welcomed by users who perceive it as protecting them, safeguarding their privacy, and being effective in achieving these goals.

However, defaulting users to PDNS might have drawbacks. Privacy issues may arise in jurisdictions without privacy-preserving regulations when inspecting DNS queries. Participants in different studies expressed privacy concerns, and experts highlighted that DNS data may be used by some PDNS providers for commercial purposes. Thus, forcing this countermeasure might not please privacy-conscious users.

Only 9% of the invited ISP customers opted in for PDNS even after a malware infection. Some users preferred to manage their own security or did not consider PDNS effective for their circumstances. Dodier et al. [36] show how ignoring users' priorities and values can result in users circumventing security measures or refusing to implement them. Hence, enforcing PDNS might be counterproductive for these types of users since they might adopt riskier behaviors to trespass DNS blocking or users may adopt self-censoring behaviors [34].

Our findings suggest that enterprises may oppose DNS blocking if they are forced to employ it by default. Although the organization representatives spoke variously of advantages, many disadvantages were also cited; deploying PDNS would not necessarily negate those concerns.

5.3 Government initiatives

Only 8% of the survey participants had a favorable opinion of the government as PDNS provider, while 53% participants preferred their ISP, follow by 34% preferring a commercial company. When asked which provider they would not choose, 65% said the government. These findings suggest PDNS initiatives may be misguided. Our findings suggest that if governments want to stimulate PDNS use, they need to provide users with different alternatives. Users prefer ISPs as providers, so government resources can be directed to involve this actor.

Cost is one of the factors that organizations and survey participants seem to consider for adoption. Government initiatives that are free can be an advantage over commercial providers. Organizations that adopted commercial providers highlighted the importance of global threat intelligence, a capability that local governments might not be able to offer. Service level agreements, efficiency, and effectiveness of the service are among the factors organizations consider for adoption. To match commercial providers, government initiatives may have to compete.

These findings also imply that before proposing user-facing security technologies, user needs and adoption factors should be assessed. Also, determining who users prefer as the intervention's 'facilitator' to adopt a security behavior is crucial.

This can determine the success or failure of the behavior.

5.4 Recommendations

From our analysis and results, we propose the following recommendations.

Increase PDNS visibility for users. Our findings demonstrate that 71 out of the 121 participants who had never heard of PDNS describe the service as useful. So, users who need the service may not know it exists. Positioning solutions to be easily found by those who can use them is then a challenge. In addition, those providing the services should communicate the benefits and differences of PDNS to end users, distinct from other security measures.

Subsidizing ISPs. Few users and enterprises want their government PDNS. Governments could support ISPs in offering PDNS as our participants mostly saw the ISP as best-placed and prepared to manage such a solution. Subsidizing ISP DNS software and staff is one option. In this way, the PDNS alternative can be available to their customers. A remaining challenge that is pointed out in Section 5.5 is to investigate ISPs' incentives to actually offer PDNS.

Blocklist sharing. Sharing blocklists with PDNS resolvers as other existing abuse data is shared (e.g. as Shadowserver does [37]) might be an alternative for governments. Enterprises can subscribe to receive these blocklists and implement them in the way they see fit. Two enterprises deployed their own in-house PDNS and supported this. This can provide another approach to deploying PDNS, while complementing options for paid-for commercial threat intelligence.

5.5 Limitations and Future Work

We calculated PDNS penetration using the 'first use' resolver from APNIC data. Thus, our results are a lower-bound estimate of PDNS penetration since we do not include 'all resolvers' that may view users' DNS requests.

Instead of a random sample of the general population, we recruited survey respondents using Prolific. Tang et al [38] suggest that Prolific data is representative of user views and experiences. We recruited participants from different regions, so views are not localized.

We interviewed participants who work in 12 enterprises in government, banking, university, cable industry, and ISPs. We found recurring themes that drove or hindered PDNS adoption. Why an organization adopts PDNS might vary, but more organizations' viewpoints do not invalidate our findings.

This work focuses on public DNS resolvers advertising themselves as PDNS and particularly protecting against botnets, malware, phishing, and spam; other categories like adult content were not considered.

Further research may determine whether ISPs are using PDNS without offering it as a service. Which incentives ISPs have to offer PDNS is also worth exploring as well as privacy trade-offs users might be willing to make. Gender was a control variable in our survey instrument, so more research may need to confirm gender differences in PDNS adoption. We did not find differences in PDNS adoption across regions; however, certain regions in our sample fell below 30 observations, so further research may corroborate these findings.

6 Related Work

Nisenof et al. [15, 16] study users' preference settings of encrypted DNS. They found DNS provider knowledge and trust are related. We found various reasons why participants choose a PDNS provider at the DNS resolver level. ISPs were the favored choice not only because of familiarity or trust, but also because of privacy reasons and participants thought that they were the logical party to do it. Besides participants' distrust in their governments, they also describe other reasons such as lack of capability.

In a case study with Telenor Denmark, Fejrsko et al. [39] found that third-party resolvers might be used to overcome censorship. In our survey, participants were inclined to adopt the service when their perceived vulnerability to malware or data theft increased, provided they already had other defenses in place, perceived utility of the service, based on who is the provider, and cost. Also, [39] estimates DNS traffic towards resolvers that offer malware filtering or parental control for Telenor Denmark, while our work uses a global secondary dataset to determine usage of PDNS resolvers that prevent botnets, malware, pharming, phishing, and spam.

7 Conclusion

Using APNIC dataset, we found that commercial PDNS resolvers are marginally used in different regions with Africa having the highest adoption rate at 2%. Nonetheless, some countries, with Israel on the lead, have a high rate of adoption. Four human studies identified PDNS adoption factors for users and organizations. Perceived vulnerability, perceived usefulness, and cost played an important role in users' adoption. Enterprises used PDNS for global threat intelligence, layered security, believing security was important, and compliance with government regulations. Also, our findings demonstrate the need of considering user preferences for intervention facilitators when recommending user-facing security solutions like PDNS.

Acknowledgments

We thank our anonymous reviewers. We thank Geoff Huston for granting us access to APNIC dataset. We thank Maaike van Kesteren's interview transcription assistance. We thank Ralph van Gurp for the data collection of the ISP interviews. This publication is part of the MINIONS project (grant no. 628.001.033) of the "Joint U.S.-Netherlands Cyber Security Research Programme" which is (partly) financed by the Dutch Research Council (NWO); and the "Hestia Research Programme" (grant no. VidW.1154.19.011).

References

[1] D. Yang, Z. Li, H. Jiang, G. Tyson, H. Li, G. Xie, and Y. Zeng, “A deep dive into dns behavior and query failures,” *Computer Networks*, vol. 214, p. 109131, 2022.

[2] R. Radu and M. Hausding, “Consolidation in the dns resolver market–how much, how fast, how dangerous?” *Journal of Cyber Policy*, vol. 5, no. 1, pp. 46–64, 2020.

[3] Google, “Official Google Blog: Introducing Google Public DNS,” dec 2009. [Online]. Available: https://googleblog.blogspot.com/2009/12/introducing-google-public-dns.html

[4] European Commission and the High Representatitve of the Union for Foreign Affairs and Security Policy, “Study on Domain Name System (DNS) abuse - Publications Office of the EU,” 2022. [Online]. Available: https://op.europa.eu/en/publication-detail/-/publication/7d16c267-7f1f-11ec-8c40-01aa75ed71a1/language-en/

[5] Cisco, “Home Internet Security | OpenDNS,” 2022. [Online]. Available: https://www.opendns.com/home-internet-security/

[6] “Quad9 | A public and free DNS service for a better security and privacy.” [Online]. Available: https://www.quad9.net/

[7] Cloudflare, “Introducing 1.1.1.1 for Families,” 2020. [Online]. Available: https://blog.cloudflare.com/introducing-1-1-1-1-for-families/

[8] Yandex, “Yandex DNS,” 2022. [Online]. Available: https://dns.yandex.com/

[9] National Security Agency, “Selecting a Protective DNS Service Why Protective DNS? How does it work?” Tech. Rep., 2021.

[10] National Cybersecurity Centre, “Protective Domain Name Service (PDNS) - NCSC.GOV.UK,” 2020. [Online]. Available: https://www.ncsc.gov.uk/information/pdns

[11] CIRA Canadian Shield, “CIRA Canadian Shield | Free public DNS for Canadians | CIRA.” [Online]. Available: https://www.cira.ca/cybersecurity-services/canadian-shield

[12] E. commission, “Funding & tenders,” 2022. [Online]. Available: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/cef-dig-2021-cloud-dns-works

[13] Whalebone, “Press Release: DNS4EU | Whalebone,” 2022. [Online]. Available: https://www.whalebone.io/post/press-release-dns4eu

[14] N. Tupas, “ACSC launches new cyber guard for government data - Defence Connect,” 2021. [Online]. Available: https://www.defenceconnect.com.au/intel-cyber/8911-acsc-launches-new-cyber-guard-for-government/-data

[15] A. Nisenoff, N. Feamster, M. A. Hoofnagle, and S. Zink, “User expectations and understanding of encrypted dns settings,” in *Proc. NDSS DNS Privacy Workshop, Virtual Event*, 2021.

[16] A. Nisenoff, R. Sharma, and N. Feamster, “Understanding user awareness and behaviors concerning encrypted dns settings,” *arXiv preprint arXiv:2208.04991*, 2022.

[17] G. Huston, “Recursive resolvers,” 2022. [Online]. Available: https://stats.labs.apnic.net/rvrcsv/

[18] R. Abu-Salma, M. A. Sasse, J. Bonneau, A. Danilova, A. Naiakshina, and M. Smith, “Obstacles to the adoption of secure communication tools,” in *2017 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2017, pp. 137–153.

[19] Prolific, “Prolific · Quickly find research participants you can trust.” 2022. [Online]. Available: https://www.prolific.co/

[20] G. Huston, “Measuring the End User,” 2016. [Online]. Available: https://labs.apnic.net/presentations/store/2016-02-10-ad-measurement.pdf

[21] M. George, “Measuring the Internet for fun and profit,” 2012. [Online]. Available: https://labs.apnic.net/?p=83

[22] B. J. Fogg, “A behavior model for persuasive design,” in *Proceedings of the 4th international Conference on Persuasive Technology*, 2009, pp. 1–7.

[23] ——, *Tiny habits: The small changes that change everything*. Eamon Dolan Books, 2019.

[24] K. Fitzner and E. Heckinger, “Sample size calculation and power analysis: a quick review,” *The Diabetes Educator*, vol. 36, no. 5, pp. 701–707, 2010.

[25] D. G. Kleinbaum, K. Dietz, M. Gail, M. Klein, and M. Klein, *Logistic regression*. Springer, 2002.

[26] T. W. Arnold, “Uninformative parameters and model selection using akaike’s information criterion,” *The Journal of Wildlife Management*, vol. 74, no. 6, pp. 1175–1178, 2010.

[27] V. Braun and V. Clarke, “Using thematic analysis in psychology,” *Qualitative research in psychology*, vol. 3, no. 2, pp. 77–101, 2006.

[28] ——, “One size fits all? what counts as quality practice in (reflexive) thematic analysis?” *Qualitative research in psychology*, vol. 18, no. 3, pp. 328–352, 2021.

[29] J.-B. E. Steenkamp, M. G. De Jong, and H. Baumgartner, “Socially desirable response tendencies in survey research,” *Journal of Marketing Research*, vol. 47, no. 2, pp. 199–214, 2010.

[30] M. Szumilas, “Explaining odds ratios,” *Journal of the Canadian Academy of Child and Adolescent Psychiatry*, vol. 19, no. 3, pp. 227–229, aug 2010. [Online]. Available: http://www.csm-oxford.org.uk/

[31] P. Hünermund and B. Louw, “On the nuisance of control variables in regression analysis,” *arXiv preprint arXiv:2005.10314*, 2020.

[32] P. Sheeran and T. L. Webb, “The intention–behavior gap,” *Social and personality psychology compass*, vol. 10, no. 9, pp. 503–518, 2016.

[33] S. Parkin, E. M. Redmiles, L. Coventry, and M. A. Sasse, “Security when it is welcome: Exploring device purchase as an opportune moment for security behavior change,” in *Proceedings of the Workshop on Usable Security and Privacy (USEC’19)*. Internet Society, 2019.

[34] P. Briggs, D. Jeske, and L. Coventry, “Behavior Change Interventions for Cybersecurity,” in *Behavior Change Research and Theory: Psychological and Technological Perspectives*. Elsevier Inc., jan 2017, pp. 115–136.

[35] S. Roeser, “Nuclear energy, risk, and emotions,” *Philosophy & Technology*, vol. 24, pp. 197–201, 2011.

[36] S. Dodier-Lazaro, R. Abu-Salma, I. Becker, and M. A. Sasse, “From paternalistic to user-centred security: Putting users first with value-sensitive design,” in *CHI 2017 Workshop on Values in Computing*. Values In Computing., 2017.

[37] Shadowserver, “The Shadowserver Foundation,” 2022. [Online]. Available: https://www.shadowserver.org/

[38] J. Tang, E. Birrell, and A. Lerner, “Replication: How well do my results generalize now? the external validity of online privacy and security surveys,” in *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, 2022, pp. 367–385.

[39] M. Fejrskov, E. Vasilomanolakis, and J. M. Pedersen, “A study on the use of 3rd party dns resolvers for malware filtering or censorship circumvention,” in *IFIP International Conference on ICT Systems Security and Privacy Protection*. Springer, 2022, pp. 109–125.

[40] H. Asghari and A. Noroozian, “GitHub - hadiasghari/pyasn: Python IP address to Autonomous System Number lookup module. (Supports fast local lookups, and historical lookups using archived BGP dumps.),” 2022. [Online]. Available: https://github.com/hadiasghari/pyasn

A Public DNS resolvers classification

Table 2: Public DNS resolvers classification

Classification	Public DNS resolver name	IP addresses
Protective DNS (PDNS)	114 DNS	114.114.115.115
	AliDNS	223.6.6.6
	Alternate DNS	198.101.242.72
	Baidu DNS	180.76.76.76
	CleanBrowsing	185.228.168.9
	Comodo Secure DNS	8.26.56.26
	DNS PAI	101.226.4.6
	DNSPod	119.29.29.29
	Green Team DNS	81.218.119.11
	Neustar	156.154.70.1
	One DNS	117.50.10.10
	OpenDNS	208.67.222.222
	SafeDNS	195.46.39.39
Possible Protective DNS	Cloudflare	1.1.1.1, No Malware: 1.1.1.2 No Malware and adult content: 1.1.1.3
	Yandex	Basic: 77.88.8.8,77.88.8.1, Safe: 77.88.8.88,77.88.8.2, Family: 77.88.8.7,77.88.8.3
	Quad9	9.9.9.9 No filtering: 9.9.9.10
No Protective DNS	CNNIC SDNS	1.2.4.8
	DNS.Watch	84.200.69.80, 84.200.70.40
	Freenom World	80.80.80.80
	Google Public DNS	8.8.8.8
	Hurricane Electric DNS	74.82.42.42
	Open NIC	96.90.175.167
	Oracle Dyn	216.146.35.35, 216.146.36.36
	Quad101	101.101.101.101
	Uncensored DNS	91.239.100.100
	Verisign OpenDNS	64.6.65.6
No information	Free DNS	45.33.97.5
	Level 3	209.244.0.3
	puntCAT	109.69.8.51

B Focus groups and Pilot

Before launching the Prolific survey, we performed two focus groups. The first included five participants from our computer science department and the second had four people without a background in computer science. Thanks to the first focus group, we reduced the survey size and switched from a conjoint analysis to a standard survey because participants said it was easy to flick through the options. We toned down technical explanations of PDNS and further explanations were added to the questions after the second focus group. We ran a pilot with 10 participants in Prolific to check everything was working fine. We didn't change any questions, thus we used pilot data in the study's results.

C DNS Measurement

A DNS measurement similar to the APNIC data collection was integrated into the Prolific survey. We included a Javascript that was triggered when participants submitted their unique Prolific ID. The Javascript fetched `'https:// prolific ID + .[DOMAIN NAME UNDER OUR CONTROL]'`. We recorded their resolver's IP addresses to determine if they were using PDNS or not. We mapped participants' IP and their resolvers' IP to ASes using Pyasn [40]. Out of the 295 participants, we obtained DNS logs for 285 of them.

D Survey instrument

https://doi.org/10.4121/22232911.v1

E Interview protocol ISP

Informed consent

1) What kind of Internet-connected devices do you own?

2) Do you think that your online devices are secure against being abused? Why or why not?

3) What do you think can be the consequences of abuse of Internet-connected devices?

4) Who do you feel should be responsible for the security of Internet-connected devices?

5) Do you use any security software or services or other security precautions to protect your Internet-connected devices?

- **If 'Yes' answered to question 5:** 6) What kind of security measures do you use?
- **If 'No' answered to question 5:** 6) Why you do not use any security measures?

7) Did you enable the [ISP name] [service name]?

- **If 'Yes' answered to question 7:** 8) Why did you enable the [service name]?
- **If 'No' answered to question 7:** 8) Why you did not enable the [service name]?

9) Do you think there could be any drawbacks associated with the use of services like [service name]?

10) How do you feel about your ISP offering the [service name]?

Demographics questions

F Enterprise Interviews

Informed consent

1) What is your role in this organization?

2) What is your organizations' core business?

3) How many employees does your organization have?

4) What network security concerns does your organization have?

5) Do you have network security policies and measures that address the network security concerns that your organization has?

6) How does your users' activities relate to those policies and security measures?

7) What kind of DNS resolver does your organization use?

8) Does your organization use any form of filtering in the network at DNS level?

9) Are you aware of services that filter malicious domains?

- **If the organization uses Protective Domain Name System:**

10) Why does your organization use these subsets of measures [mentioned in question 5] and PDNS?

11) Why did your organization choose to use PDNS as an additional measure?

12) How is PDNS used in your organization?

13) How costly it is to use PDNS versus other security measures?

14) Which results of the use of PDNS are most valuable? How often does this occur?

15) Have your organization ever had any problems in the operation of the network due to the use of PDNS?

16) What do you think about government initiatives about PDNS? (e.g. CIRA Canadian shield, The United Kingdom, Australia, and DNS4EU)?

17) Will your organization change your current PDNS for one provided by the government?

- **If the organization does not use Protective Domain Name System:**

(Note: Definition of PDNS was provided in case the participant didn't know what PDNS was)

10) Could your organization consider using something like PDNS?

11) Do you think that a service such as PDNS can be an addition to your security measures?

12) What factors will your organization consider to use a service such as PDNS as an additional measure?

13) How costly do you think the use of PDNS can be versus other security measures?

14) Which results of the use of a service such as PDNS could be most valuable to your organization?

15) Could you foresee any problems with the use of PDNS in the operation of the network?

16) What do you think about government initiatives about PDNS? (e.g. CIRA Canadian shield, The United Kingdom, Australia, and DNS4EU)

17) Will your organization consider using a PDNS service provided by the government?

G Experts interviews

Informed consent

1) What is your experience with DNS?

2) What do you understand as Protective Domain Name System?

3) What do you think of Protective Domain Name System for security purposes?

4) How Protective Domain Name System is different from other current available security solutions?

5) Do you have any concerns about the operation of Protective Domain Name System ? Prompts: (i) Who should be offering this service? (ii) Who should be using this service? (iii) What factors should be considered in order to adopt PDNS? (iv) Pros and cons / factors for success and failure

6) What do you think about government initiatives about Protective Domain Name System? (e.g. CIRA Canadian shield, The United Kingdom, Australia, and DNS4EU)

H Qualitative coding

Table 3: Summary of qualitative coding scheme ISP interviews

Themes	**Code examples**	**Respondents** **n=24**
Concerns about the service	Privacy, data usage, cost	21 (88%)
Reasons for not adoption	Other SW to block malware, cost once enabled	15 (62.5%)
Belives on abuse	Identity fraud, phishing, spread malware, data stolen	15 (62.5%)
Trust	Trust ISP, distrust email	11 (46%)
Reasons for adoption	Useful service, prevent malware, ISP advice	9 (37.5%)

Table 4: Summary of qualitative coding scheme enterprise interviews

Themes	**Code examples**	**Respondents** **n=12**
Awareness of PDNS	Knows about PDNS, does not know about PDNS	12 (100%)
Concerns about PDNS	Privacy, false positives	9 (75%)
Government PDNS	Welcome government initiatives, Do not welcome government initiatives, useful to have options	9 (75%)
Factors to consider for adoption	Layered security, threat model	7 (58%)
Reasons to implement PDNS	Global TI, reputation	6 (50%)

Table 5: Summary of qualitative coding scheme experts interviews

Themes	**Code examples**	**Respondents** **n=9**
Factors for adoption	Performance, users awareness, organizations' security strategy	9 (100%)
Provider	Who should offer PDNS, PDNS provider, gov as provider	9 (100%)
Limitations of PDNS	What can go wrong, complementary solution	9 (100%)
Types of blocking	Legal basis blocking, blocking for security purposes, benign content blocking	8 (89%)
PDNS vs other security measures	DNS path broken, no installation, all devices protected	8 (89%)
Privacy	Data sharing, data monetization, privacy	7 (78%)
Transparency	Who decides what to block, transparency	6 (67%)
Centralization	Options to choose, diversification	6 (67%)

I Variables included in the final ordinal regression model

Reference category	Variables	Explanation of coding	Survey questions
	Concerns	Factor analysis	Q24,Q25,Q26
	Perceived vulnerability	Factor analysis	Q6,Q7,Q8
	Perceived severity	Factor analysis	Q9,Q10,Q11,Q12
	Useful	Continuous scale	Q19
No security installed by themselves	Install security themselves	True if participant recall setting up security features in his internet-connected devices by himself and did not provide any other answer	Q13
Do not use any security tool	Use other security measures	True if the participant uses Antivirus or Firewall or Ad blocker or any other tools to protect his devices and did not answer that he does not implement any security tool.	Q14
Does not use parental control	Use parental control	True if participant uses parental control	Q15
Not aware	Aware	True if participant heard before of a similar service like PDNS only	Q17
	Unsure	True if the participant was not sure of hearing of a similar service like PDNS only	
Not willing to pay	Willing to pay	True if participants were willing to pay for PDNS service.	Q34
Government provider	Commercial provider	True if commercial provider was selected and not government or ISP provider or other provider.	Q30
	ISP provider	True if ISP was selected as provider and not government or commercial provider or other provider.	
	Other provider	True if other provider was selected and not government,or ISP provider or commercial provider.	

Control variables:

Reference category	Variables	Explanation of coding	Survey questions
Male	Female	True if participant identify as female and not as male or other genders	Q36
	Other genders	True if participant identify as other gender and not as Male or Female	

J Top 20 countries with PDNS usage

Table 6: Top 20 countries with the highest percentage of DNS queries answered by PDNS (Period: January to June 2022)

				Non Public DNS resolvers			Public DNS resolvers			
cc	**avg daily queries**	**Internet users**	**% sampled**	**% Same AS**	**% In country**	**% Out country**	**% PDNS**	**% No PDNS**	**% Possible PDNS**	**% No Info**
IL	53,235	7002759	0.76%	50.4%	2%	0.3%	34%	12.1%	1.1%	0.1%
AF	10,963	9327489	0.12%	25%	0%	5%	25%	40%	4%	1%
CY	15,205	1011831	1.5%	53.4%	12.4%	0.4%	23%	8.5%	1.8%	0.5%
ME	18,283	449989	4.06%	54.4%	0.1%	1%	22.3%	22%	0.2%	0%
TZ	45,146	23142960	0.2%	44%	10%	0%	9%	36%	1%	0%
GE	38,407	32543600	0.118%	49%	25%	0%	8%	13%	5%	0%
ZM	22,695	9870427	0.23%	3%	0%	0.3%	7.3%	72.4%	0%	17%
NG	213,900	126078999	0.17%	65%	3%	2%	7%	23%	0%	0%
IR	94,366	67602731	0.14%	26%	9%	31%	3%	8%	22%	1%
AL	57,115	2160000	2.64%	67.1%	0.4%	0.1%	2.6%	25.3%	4.3%	0.2%
US	871,976	313322868	0.28%	62.4%	10%	2.1%	2%	20.1%	3%	0.4%
EG	475,809	49231493	0.97%	68%	13%	0.5%	2%	16%	0.5%	0%
VN	152,645	84883000	0.18%	68.4%	0.8%	0.2%	1.1%	27.5%	1.9%	0.1%
ID	1,320,259	212354070	0.62%	68%	17%	0%	1%	12.4%	1.6%	0%
BR	525,834	150457635	0.35%	48.3%	15%	1.4%	1%	28.3%	6%	0%
TR	228,978	69107183	0.33%	53%	31%	0%	1%	14%	1%	0%
UA	158,809	40912381	0.39%	68%	4%	1%	1%	20%	6%	0%
PH	595,824	95200000	0,63%	45%	34%	0.2%	0.4%	18%	2.3%	0.1%
IN	3,207,855	755820000	0.42%	58.1%	27.2%	0.1%	0.2%	14%	0.3%	0.1%
BD	790,017	117310000	0.67%	58%	5%	0.4%	0.2%	32.4%	4%	0%

Note: **% Same AS:** Percentage of average daily queries which resolvers ARE in the same AS as the users and NOT known public DNS resolvers. **% In country:** Percentage of average daily queries which resolvers are NOT known public DNS resolvers and NOT in the same AS as the users, but ARE geolocated in the same country as the user. **% Out country:** Percentage of average daily queries in which resolvers are NOT known public DNS resolvers and NOT in the same AS as the users but, and NOT geolocated in the same country as the user. **% Public DNS resolvers:** percentage of average daily queries which are answered by resolvers as categorized in Appendix A.

K Ordinal Logistic Regression

Figure 1 displays on the left side the variables with beta (β) which is the estimated regression coefficients of the variables (all the beta values in the graph are significant at $p < 0.1$), and their standard error. On the right side the odds ratio (OR), which is the exponentiated regression coefficient, and their confidence interval.

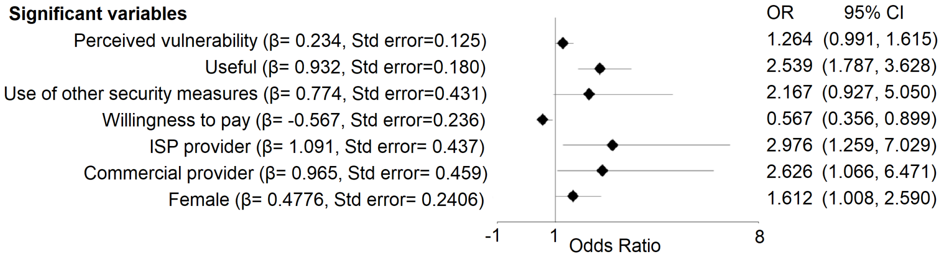

Figure 1: Significant predictor variables