Policy and Internet

Policy & Internet, Vol. 9999, No. 9999, 2019

Privacy by Infrastructure: The Unresolved Case of the Domain Name System

Samantha Bradshaw and Laura DeNardis

Digital privacy concerns are primarily viewed through the lens of personal data and content. But beneath the layer of content, less visible issues of infrastructure design and administration raise significant privacy concerns. The Internet's Domain Name System (DNS) is one such terrain. There is already a great deal of attention around how the DNS intersects with freedom of speech, trademark disputes, cybersecurity challenges, and geopolitical power struggles in the aftermath of transitioning the historic U.S. oversight role to the global multistakeholder Internet governance community. However, the privacy implications embedded in the technical architecture of the DNS have received less attention, perhaps because these issues are concealed within complex technical arrangements outside of public view. This article explores privacy issues in the DNS by examining two contemporary, and still unresolved, case studies: the WHOIS system as a de facto *Internet identity system revealing website registrants; and privacy in domain name queries, which have historically been unencrypted and therefore reveal personal information about what sites individuals visit. DNS privacy challenges not only demonstrate the important connection between infrastructure and rights, but also exemplify how cross-border, universal technologies come into conflict with the bounded laws of nation states. It is a critical moment of opportunity to examine these cases because their resolution will help determine the future of basic privacy rights online.*

KEY WORDS: Internet governance, Domain Name System, privacy, WHOIS, DNS queries, freedom of expression, cybersecurity

数字隐私顾虑主要通过个人数据和内容进行查看。然而在内容的表象下，模糊的网络基础设施问题及行政问题引起了显著的隐私顾虑。网络域名系统(Internet's Domain Name System, DNS)则是其中之一。现已有大量关注聚焦于——将美国监管角色转变为全球多方利益相关者(multistakeholder)共同治理互联网社区之后——DNS如何与以下几点产生交集： 言论自由、商标争议、网络安全挑战、以及地缘政治权力斗争。然而， DNS技术架构中所嵌入的隐私含义却并未受到较多的关注，这也许是因为这些问题被隐藏在复杂的技术协议中，无法出现在大众视野。本文通过检验两个有待解决的案例研究， 进而探索了DNS中涉及的隐私问题。这两个案例研究分别是：作为事实上的互联网识别体系，揭示网站注册登记者的WHOIS 系统；和域名请求中的隐私。后者曾经被破解， 因此泄漏了个人所浏览过的网站信息。DNS隐私所面临的挑战不仅证明了网络基础设施和权利之间的重要联系，同时举例证明了跨边界的普遍技术如何与国家法律边界产生冲突。对这些案例进行检验则是关键的机遇时刻，因为这些问题的解决将会帮助确定今后的网络基本隐私权。

关键词： 网络治理，域名系统，隐私，WHOIS，DNS 请求，言论自由，网络安全

doi: 10.1002/poi3.195

Las preocupaciones sobre la privacidad digital se ven principalmente a través de la perspectiva de datos personales y contenido. Pero debajo de la capa de contenido, los problemas menos visibles de diseño y administración de la infraestructura plantean importantes problemas de privacidad. El Sistema de Nombres de Dominio (DNS) de Internet es uno de esos terrenos. Ya se le da mucha atención a cómo el DNS está en una coyuntura con la libertad de expresión, disputas de marcas, desafíos de seguridad cibernética y luchas de poder geopolíticas tras la transición del histórico papel de supervisión de los EE. UU. a una comunidad mundial de gobernanza de múltiples partes interesadas. Sin embargo, las implicaciones de privacidad incorporadas en la arquitectura técnica del DNS han recibido menos atención, tal vez porque estos problemas se ocultan dentro de arreglos técnicos complejos fuera de la vista del público. Este artículo explora problemas de privacidad dentro del sistema DNS al examinar dos estudios de caso contemporáneos que están todavía sin resolver: el sistema WHOIS como un sistema de identidad de Internet de facto que revela a los registrantes del sitio web; y la privacidad en las consultas de nombres de dominio, que históricamente no se han cifrado y, por lo tanto, revelan información personal sobre qué sitios visitan los individuos. Los desafíos de privacidad de DNS no solo demuestran la conexión importante entre infraestructura y derechos, sino que también ejemplifican cómo las tecnologías universales transfronterizas entran en conflicto con las leyes limitadas de los estados nación. Es una oportunidad crítica para examinar estos casos porque su resolución nos ayudará a determinar el futuro de los derechos básicos de privacidad en línea.

PALABRAS CLAVES: gobernanza de Internet, Sistema de Nombres de Dominio, privacidad, WHOIS, búsquedas de DNS, libertad de expresión, ciberseguridad

Introduction

Governance of the Internet's Domain Name System (DNS) has long been a source of global political contention. The highest profile debate, both real and symbolic, involved the 2016 transitioning of the historic role of the U.S. Department of Commerce in overseeing certain aspects of DNS administration, such as changes to the authoritative root zone file that maps top-level domains to their corresponding Internet Protocol (IP) addresses. But the politics of the DNS extend far beyond the questions surrounding this authority. DNS design and administration raise numerous, less visible, public interest issues—including conflicts over property and ownership, such as copyright enforcement and domain name trademarks; questions related to national security and cybersecurity; and human rights concerns around the distribution of critical Internet resources, or what counts as free speech in domain names (Bradshaw & DeNardis, 2018). Privacy is another important issue that inherently arises in the DNS, but only a few scholars have examined these issues to date (Bruen, 2015; Elliott, 2009; Mueller & Chango, 2008). The European Union's (EU's) General Data Protection Regulation (GDPR) which came into force in May 2018 further complicated debates around privacy in the DNS.

Discourses on digital privacy have focused largely on content-centric concerns, including: *government surveillance*, highlighted by disclosures about the expansiveness of National Security Administration (NSA) surveillance programs;

corporate surveillance and the paradigm of "free-to-use" services, whereby online business models depend upon the collection, retention, and sharing of personal data; *cybercrime and data breaches* that have compromised consumer retail information, health care data, personal emails and online accounts, and government records for the purposes of fraud or identity theft; and *national security tensions* over the extent to which law enforcement can access encrypted communications and smartphone data.

Beneath this layer of communication and content, privacy issues are also embedded in deeper layers of infrastructure and code. The Internet's technical layers are not as visible to end users, but nevertheless have enormous implications for Internet governance and policy (Braman, 2011; Cath & Floridi, 2017; DeNardis, 2014; Epstein, Katzenbach, & Musiani, 2016; MacKinnon, 2012; Mueller, 2010; Zittrain, 2008). *Privacy by infrastructure* reflects how arrangements of this technical architecture have implications for personal privacy. These concerns include questions around protocol design, encryption strength, surveillance mechanisms at Internet exchange points, cryptography backdoors, or whether to assign unique identifiers to information flows.

The DNS is also a critical concern of privacy by infrastructure, and one that underlies almost every transaction over the Internet. As a massive, globally distributed system of physical hardware and software, protocols, virtual identifiers, and institutions that organize, administer, and coordinate the Internet's addressing space, its main function is to translate human-readable domain names (www.american.edu) into the binary addresses (147.9.4.186) that routers use to locate online services and information, somewhat analogous to a telephone directory. Although the DNS performs a critical Internet operation, it functions behind the scenes and, not surprisingly, is largely missing from mainstream cyber policy discussions.

DNS infrastructure has always created an inherent set of privacy concerns. First, the Internet requires the use of globally unique IP addresses,[1] either assigned permanently or temporarily for a session. These virtual identifiers, in combination with other information, create a path for identifying individual users as they access or exchange information online. Second, requests to the DNS are almost always made "in the clear," meaning that even if content is encrypted, the fact that a connection was requested to an end point is not. Unencrypted DNS query data is susceptible to surveillance, which can have implications for individual privacy as well as security. Third, the DNS was designed without verification measures to authenticate domain names, which creates susceptibility to spoofing and man-in-the-middle attacks. While the DNS Security Extensions Protocol (DNSSEC) offers validation of DNS records via digital certificates, the transfer of the DNS record is still conducted in-clear, and thus would not protect against the collection or passive monitoring of DNS queries. Although this is generally considered to be a technical security challenge (i.e., authenticating a domain name), the inherent trust assumed by DNS transactions also creates privacy concerns by providing more opportunities for surveillance or unauthorized access to personal data stored on servers or in the cache. Fourth, and arising historically in an environment in which there were only a small number of (trusted) users, the DNS has included a system (WHOIS) in

which personal information about website registrants is made publically available. However, in the current global environment where online harassment, identity theft, spam, censorship, and surveillance are widespread there remain several critical questions about whether and under what conditions websites can be registered anonymously. Finally, the DNS is distributed across hundreds of registries and operators in order to improve the reliability and performance of the system. These operators are geographically diverse and have different policies for protecting user privacy, and users have little-to-no control over where or how their DNS requests are sent and managed.

Drawing from the archival mailing lists of DNS privacy working groups, meeting proceedings of the Internet Engineering Task Force (IETF), registry policies, and relevant Internet Request for Comments (RFC), this article examines two unresolved issues: WHOIS as an identity disclosure system, and privacy concerns in DNS queries. Similar to all areas of Internet governance, these issues are unresolved because of competing interests of intellectual property rights holders, law enforcement, privacy advocates and private company. For example, law enforcement and intelligence gathering agencies have an interest in readily accessing identifying information about domains used to engage in piracy, terrorism, or criminal activities. On the other hand, laws seeking to protect privacy, such as the EU's sweeping data privacy directive (GDPR) establish legal protections and penalties around personal data disclosure. The technical arrangements around the DNS are now an arena of conflict and negotiation in which these debates are mediated.

WHOIS as the Internet's Identity Disclosure System

Throughout the Internet's history, anyone interested in learning the identity of who owns and operates a website could search for this information in a publicly available directory similar to a telephone directory. The WHOIS system[2] is a freely available, searchable, global directory in which anyone historically has been able to look up the identity and associated personal information of a domain name registrant. Some registrars have offered proxy registration services that mask identities, but generally, the default registration process discloses personal information. For individuals who have registered a domain name for a personal website, blog, or small business, a WHOIS search can reveal a great deal of personally identifiable information, including the registrant's name, phone number, email, fax number, and home address. For an institution holding the registration, this would include an employee's name, and the address and other identifying information for the institution.

WHOIS is not a single, centrally administered database, but a collection of independently managed directories run by registrars and registries accredited (for generic top-level domains; e.g., ".org") by the Internet Corporation for Assigned Names and Numbers (ICANN). Together, these directories enable global searches of who has registered any domain name or IP address. ICANN is the not-for-profit global institution tasked with overseeing domain names and IP addresses, although it delegates operational responsibility to many institutions, including

domain name registrars, Internet registries that oversee the DNS mapping for top-level domains, and regional Internet registries that further allocate and assign IP addresses. The WHOIS system predates ICANN, which was formed in contract with the U.S. government in the late 1990s.

WHOIS, which dates back to 1982, was designed to identify anyone registering a name on the Advanced Research Projects Agency Network (ARPANET). This directory system, originally described in RFC 812, required individuals with an ARPANET host directory to register their name, mailing address, zip code, and phone number in this identification database (Harrenstien, Stahl, & Feinler, 1985; White & Harrenstien, 1982). The existence of such a directory in the pre-Web (and even pre-DNS) years did not raise significant privacy concerns. ARPANET connected a relatively closed and trusted user community, and the information captured in the directory would not have been an individual's personal details, but rather the institutional location and phone number where the ARPANET host resided.

The WHOIS protocol also had pragmatic origins in creating a way for network operators on ARPANET to locate a phone number for other operators to report or troubleshoot problems (Newton, 2006). There were no commercial or social interests, and access was limited primarily to research and defense communities. Because of the small and trusted environment in which ARPANET arose, the system did not have the type of security or privacy features that a modern system might include. WHOIS eventually became closely associated with the DNS because of its ability to find domain names or IP addresses and their associated registrants.

The WHOIS protocol is a simple Transmission Control Protocol (TCP)-based query and response protocol. The following, an example taken directly from the most recent WHOIS specification from 2004, RFC 3912 (Daigle, 2004), shows the packets that would be sent between a client requesting information about an identifier "Smith" and how information is returned:

```
Protocol Example
If one places a request of the WHOIS server located at whois.nic.mil
for information about Smith, the packets on the wire will look
like:
client server at whois.nic.mil
open TCP ---- (SYN) ------------------------------>
<---- (SYN+ACK) -------------------------
send query ---- Smith<CR><LF> --------------------->
get answer <---- Info about Smith<CR><LF> ---------
<---- More info about Smith<CR><LF> ----
close <---- (FIN) ------------------------------
----- (FIN) ---------------------------->
```

From a technical standpoint, the protocol performs a simple directory function using a query and response. From a policy standpoint, several complex privacy concerns arise, as became apparent during the period of commercialization and rapid growth of the Internet in the 1990s and early 2000s.

Unresolved WHOIS Privacy Concerns

Should someone who registers a domain name be able to do so anonymously, thereby operating a website without disclosing their identity to the public or to authorities? Or should there be transparency and disclosure of the people or institutions behind every online presence? Public interest concerns such as combating terrorism, enforcing laws around defamation, cyberbullying, hate speech, spam, and protecting intellectual property rights favor transparency. Values of freedom of expression, innovation generativity, and individual privacy favor anonymity at the level of domain name registration. For example, for those operating politically sensitive websites, the exposure of personal information can lead to both online and offline harassment and, potentially, physical intimidation and harm. The procedural decisions around whether to require domain name registration transparency, openness, and searchability is not just a black and white issue of whether citizens should be able to anonymously operate a website. More granular questions include the possibility of public-facing anonymity but with registration data available to law enforcement under certain conditions, and if so, what conditions, as well as whether registrants should have some choice over what personally identifiable information is publicized online. Because of the high stakes of these often-conflicting public interest concerns, questions pertaining to anonymity in domain names have consumed policy debates for decades. The default norm has not been anonymity and privacy, but rather transparency and public access to personal information about domain name registrants.

In 2001, the Judiciary Committee of the U.S. House of Representatives held a hearing entitled "WHOIS Database: Privacy and Intellectual Property Issues," which examined a number of emerging issues related to WHOIS (US Judiciary Committee, 2001). One dimension of the debate has involved whether there should be a distinction between individual registrants and institutional registrants in terms of what data is published. On the one hand, what is objectionable about online businesses having to provide their place of business and contact information? On the other, why should an individual operating a website for political speech (or for publishing photos of their cat) have personally identifiable information published? It was already clear in 2001 that the distinction between institution and individual was not meaningful: many institutions engage in political speech, and many individuals operate online businesses. It was also clear that businesses with an interest in intellectual property rights enforcement were central to the debate, portraying WHOIS as a primary mechanism for identifying perpetrators of intellectual property rights infringement, whether sharing pirated movies, selling counterfeit products, or cybersquatting domain names (US Judiciary Committee, 2001).

As the Internet grew internationally and commercialized, concerns were raised that the availability of personal registrant information would expose individuals to problems such as spam and harassment. Registrant information became a resource for law enforcement to identify criminals engaging in online identity theft, piracy, terrorism and other illegal practices. The public availability of this registrant information also quickly raised concerns for free speech, such as

whether authoritarian regimes could use this registration information as a tool for tracking down and then censoring or imprisoning political adversaries, activists, and alternative media.

Under its 2009 "Affirmation of Commitments" contractual agreement with the U.S. Department of Commerce, ICANN perpetuated WHOIS—also called the Registration Directory Service—as part of the U.S. government's strategy to privatize and internationalize the administration of names and numbers. The contract required all accredited registrars to provide a WHOIS directory service of information about domain name registrants. If the registered name holder did not provide accurate information, the domain could be suspended. ICANN first contracted with accrediting registrars in 1999, immediately after the entity's formation. Under the accreditation agreement, the registrar was required to provide a WHOIS service offering "free public query-based access" to accurate data about registered names including the following elements (among others), unless an alternative was approved in writing (ICANN, 2013):

> 3.3.1.6 The name and postal address of the Registered Name Holder;
>
> 3.3.1.7 The name, postal address, e-mail address, voice telephone number, and (where available) fax number of the technical contact for the Registered Name; and
>
> 3.3.1.8 The name, postal address, e-mail address, voice telephone number, and (where available) fax number of the administrative contact for the Registered Name.

Although some registrars offer proxy services to individuals who wish to mask public-facing personal information, ICANN also provides an online "WHOIS Inaccuracy complaint form" where anyone can notify ICANN about incomplete or inaccurate WHOIS data, whether personal or proxy contact information.

The basic function of domain name registration has remained largely unchanged for decades, but it is also a system whose future has been debated for years. Since 2008, ICANN has initiated a series of technological and policy studies to examine evolutionary possibilities for the system. There have also been several working groups and processes to examine issues around domain name identification. For example, open issues from the 2013 Registrar Accreditation Agreement led ICANN to charter a working group called the Privacy & Proxy Services Accreditation Issues Working Group. One of the questions posed related to a potentially significant change in WHOIS policy: should the use of proxy services "be restricted only to registrants who are private individuals using the domain name for non-commercial purposes" rather than remaining available to all individuals, noncommercial organizations and companies, as had been the case (ICANN, 2015). Again, making a commercial versus noncommercial distinction

regarding who can use a privacy/proxy service is not at all clear: Would this be based on organizational form (e.g., type of incorporation), type of transaction, presence of advertisements, or be dependent upon occurrence of financial exchanges? Individuals working from home could be deemed commercial and have their home addresses published. Large media companies providing free content online could be deemed noncommercial under certain circumstances. The Working Group has acknowledged these complexities (Expert Working Group, 2014).

Media content companies, entertainment companies, and those with a high stake in intellectual property enforcement issues have consistently pushed for more restrictions on proxy service eligibility. However, the Electronic Frontier Foundation has noted the dangers faced by the possibility of no longer allowing commercial domains to use proxy registration services (Malcolm & Stoltz, 2015). Others have suggested that all the deliberations about the future of WHOIS policy have not resulted in significant consensus, never mind policy change. For example, Google's Senior Trademark Counsel Andy Abrams issued a response that described the overall scope and comments of the Working Group's initial report as "misguided," suggesting that the recommendations "will not resolve the issues they are ostensibly designed to address" (Google, 2015). Instead the Google submission recommended that the community turn its attention to solving a greater problem affecting WHOIS, such as botnets and phishing.

To combat some of the shortcomings of WHOIS, one technical alternative that has emerged from the engineering community is the Registration Data Access Protocol (RDAP), which seeks to standardize the registration queries and responses, facilitate internationalization by supporting languages other than English, and facilitate redirection of query referrals to other registries (APNIC, 2017). RDAP was developed out of the IETF's "WEIRD" (Web Extensible Internet Registration Data Service) working group. While this protocol does not directly speak to privacy concerns, it does serve to entrench the default norms of collecting and sharing data related to domain name registration.

After decades of policy and technical deliberation about domain name registration policy, overarching privacy questions remain, including the use of proxy services, approaches to default settings, the role of ICANN accreditation, and—particularly in the context of the EU's strong privacy regulations—whether public disclosure of registration information violates data protection laws. As part of a trajectory of laws addressing personal data protection, the EU adopted the GDPR, effective May 2018. Replacing the EU Data Protection Directive, the GDPR imposed a new set of rules and obligations on organizations that collect personal data of EU residents. The new EU privacy regulation raised questions about whether ICANN policies around the collection, management, and publication of registrant information comply with the GDPR. Because of the substantial financial penalties incurred for noncompliance with the GDPR, registrars have been rightly concerned. The EU GDPR specified a data minimization principle in which personal data shall be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed," and a binding purpose principle where data may only be

"collected for specified explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes" (General Data Protection Regulation, 2018). As of mid-2018, ICANN was put in the position of making major revisions in compliance with the GDPR (ICANN, 2018) . On the surface, this seems not to comport with the many secondary and tertiary uses of Web registrant data. Domain name registrars, who are required by ICANN to publicly list registrant data have pushed back against the possible consequences of GDPR constraints on data collection and publication. This is another indication of the complex challenges of DNS privacy, and how regional rules are not restricted to geography, but can affect universal systems of Internet infrastructure.

Unresolved Privacy Concerns in DNS Queries

In American pop culture, the phrase "More Cowbell" instantly invokes a hilarious Saturday Night Live skit starring Christopher Walken, Will Ferrell, and Jimmy Fallon spoofing the 1980s rock-band Blue Oyster Cult. In the skit, Christopher Walken's character famously proclaimed, "I've got a fever and the only prescription is more cowbell." Years later, someone in the NSA displayed a sense of humor when naming a DNS monitoring program MORECOWBELL. Despite this touch of levity, the existence of this program raises serious questions around how the DNS can be monitored, and the various privacy considerations inherently raised by its operation.

When the DNS was first designed, confidentiality of query data was not a concern because the information in the pre-Internet/ARPANET days was qualitatively different than the heterogeneity and sensitivity of online resources that would emerge as the Internet evolved. Because of this historical context, the DNS treats all query information as public data by default. According to RFC 4033: "DNS was originally designed with the assumptions that the DNS will return the same answer to any given query regardless of who may have issued the query, and that all data in the DNS is thus visible" (Larson, Massey, Rose, Arends, & Austein, 2005). This characterization is appropriate as the DNS performs a lookup function for universally consistent names and numbers analogous to an address book. However, there is an important differentiation to be made between the name and corresponding IP number of a website, and the transactional data (or metadata) that is exchanged as the DNS retrieves this information for the user who requests it.

Every time a user visits a website using an Internet browser or mobile device, the DNS will query the location of that content on the network. These queries perform the behind-the-scenes task of translating an individual's request for a certain resource into an IP address. This function is carried out by special DNS servers, which are usually provided by an Internet Service Provider (ISP). However, third-party name resolution services are also offered by private companies and nonprofit organizations.

DNS lookups are conducted via the process of recursive resolving, whereby a user's device sends a request to its DNS resolver to systematically search the DNS

hierarchy for information about a website's virtual location. Internet RFC provide a more detailed description of the process, but recursive resolution can basically be understood to occur in several stages (Mockapetris, 1987a, 1987b). First, a query is sent to the top of the DNS hierarchy (or the root zone) asking for the location of the website (Figure 1). If the queried DNS server does not have the answer, it will forward the request further down the hierarchy. This iterative process is repeated until the resolver locates the authoritative name server hosting the requested name. Because this process can be time-consuming, previous lookups are often cached locally to improve the speed of query requests. These cached records are assigned a "time to live" record that is stored temporarily, until the record expires.

DNS queries are used for almost every activity online. In terms of scale, one web page load can involve approximately 10–15 DNS queries to deliver content to users, which means an average household can perform between 1,000 and 1,500 DNS queries a day (Verisign, 2015). Whether a user wants to send an email or access a website, the DNS needs to query servers to find and deliver information across the network. Even when making a phone call over the Internet using Voice over IP (VoIP), DNS architecture is typically used to facilitate a connection between the end points and the VoIP server (Conroy, Fujiwara, & Bradner, 2011). Accessing and monitoring DNS query records can therefore disclose a connection that occurred between two end points (and potentially two people) on a network—including any voice calls made via VoIP.

Certain technical design choices within the DNS resolution process raise concerns for individual privacy. A common belief is that DNS queries do not contain content, and therefore do not disclose personally identifiable or private information. Although query data indeed contains no "content" like email text, images, or search terms, it can reveal the sites a user visits, as well as other transactional metadata such as the user's IP address, location, and time of request. Thus, query data can disclose sensitive information-seeking practices related to

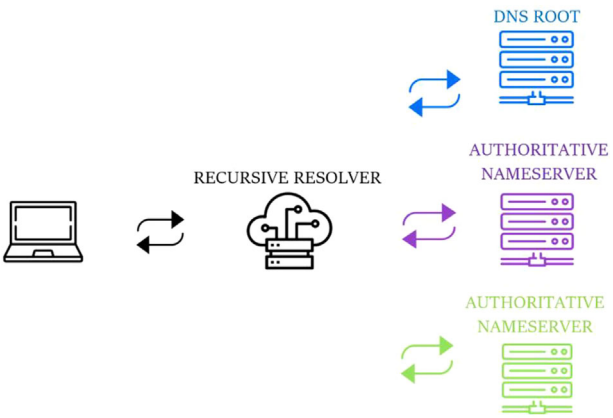

Figure 1. DNS Resolution (Simplified).

such topics as addiction services, gender identity, disease treatment, pornography, abortion clinics, mental illness, employment, or online dating services. Today, most concerns about the privacy of this information center around search engine data retention, smartphone data collection, and government surveillance practices. But the DNS resolution process raises similar concerns about the prospects for unauthorized access to such information, and practices for how query information is retained, aggregated, and shared.

The distributed nature of the DNS is another factor that can compromise personal privacy. Instead of having a single, centralized organization administering the entire Internet namespace, individual entities manage different domains. For example, governments can maintain their country-code domains (such as .ca or .cn), while an educational association can manage the .edu namespace. Although the distributed nature of the DNS allows changes to the records to be made quickly and accurately, it simultaneously increases its latency when individual users search for content online, as the system must establish multiple connections and transmit information across the network (Cohen & Kaplan, 2000). Resolvers must query at least one, but often several, authoritative name servers until it is directed to the correct address.

With the growing demand for faster access to Internet content, most modern-day Internet browsers will pre-resolve domains found in the hyperlinks of web pages, so they are ready to be accessed immediately if a user then decides to click on any of them. The goal of prefetching is to strike a balance between correctly guessing which links users will follow on a page, and reducing the number of "missed" or wasted lookups. While prefetching domain names can help optimize viewing speeds for Internet users, it also affects personal privacy by providing more data points for those monitoring DNS records to analyze and correlate. When a user's device sends a query request to its DNS resolver it will often ask for the Web server's domain. For example, if a user is trying to access www.wikipedia.org/corruption, the resolver is only aware of the fact that the user wants to connect to Wikipedia's webserver (www.wikipedia.org). In some cases, a Web server that hosts or aggregates content for a user—such as Wikipedia or Google—might not reveal much about their intentions. However, when domain names are prefetched there could be enough metadata associated with the requests to identify a user (Krishnan & Monrose, 2010). Domain name prefetching occurs quite often and is built into most modern-day browsers including Chrome, Internet Explorer, and Firefox (Souders, 2013). In Google Chrome, when a user types in the search bar, the domain names of autocompleted URLs are also prefetched (Stark, Huang, & Israni, 2012). However, users have very little control over what content is prefetched and how underlying algorithms make these decisions.

Another technical feature of DNS queries is that they are almost always unencrypted. As explained in an informational RFC draft: "DNS traffic is today sent in clear (unencrypted), except a few cases when the IP traffic is protected, for instance in an IPsec VPN" (Bortzmeyer, 2015). Because DNS queries are unencrypted, they can be observed at multiple points across the network,

including the location of the initial query to the authoritative servers responding to requests (Conrad, 2012). It was commonly assumed that data in the DNS did not warrant encryption because there was no additional information that could be gleaned if one could access the content of the lookup (Koch, 2013). Therefore, even if communications between two end points are secured with end-to-end encryption, meaning the exchanged content is not visible, the DNS exchange facilitating the connection will be. As end-to-end encryption becomes more prominent across the Internet's application layer, the DNS could thus become the "weakest link" in privacy (Bortzmeyer, 2015). Although recently there have been several initiatives by companies to offer encrypted DNS requests, many of these fixes have to be configured by users who might not have the technical capacity or understanding to implement them. Due to the technical norm of unencrypted queries, two points of potential privacy risk enter the DNS resolution process: the exchange between an end user's device and the recursive resolver; and the exchange between this recursive resolver and an authoritative DNS server (Hallam-Baker, 2014).

Privacy Risks Associated With Recursive Resolvers

With the exception of locally cached lookups, recursive resolvers see almost all the query data sent to and from a user's device. An ISP typically facilitates recursive requests, however, fragmented privacy laws have meant that many ISPs are not required to specify how query data is collected, stored, processed, shared, or even sold to third parties (Figure 2).

Some suggest that the role of ISPs in facilitating recursive lookups may not be problematic because changes in Internet access have limited the amount of consumer data ISPs can access via DNS queries (Swire, Hemmings, & Kirkland, 2016). In the early 1990s, people connected mainly via a personal desktop computer. DNS query data would be logged from a single stationary device located in an individual's home, making user identities much easier to track and

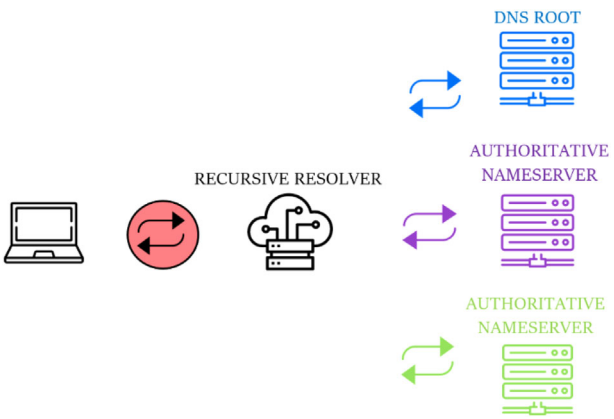

Figure 2. Privacy Concerns Between the User and Recursive Resolver.

observe. Today, however, users are connecting from different portable devices over a combination of network services, from mobile phones to various Wi-Fi access points. From a privacy standpoint, some argue that this combination of "mobility" and "multiplicity" is making it much more difficult for any single ISP to track a single user's activity online (Swire et al., 2016). However, these claims do not consider that most users still use their home networks to process many Internet requests. By simply observing traffic patterns (and not necessarily the content of the traffic) it is possible to determine a significant amount of information about any given household such as the types of devices users have in their home, how often they use each device, the websites they are visiting and how often, or the times at which the user is likely to be home (Grover et al., 2013). And although a user's Internet connection is less fixed than in the past, the rise of shared Wi-Fi hotspots can provide a single ISP with much more information about users than in the past, allowing them, for example, to access geolocation data to track movement over time (Feamster, 2016).

Several third-party DNS resolvers also offer resolution services to Internet users. Private companies, such as Dyn, typically provide resolution and other DNS management and optimization services for companies hosting content online. Other commercial organizations, such as Google, Cisco, and Cloudflare, provide DNS resolution services that users can set up for free. In addition, some not-for-profit organizations such as OpenNic, also operate DNS resolvers. Overall, there has been a growing number of users and businesses utilizing third-party resolution and DNS management services. For example, Google's Public DNS service processes more than 70 billion requests per day (Google, 2012).

Third-party providers give users some control over their query data, and thus are playing an important intermediary role by offering users alternative options to connect and browse Internet content. We conducted a systematic analysis of the privacy policies of 19 third-party DNS resolvers, in order to examine the kinds of information that was collected (personally identifiable data, metadata, and query data, such as the requested domain name and when it was accessed), how this information was used (for marketing or advertising, and policies on third-party use), and guidelines around data storage. We found very little consistency in the privacy practices of these providers. Most providers (12 of the 18 we examined) collect some personally identifiable information and metadata from users, and only four (DNS Watch, FreeDNS, Uncensored DNS, and Cloudflare) do not collect any information from users. Some providers, such as OpenNic, allow users to customize what DNS servers they connect to, where they are located, and how much information is logged; thus the levels of privacy afforded to users is different depending on the resolver they select. And although third-party providers offer resolution services, very few provided specific information about what DNS query data was collected, used, and stored. Table 1 summarizes these findings.

The central role of recursive resolvers in connecting users to content and others on the network acts as a "hidden point of control" for controlling access to Internet content or monitoring user behavior. Recursive resolvers are the closest connection to the individual, and thus have access to some of the most sensitive

Table 1. Systematic Comparative Analysis of Third-Party DNS Resolver Privacy Policies

Service Provider	Collect PII Data?	Collect Metadata?	Query Data?	Marketing/Advertising?	Third-Party Use?	Data Storage?
Level 3	Y	Y	No info	Y	Y	Indefinite
Verisign	Y	Y	No info	Y	Y	No info
Google Public DNS	Y	Y	Y	Y	Anonymized	Temporary and permanent
Quad 9	Only IP address	Y	Y	N	Anonymized	Partial and full records, stored permanently
DNS.Watch	No info	N	N	N	Anonymized	No info
Comodo Secure DNS	Y	Y	No info	Aggregated	Aggregated	Indefinite
Open DNS (Cisco)	Y	Y	No info	Y	Y	Indefinite
Green Team	No info	No info	No info	No info	No info	No info
Safe DNS	Y	Y	Y	N	Y	No info
Open NIC	*	*	*	*	*	*
Smart Viper	Y	Y	No info	N	N	No info
Oracle + Dyn	Y	Y	No info	Y	Y	No info
Free DNS	N	N	N	N	N	N/A
Alternate DNS	Y	Y	Y	Registered	Registered	N/A
Yandex.DNS	Y	Y	Y	Y	Y	Indefinite
Uncensored DNS	N	N	N	N	N	N
Neustar	Y	Y	No info	Y	Registered	Temporary, length depends on kind of information
Cloudflare	N	N	N/A	N	N	N/A

Source: Authors' data collected from: Level 3, 2018; Verisign, 2018; Google, 2016; Quad 9, 2018; Comodo, 2018; Cisco, 2018; Norton, 2018; SafeDNS, 2015; SmartViper, 2018; Dyn, 2018; FreeDNS, 2018; Alternate DNS, 2016; Neustar, 2017; Cloudflare, 2018; DNS Watch, 2018). OpenNIC leaves privacy up to the individual operator of the authoritative name servers part of the network. They do not have an overarching privacy guideline for server operators, but they do publish information about what is collected by the servers in their network.

information about what individuals access online, who they connect with, when and how often connections are made, and from where. How operators protect query data matters immensely for individual privacy. Although DNS queries are the starting point for most online activity, there are no clear or specific laws or

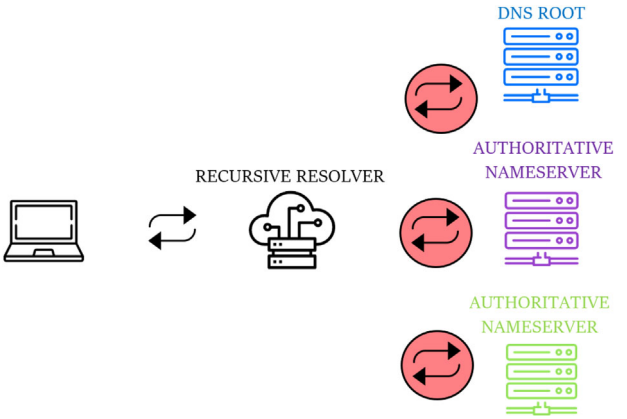

Figure 3. Privacy Concerns Between the Recursive Resolver and Authoritative Name Servers.

guidelines regulating how query data should be collected, aggregated, shared, and stored by recursive resolver providers.

Privacy Risks Associated With Authoritative Name Servers

In addition to privacy issues between the end user and the recursive resolvers, the second point of privacy risk occurs between recursive resolvers and authoritative name servers. Authoritative name servers are special servers responsible for a dedicated part of the namespace, to distribute the administrative authority across the DNS. These dedicated "zones" form a hierarchy with the root zone at the top, and the zones corresponding to top-level domains (such as .com, .net, or .org) or country-code domains (.ca, .cn) at the second level (Figure 3).

The technical function and intermediary role provided by authoritative DNS servers have privacy implications. As part of the resolution process, the DNS passes query information through the DNS hierarchies to various authoritative name servers, which direct users to the IP address they are querying. A key issue in DNS privacy is that requests include the full "Query Name" for each recursive query. Thus, each authoritative name server queried across the DNS hierarchy would know the URL of the website the user was seeking.

Although authoritative name servers are limited in their observational abilities because of caching, they are still able to see some Internet queries. According to Internet RFC 7626, "this subset of information may be sufficient to violate some privacy expectations" especially given the concentration of authoritative name servers among popular domains (Bortzmeyer, 2015). For example, among the world's most popular websites listed in the Alexa Top100k, Amazon's DNS servers host 10 percent of Internet domains (Vinot, 2015). As Internet RFC 7626 notes: "With the control (or the ability to sniff the traffic) of a few nameservers, you can gather a lot of information" (Bortzmeyer, 2015).

With recursive resolvers, there is typically a terms of use agreement between the provider (whether an ISP or a third party) and the user. Although these

agreements can be vaguely worded and might not contain specific information about query data, most recursive resolution providers lay out some provisions surrounding the use of customer data, and must adhere to national data protection and privacy laws. However, most users will have no control or awareness of the role of the authoritative name servers and their observational abilities, and no direct contractual agreements to afford user protection.

Ongoing Debates Surrounding DNS Queries

The Internet's technical community is aware of the confidentiality challenges around DNS resolution. This section is not an exhaustive technical treatment of either the problems or the many possible solutions to privacy challenges in DNS queries, but it starkly emphasizes the technical complexities around these issues and why they are often concealed, albeit not intentionally, from public discourse.

Several IETF initiatives have identified challenges for privacy in the DNS and ways to enhance confidentiality in the query process. In 2014, the IETF formed the DNS Private Exchange (DPRIVE) working group to develop "mechanisms to provide confidentiality to DNS transactions, [and] to address concerns surrounding pervasive monitoring" (DPRIVE, 2018). The DPRIVE working group is primarily concerned with finding technical solutions to privacy issues that occur between the user and resolver, but, later, may consider mechanisms for improving privacy between resolvers and authoritative servers (DPRIVE, 2018). Other technical initiatives involve developing new protocols that would encrypt DNS packets. During the 2014 IETF-89 London meeting, a Birds of Feather session titled "Encryption of DNS Requests for Confidentiality" was held to discuss the strengths and limitations of new protocols that would encrypt DNS requests (IETF, 2014). Many of these technical solutions, such as "Confidential DNS" or "TLS for DNS," are still being discussed and have not been implemented across the network (Hogg, 2016). However, the DNS requires privacy-specific extensions. As mentioned, significant strides have been made to improve the security of the DNS—especially through the development and implementation of DNSSEC. However, this extension will not address the privacy issues raised in this article.

At the moment, users are left with very few technical options for protecting their confidentiality in DNS queries. For technologically informed individuals, options such as alternative or proxy servers, the Tor network, or properly configured virtual private networks (VPNs) can be used to enhance their privacy when making DNS queries, or a third-party DNS resolver can be configured. But these solutions alone do not mitigate all of the risks to privacy at various points in the DNS resolution process, such as unencrypted DNS data or requests made to authoritative name servers. Furthermore, all of the technical solutions currently proposed address limitations to how data is transferred and moved through the query process, but they do not address questions to do with data at rest or how it is collected, stored, and processed by the various actors in the DNS ecosystem. For this, best practices and privacy policies need to be in place. Although there have been best practices developed for operating DNS servers (Dickinson, 2018), no standardized solutions to

DNS privacy have been implemented. Instead, users must rely on the privacy policies of their ISPs, alternative name servers, or proxy resolvers to protect their privacy online. However, both the market and national jurisdictions remain highly fragmented in terms of the level of privacy recursive resolvers provide to users.

Conclusion: Connecting Privacy to Free Speech and Security

The public policy issues instantiated in the Internet's core systems of infrastructure help emphasize that privacy is about more than just protecting the content that flows over the Internet's infrastructure. It is also about the Internet's technical architecture itself and the ways in which it is designed, administered, and regulated. The engineering considerations made (or not made), and implemented (or not implemented) around privacy can raise different types of harms to individuals and to society, ranging from financial damage, reputational injury, threats to personal safety, chilling effects on free speech and democratic deliberation, economic exploitation, and system disruption.

In the case of domain name registration policy, privacy is often not just about personal safety and reputation. The publication of a registrant's name, home address, phone number, and email address raises obvious concerns about the potential for stalking, threats, spam, and harassment. But it also shapes what counts as freedom of expression online. In democratic societies, there has always been a close association between the possibility of anonymity and the prospects for free expression. This is certainly the case with domain name registration because of the nature of the personal information collected, which includes offline identity and one's physical address. In a similar vein, DNS query data contains sensitive information-seeking practices and metadata that can reveal a user's identity and preferences. One could glean the kinds of websites a user visits, including sensitive searches for services, and metadata surrounding lookups could provide insight into how long someone visits a website, when they are home, and how many people are in the house.

This article also makes clear the links between privacy and security concepts. RFC 6973 "Privacy Considerations in Internet Protocols" emphasizes the many types of privacy issues associated with security threats, including surveillance, unauthorized access to stored data, and misattribution attacks that falsely authenticate information (Hansen et al., 2013). Within the DNS, the close connection between privacy and security is no different. DNS query data can be monitored and spoofed to launch a man-in-the-middle attack to commit fraud or identity theft, or to identify the usage patterns of an individual or tell when they are away from home, opening up opportunities for more physical threats to property or to personal security. Finding solutions to these interwoven challenges will require an approach that considers both privacy and security values, such as confidentiality, data integrity and verification. And solutions that address security issues alone will not be enough. We recommend that privacy-specific extensions, such as those designed to encrypt DNS records, will be necessary for protecting against passive monitoring of the DNS. With ongoing innovation in the Internet of Things, these design choices

become ever more important, as more objects connecting to the network create more vulnerability or points for data collection and analysis.

Thus far, there is far more public debate about information security and data protection at the level of Internet content than at the level of infrastructure and the DNS. While many privacy frameworks apply to protecting the content of communications from surveillance, unauthorized access, or breach, they have not necessarily been analyzed in the context of Internet infrastructure and the DNS. Similarly, the legal regime surrounding data protection and privacy has just begun to develop. There are no clear or precise laws on DNS data protection, and it is unclear how the various national, regional, or global principles on data protection would apply in a legal context. There is also little transparency or consistency surrounding how DNS data is collected, analyzed, used, and sold. In the case of domain name registration, hundreds of different registrars collect and publish personal information in a variety of formats in the WHOIS database. Some offer proxy services to their customers, but others do not allow users to register websites without providing their personal information for publication. In the case of DNS queries, ISPs or other third-party resolution servers also provide very little information on how query data is collected, stored, processed, and shared. We recommend that best practices be developed and implemented for the collection, analysis, use, and storage of DNS records. Recursive name server operators should be required to have a privacy policy that has clear guidelines for the collection, use, and storage of query data. Given that the transactions that occur over the Internet and the associated metadata can expose just as much sensitive information as the actual content, it is important that privacy in the Internet's infrastructure be lifted into mainstream discussions on protecting user privacy online.

Samantha Bradshaw, M.A., Doctoral Candidate, Information, Communication and the Social Sciences, Oxford Internet Institute, University of Oxford, Oxford, United Kingdom [sam.r.bradshaw@gmail.com].

Laura DeNardis, Ph.D., Professor, School of Communication, American University, Washington DC.

Notes

1. Due to the limited number of globally unique IP addresses (resulting from the IPv4 standard which only creates approximately 4.3 billion unique numbers), address sharing via Network Address Translation is common. This, however, still requires a globally unique IP address.
2. Pronounced "Who Is."

References

Alternate DNS. 2016. *Alternate DNS—Privacy*. https://alternate-dns.com/privacy.html.

APNIC. 2017. *Definition of Registration Data Access Protocol*. https://www.apnic.net/about-apnic/whois_search/about/rdap.

Bortzmeyer, S. 2015. *DNS Privacy Considerations*. RFC 7626. https://tools.ietf.org/html/rfc7626.

Bradshaw, S., and L. DeNardis. 2018. "The Politicization of the Internet's Domain Name System: Implications for Internet Security, Universality, and Freedom." *New Media & Society* 20 (1): 332–50.

Braman, S. 2011. "Privacy by Design: Networked Computing, 1969–1979." *New Media & Society* 14 (5). https://journals.sagepub.com/doi/abs/10.1177/1461444811426741?journalCode=nmsa.

Bruen, G.O. 2015. *WHOIS Running the Internet: Protocol, Policy, and Privacy*. Hoboken, NJ: Wiley.

Cath, C., and L. Floridi. 2017. "The Design of the Internet's Architecture by the Internet Engineering Task Force (IETF) and Human Rights." *Science and Engineering Ethics* 23 (2): 449–68.

Cisco. 2018. *Cisco Online Privacy Statement—Cisco*. https://www.cisco.com/c/en/us/about/legal/privacy-full.html.

Cloudflare. 2018. *1.1.1.1—The Internet's Fastest, Privacy-First DNS Resolver*. https://1.1.1.1/.

Cohen, E., and H. Kaplan. 2000. "Prefetching the Means for Document Transfer: A New Approach for Reducing Web Latency." *IEEE INFOCOM Conference*. http://www.cs.tau.ac.il/~haimk/papers/prefetch.ps.

Comodo. 2018. *Privacy Policy*. 2018. https://www.comodo.com/repository/Comodo-Privacy-Policy-(05252018).pdf.

Conrad, D. 2012. "Towards Improving DNS Security, Stability, and Resiliency." *Internet Society*. https://dev.www.isocdev.org/towards-improving-dns-security-stability-and-resiliency-0.

Conroy, L., K. Fujiwara, and S. Bradner. 2011. *The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)*. RFC 6116. https://tools.ietf.org/html/rfc6116.

Daigle, L. 2004. *WHOIS Protocol Specification*. RFC 3912. https://tools.ietf.org/html/rfc3912.

DeNardis, L. 2014. *The Global War for Internet Governance*. New Haven, CT: Yale Unviersity Press.

Dickinson, S. 2018. "Recommendations for DNS Privacy Service Operators." Internet Draft. https://tools.ietf.org/pdf/draft-dickinson-bcp-op-00.pdf.

DNS Watch. 2018. *Fast, Free and Uncensored. DNS.WATCH.—DNS.WATCH*. https://dns.watch/why.

DPRIVE. 2018. *DPRIVE Charter*. https://tools.ietf.org/wg/dprive/charters.

Dyn. 2018. *Oracle's Privacy Policy*. https://dyn.com/legal/dyn-privacy-policy/.

Elliott, K. 2009. "The Who, What, Where, When, and Why of WHOIS: Privacy and Accuracy Concerns of the WHOIS Database." *Science and Technology Law Review* 12 (141): 33.

Epstein, D., C. Katzenbach, and F. Musiani. 2016. "Doing Internet Governance: Practices, Controversies, Infrastructures, and Institutions." *Internet Policy Review* 5 (3). https://policyreview.info/articles/analysis/doing-internet-governance-practices-controversies-infrastructures-and-institutions.

Expert Working Group. 2014. *Final Report from the Expert Working Group on GTLD Directory Services: A Next-Generation Registration Directory Service (RDS)*. June 6. https://www.icann.org/en/system/files/files/final-report-06jun14-en.pdf.

Feamster, N. 2016. "What Your ISP (Probably) Knows About You." *Freedom to Tinker*. https://freedom-to-tinker.com/2016/03/04/what-your-isp-probably-knows-about-you/.

FreeDNS. 2018. *FreeDNS—Your Open DNS*. https://freedns.zone/en/.

General Data Protection Regulation. 2018. *Principles Relating to Processing of Personal Data*. http://www.privacy-regulation.eu/en/article-5-principles-relating-to-processing-of-personal-data-GDPR.htm.

Google. 2012. "Google Public DNS: 70 Billion Requests a Day and Counting." *Official Google Blog* (blog). February 14. https://googleblog.blogspot.com/2012/02/google-public-dns-70-billion-requests.html.

Google. 2015. *Public Comment on GNSO Privacy & Proxy Services Accreditation Issues Working Group Initial Report by Google*. https://forum.icann.org/lists/comments-ppsai-initial-05may15/pdfsWcMcbo6mh.pdf.

Google. 2016. "Your Privacy|Public DNS." *Google Developers*. https://developers.google.com/speed/public-dns/privacy.

Grover, S., M.S. Park, S. Sundaresan, S. Burnett, H. Kim, and N. Feamster. 2013. "Peeking Behind the NAT: An Empirical Study of Home Networks." *Proceedings of the 13th ACM Internet Measurement Conference*. https://dl.acm.org/citation.cfm?id=2504736.

Hallam-Baker, P. 2014. "DNS Privacy and Censorship: Use Cases and Requirements." Internet Draft. https://tools.ietf.org/html/draft-hallambaker-dnse-01.

Hansen, M., J. Morris, A. Cooper, R. Smith, H. Tschofenig, J. Peterson, and B. Aboba. 2013. *Privacy Considerations for Internet Protocols*. July. https://tools.ietf.org/html/rfc6973.

Harrenstien, K., M. Stahl, and E. Feinler. 1985. "NICNAME/WHOIS." RFC 954. https://www.ietf.org/rfc/rfc954.txt.

Hogg, S. 2016. *IETF Proposed Solutions for Improved DNS Privacy (Part 2 of 2)*. https://community.infoblox.com/t5/IPv6-Center-of-Excellence/IETF-Proposed-Solutions-for-Improved-DNS-Privacy-Part-2-of-2/ba-p/5472.

ICANN. 2013. *ICANN Registrar Accreditation Agreement*. June 27. https://www.icann.org/en/system/files/files/approved-with-specs-27jun13-en.pdf.

ICANN. 2015. *Initial Report on the Privacy & Proxy Services Accreditation Issues Policy Development Process*. 2015. https://gnso.icann.org/sites/default/files/filefield_47597/ppsai-initial-05may15-en.pdf.

ICANN. 2018. *Temporary Specification for GTLD Registration Data*. https://www.icann.org/en/system/files/files/gtld-registration-data-temp-spec-17may18-en.pdf.

IETF. 2014. *Encryption of DNS Requests for Confidentiality (DNSE) (BOF)*. https://www.ietf.org/proceedings/89/dnse.html.

Koch, P. 2013. "Confidentiality Aspects of DNS Data, Publication, and Resolution." Internet Draft. https://tools.ietf.org/html/draft-koch-perpass-dns-confidentiality-00.

Krishnan, S., and F. Monrose. 2010. "DNS Prefetching and Its Privacy Implications: When Good Things Go Bad." *LEET 10 Proceedings of the 3rd USENIX Conference on Large-Scale Exploits and Emergent Threats: Botnets, Spyware, Worms and More*. https://dl.acm.org/citation.cfm?id=1855696.

Larson, M., D. Massey, S. Rose, R. Arends, and R. Austein. 2005. *DNS Security Introduction and Requirements*. March. https://tools.ietf.org/html/rfc4033.

Level 3. 2018. *Privacy Policy*. http://www.level3.com/en/privacy/.

MacKinnon, R. 2012. *Consent of the Networked*. New York: Basic Books.

Malcolm, J., and M. Stoltz. 2015. "Changes to Domain Name Rules Place User Privacy in Jeopardy." *Electronic Frontier Foundation*. June 23. https://www.eff.org/deeplinks/2015/06/changes-domain-name-rules-place-user-privacy-jeopardy.

Mockapetris, P. 1987a. *Domain Names—Concepts and Facilities*. RFC 1034. https://www.rfc-editor.org/rfc/rfc1034.txt.

Mockapetris, P. 1987b. *Domain Names—Implementation and Specification*. RFC 1035. https://www.rfc-editor.org/rfc/rfc1035.txt.

Mueller, M. 2010. *Networks and States: The Global Politics of Internet Governance*. Cambridge, MA: MIT Press.

Mueller, M., and M. Chango. 2008. "Disrupting Global Governance: The Internet Whois Service, ICANN, and Privacy." *SSRN* Scholarly Paper ID 2798940, Social Science Research Network, Rochester, NY. https://papers.ssrn.com/abstract=2798940.

Neustar. 2017. *Neustar Privacy Center*. https://www.home.neustar/privacy/privacy-policy.

Newton, A. 2006. "Replacing the Whois Protocol: IRIS and the IETF's CRISP Working Group." *IEEE Internet Computing* 10 (4): 79–84.

Norton. 2018. *Norton ConnectSafe*. https://dns.norton.com/privacy.html.

Quad 9. 2018. "Privacy, Data Collection and Use Policy." *Quad 9* (blog). https://www.quad9.net/policy/.

SafeDNS. 2015. "Privacy Policy." *SafeDNS*. https://www.safedns.com/en/privacy-policy/.

SmartViper. 2018. *Smart Viper*. http://www.markosweb.com/policy/.

Souders, S. 2013. *Prebrowsing*. https://www.stevesouders.com/blog/2013/11/07/prebrowsing/.

Stark, E., L.-S. Huang, and D. Israni. 2012. "The Case for Prefetching and Prevalidating TLS Server Certificates." *NDSS* 12. http://crypto.stanford.edu/~dabo/pubs/abstracts/ssl-prefetch.html.

Swire, P., J. Hemmings, and A. Kirkland. 2016. "Online Privacy and ISPs: ISP Access to Consumer Data Is Limited and Often Less Than Access by Others." Institute for Information Security & Privacy, Georgia Tech., Atlanta, GA.

US Judiciary Committee. 2001. *WHOIS Database: Privacy and Intellectual Property Issues*. http://commdocs.house.gov/committees/judiciary/hju73612.000/hju73612_0f.htm.

Verisign. 2015. "Protect Your Privacy – Opt Out of Public DNS Data Collection." *CircleID*. October 20. http://www.circleid.com/posts/20151029_protect_your_privacy_opt_out_of_public_dns_data_collection/.

Verisign. 2018. *Verisign Privacy Statement*. https://www.verisign.com/en_US/privacy-statement/index.xhtml.

Vinot, N. 2015. "Vie Privée: Et Le DNS Alors?" *Null Pointer Exception* (blog). https://blog.imirhil.fr/2015/02/18/vie-privee-dns.html.

White, V., and K. Harrenstien. 1982. *NICNAME/WHOIS*. RFC 812. https://tools.ietf.org/html/rfc812.

Zittrain, J. 2008. *The Future of the Internet: And How to Stop It*. New Haven, CT: Yale University Press.