Journal of Cyber Policy

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/rcyb20

Consolidation in the DNS resolver market – how much, how fast, how dangerous?

Roxana Radu & Michael Hausding

To cite this article: Roxana Radu & Michael Hausding (2020) Consolidation in the DNS resolver market – how much, how fast, how dangerous?, Journal of Cyber Policy, 5:1, 46-64, DOI: 10.1080/23738871.2020.1722191

To link to this article: https://doi.org/10.1080/23738871.2020.1722191

Published online: 04 Feb 2020.

JOURNAL OF CYBER POLICY
2020, VOL. 5, NO. 1, 46–64
https://doi.org/10.1080/23738871.2020.1722191

Routledge
Taylor & Francis Group

Consolidation in the DNS resolver market – how much, how fast, how dangerous?

Roxana Radu[a] and Michael Hausding[b]

[a]Centre for Socio-Legal Studies, University of Oxford, Oxford, UK; [b]Internet Society Switzerland Chapter, Zurich, Switzerland

ABSTRACT

Almost all online services use a domain name resolution function to translate names typed by the user into numbers that computers understand. This basic, recursive function, performed in milliseconds and invisible to the user, was integrated from the beginning into the operation of Internet Service Providers (ISPs). This started to change with the advent of new players – such as Google, Cloudflare, Oracle – operating public resolvers and rendering the market more dynamic in the last decade. As more technologies are developed to increase the privacy and security of the domain name system (DNS) protocol, large internet companies with global operations appear better equipped to integrate the latest requirements and offer their services free to users and ISPs, further consolidating their position in the market. This article provides a timely analysis of the emerging trends of consolidation in the recursive DNS services market, focusing on its evolution in the last decade and discussing empirical evidence for the shifts occurring from 2016 to mid-2019.

ARTICLE HISTORY
Received 15 August 2019
Revised 31 December 2019
Accepted 6 January 2020

KEYWORDS
Domain name system (DNS); market consolidation; internet ecosystem; DNS resolvers; public resolvers; internet service providers (ISPs)

Introduction

Despite the recent policy focus on the consolidated position of internet giants and the public debate around their potential 'break up' in the US, or sanctioning and taxing them in the EU, not all parts of the market appear to be subject to close scrutiny. The emerging trend of consolidation in the recursive Domain Name System (DNS) services market is a case in point here. This article provides an analysis of the changes taking place in this market, focusing on its evolution in the last decade and discussing empirical evidence for the consolidation shifts occurring from 2016 to mid-2019.

To resolve domain names to IP addresses, most internet services such as web, email, chat, etc. need a basic infrastructure known as DNS resolvers. Historically, DNS resolvers were operated by internet service providers (ISPs) and automatically provisioned by the ISP on the users' devices via the Dynamic Host Configuration Protocol (DHCP).[1] This started to change with the advent of new players – such as Google, Cloudflare, Oracle etc. – operating public DNS resolvers and rendering the market more dynamic since 2009. As more technical standards are developed to increase the privacy and security of

the DNS protocol,[2] large internet companies with global operations appear better equipped to integrate the latest features and provide their services to local ISPs, further consolidating their position in the market. Most of these companies offer their public DNS free of charge, together with a range of improvements on speed, reliability, privacy and security (Nykolas 2018a), making their services attractive to end users. ISPs who configure these resolvers for their users via DHCP have the additional economic benefit of no longer bearing the cost of operating their own resolvers. Alongside these technical drivers, regulatory pressure on ISPs in certain countries and the possibility of circumventing censorship via alternative resolvers might help to consolidate the position of a few companies. Whereas a larger market share is not problematic in itself, the speed and scale of the shifts and the effects they have on the global internet ecosystem require closer scrutiny.

Starting from these assumptions, this research adopts an evidence-informed approach and aims to answer the following question: what are the shifts occurring in the recursive DNS market and what is the extent of consolidation? On the regulatory side, it integrates a key discussion of the effectiveness of governmental policies mandating network blocking in light of the changes observed in the DNS resolution. There is limited and rather scattered research on this topic, partly obscured by restricted access to data in what has become a two-sided market. We aim to close this gap by providing an empirical analysis estimating the usage of public resolvers vs. resolvers run by ISPs, based on publicly available data from the Open Observatory of Network Interference (OONI). We use active measurements on mobile platforms and OONI probes, advancing a new perspective on the consolidation dynamics observed in the market when considering the prevalent access pattern.

The remainder of this article is divided as follows. The first part investigates the changes occurring over time in the management of DNS resolvers, noting the emergence of competition between ISPs and new market players in the last decade, as well as the shifts in their roles. The second part provides a measurement of the market concentration and an analysis of the trends noticed. The final part concludes with a discussion of the findings and the effects they have on the future development of the internet.

The DNS market over time

The DNS is essential to the operation of the internet: it maps domain names that users can remember to Internet Protocol (IP) addresses that computers use to locate the information sought. Cloud services and content delivery networks all rely on the DNS, making the web experience as we know it today highly dependent on a technical functionality that has remained hidden in the technical layer and relatively abstruse in public discussion. With the exception of the political negotiations around the domain name registration system – in particular the creation and subsequent reform of the Internet Corporation for Assigned Names and Numbers (ICANN), the non-profit private American corporation that oversees the management of the DNS (Mueller 2004; Radu 2019) – the dynamics in the domain name market and its recent concentration trends have not received enough scholarly attention. Significant exceptions include recent studies by Borgolte et al. (2019) and Huston (2019), who started to shed light on effects that go beyond the technical aspects, assessing legal, economic and political consequences.

The domain name management evolved from a central list (maintained single-handedly by Jon Postel) into an automated hierarchical database around which a significant

global market gravitates nowadays. In the early days of ARPANET, the predecessor of the current internet, a text file called *hosts* was keeping track of the addresses assigned manually for about 300 computers connected in the network. It was maintained by Elizabeth Feinler at the Stanford Research Institute, in close collaboration with Jon Postel at the Information Sciences Institute, University of Southern California, who maintained the equivalent list for numerical addresses (Assigned Numbers List). This worked well until the 1980s, but as the number of computers grew, a faster and scalable solution was sought. A hierarchical system, the DNS, was introduced in 1983 by Paul Mockapetris and Jon Postel to offer an authoritative way to translate human-friendly (easy-to-remember) computer host names (such as example.com) into IP addresses (corresponding string of numbers), thus locating web pages and services within milliseconds. The process is almost invisible to the user and simultaneously available for other users on multiple devices.

Distributed on millions of computers around the world, the DNS is a hierarchical database that receives and answers trillions of queries every day. The DNS is split into two separate functions, authoritative servers and recursive resolvers that together can resolve domain names into IP addresses. The authoritative servers keep and serve authoritative data about a limited number of zones,.com for example, to recursive servers. Recursive resolvers accept (non-recursive) queries from internet devices such as servers, personal computers, mobile devices or IoT devices and return a response. To get the data for the response, they query the authoritative servers recursively until they have an answer to the client's query or discover that the domain name does not exist. They keep the answer for a given time-to-live (TTL) in a local cache to speed up further queries for the same domain name and answer these queries directly from their cache. This is why recursive resolvers are also called caching resolvers.

The recursive resolving part of the DNS, which is the focus of this article, can be viewed as its own sub-market. With nearly 4 billion internet users and even more servers, mobile- and IoT-devices requesting a DNS resolution service, the demand is high and continuously growing. On the supplier side there are at least 10 million recursive DNS servers (ICANN 2012) able to deliver that service. Historically, the market is highly competitive, as the service is standardised by the DNS protocol and the entry barrier to run a DNS resolver is low. While tech-savvy users can easily compare service quality and switch to a different DNS resolver through a configuration change on a device or a router, that option might not be a given for the majority of internet users (Open Rights Group 2019, 17).

Since 2009, there have been many players that provide alternative (also known as 'public') DNS resolvers. Among these, some are specialised in DNS resolution, such as DNS.Watch and Quad9, while others are network infrastructure operators (e.g. Verisign, Cisco), internet services companies (e.g. Google, Yandex) or internet security firms (Norton, Comodo Cybersecurity, etc.). While the services are offered free to end users by most players in this market, they require a premium for enterprise activities. This business model is characteristic of a two-sided market, in which the process of intermediation changes in accordance with the group served. The alternative DNS market provides a wide array of options to users, from no censorship to optional content filtering and from limited to enhanced privacy protections. To enterprises, the same company would provide threat intelligence, network analysis and cyberdefence drawing on the data collected by its public resolvers.

Although trends of ISP market power consolidation have been observed (in particular in the US), there is no cumulative research in this field. An OECD report (2010) pointed to broadband subscriptions and mobile internet access services as the main growth sectors at that time. Recognising the changes in the overall internet economy, the Internet Society 2019 Global Internet Report notes that DNS resolution is currently provided by a small number of players. Moreover, 'DNS protocols are even changing in a way that reinforces this trend' (Internet Society 2019, 4). According to Hoffmann (2019), Google is 'one of eight companies that currently resolves half of global Internet traffic'. Two recent empirical studies have pointed to the dominant position of one player. In his analysis from April 2018, Nykolas Z notes the strong position of Google's Public DNS with about 13 per cent of the DNS traffic in the measurement. Second came OpenDNS, with about 2 per cent of the market share. The latest market entries, Quad9, launched in November 2017, and Cloudflare (launching its 1.1.1.1 service on 1 April 2018), both had around 0.12 per cent of the total usage. The analysis was based on anonymized logs from an authoritative DNS provider with over 11,000 domains, including a total of 30,485,500 DNS requests. Huston's analysis from September 2019 concludes that Google is 'the dominant Open DNS provider across the entire Internet, while other providers appear to be used on a regional basis'.

As important as these insights are, there is a limited comparability of results due to differences in methodology. The absence of standardised public metrics means that every group of researchers starts from scratch on a new dataset, allowing for limited cross-fertilisation in studies covering similar DNS resolution aspects or looking at name-to-address mappings across various platforms. In that respect, the mobile market has received very little attention (mostly in blogs), despite the fact that there have been more users on mobile platforms than on desktop since 2016. As of April 2019, there were 4 billion unique mobile phone users (Statista 2019). Our analysis is the first to take into account mobile access and related market changes, based on empirical evidence.

The role of internet service providers

The traditional role of the ISP in the DNS system is to provide recursive name servers (resolvers) that can be used by its clients to resolve domain names to IPs to access the internet. The same is true for mobile operators that offer IP services for their mobile users: they provide a DNS resolver and configure it on the subscribers' mobile devices. Even though there was no requirement that ISPs run resolvers, they had to offer this service so that their clients could use the internet. There are thousands of ISPs around the world. In the US alone, their number exceeds 2,645 (BroadbandNow 2019), whereas the pan-European association of the ISP industry counts more than 2,300 ISPs of different sizes across the European Union and the European Free Trade Area (EuroISPA 2019).

ISPs perform several underlying roles that are not clearly differentiated in the many definitions put forward (OECD 2010), including access provision, hosting, etc. The most common understanding is that of a provider of a data connection for subscribers' internet access through a physical transport infrastructure (OECD 2004). An ISP can operate at the local, regional or national level; its clients may include individuals (households), businesses and governments. Its business model revolves around a monthly subscription for network connectivity (generally 'unlimited') and related services.

A few sets of upgrades have occurred over the years to bring us to the current DNS in use in most online applications, which have themselves evolved from static to highly dynamic content delivery. A first set of changes regarded security, which was not integrated into the original design of the network due to its access being restricted to a handful of scientists in the early days. When public access to the internet expanded exponentially, the many vulnerabilities of the DNS system, including spoofing, cache poisoning, denial-of-service attacks, etc., became obvious. These changes raised the level of expertise that DNS resolver operators needed to have to operate a secure and resilient service. In 2013, Edward Snowden's revelations of mass surveillance by intelligence agencies also triggered a focus on privacy-enhancing protocols, including at the DNS level, in the technical community.

Given the fact that resolvers were historically run by ISPs to answer queries from their network, the market share of resolvers before the entry of public DNS resolvers can be estimated to be similar to the overall ISP market share. While residential users continued to rely on their ISP, or a public resolver, to deliver the DNS resolver service, SMEs and enterprise users discovered the importance of DNS and implemented their own DNS resolver. This is also due to the need to integrate internal network resources in the DNS resolution for the organisation. Requests for internal resources are answered from the resolver who has access to a local database, while requests for external domain names are resolved recursively or forwarded to a recursive resolver.

New players

Like many other services on the internet, name resolution is a service that can be operated by anyone with some basic technological skills. This low entry barrier has brought a host of new players to the DNS market in the last decade, whose competitive advantage consisted in security improvements and user-experience optimizations. Additional features often include protection from manipulation of DNS answers or filtering of unwanted or criminal content on the internet like phishing, malware or pornographic content. Their business model is built around data collection and intelligence trends and most of these players offer a basic DNS resolver service free to the public. They are thus referred to as 'public resolvers' and are available to both individual users and ISPs and enterprises. Irrespective of whether they are manually configured on devices or an outsourced service, public DNS services are free of charge and offer the possibility of circumventing DNS-based censorship.

When Google introduced its Public DNS in December 2009, there were two other competitors on the market: UltraDNS, a Neustar-acquired company, and OpenDNS. They were both introduced in 2006 and promised a faster look-up and better protection against online fraud. OpenDNS, the seven-person start-up from California led by David Ulevitch, initially operated an ad-supported service for non-existent domains (until 2014), and extended to enterprises as a paid, advertisement-free service in 2009. Their business models were relatively similar, with a premium service for large corporations and a free service for end users, but their share of the market remained small. By June 2008, OpenDNS was handling around 7 billion queries a day (Zetter 2008).

Google entering the market was a game-changer. By 2018, Google Public DNS answered over 1,200 billion queries a day, serving 'hundreds of millions of people' according to the Google Security Blog (2018). Today, that number would be many times greater

as Google's service grew to be the 'largest and most well-known DNS service in existence' (de Vries et al. 2019). Its continuous growth was anticipated and feared from the start. At the launch of Google's DNS, the CEO of OpenDNS warned about the danger of concentrating many services into a single hand:

> It's not clear that Internet users really want Google to keep control over so much more of their Internet experience than they do already – from Chrome OS at the bottom of the stack to Google Search at the top, it is becoming an end-to-end infrastructure all run by Google, the largest advertising company in the world. I prefer a heterogeneous Internet with lots of parties collaborating to make this thing work as opposed to an Internet run by one big company. (cited in Singel 2009)

With the advent of alternative DNS resolution, there has been a shift towards a two-sided market that is currently flourishing. Two-sided markets include two distinct user groups with diverse interests that receive benefits in economies of scale through the work of an intermediary. The value obtained by one group of users increases based on the number and quality of the other group. Intermediaries would thus work with different functionalities and adopt differentiated pricing strategies for supplying both sides of the market (OECD 2010). In the case of recursive DNS services offered for free, it is the data that is important, providing DNS resolver operators access to large amounts of information that reflects internet usage and the internet ecosystem at large, in particular information that enables them to identify new security threats (such as newly registered domain names), the exploitation of vulnerabilities and the occurrence of indicators of compromise. In turn, using the DNS intelligence for defending the network against phishing and malware renders the services better and more secure.

Network blocking

The strategic importance of DNS resolvers has been capitalised on by large market players, but has also been recognised by governments on various occasions. Certain governments have developed their own system for public sector use. The UK government, for example, has encouraged the deployment of its own free-to-use recursive resolver for public sector organisations, called the Protective Domain Name System, developed by the National Cyber Security Centre (NCSC) and implemented by Nominet UK. Other countries have played close attention to this technical feature for various national interests, including the suppression of political dissent. Laws that limit access to internet services and measures that lead to partial or complete blackout of the internet have been passed in a number of countries, democratic and authoritarian alike. In addition to network management measures against congestion and against vulnerabilities, DNS-blocking occurs for reasons as diverse as banning online foreign gambling in Switzerland, eliminating child abuse material in many European countries or limiting political speech in China.

Access to the DNS was a function initially performed by ISPs in an agnostic way, relying on a DNS resolver application and requests to the distributed authoritative DNS servers. By running the default DNS resolver, the ISP is in the traffic path and can monitor and control the internet traffic using its DNS servers. Although there were no specific policies linked to DNS lookup, ISPs were – and continue to be – bound by telecommunication regulations, such as confidentiality and privacy provisions, but also by national laws banning access to certain types of information. Paradoxically, one of the reasons why alternative DNS

resolvers might be preferred is their capacity to circumvent the legally-imposed limitations that ISPs would need to respect under national law.

Rather than a by-product of the services provided, fighting censorship might be an important branding point for certain DNS resolver companies, such as DNS.Watch. In their words, 'our resolvers only deliver uncensored records' (DNS.Watch 2019), highlighting in particular their small size as an advantage when governments try to block big(ger) alternative DNS resolvers. Others, such as OpenDNS, Comodo Secure DNS, Norton ConnectSafe, SafeDNS have branded themselves on their optional content filtering approach, giving the user the capacity to select the level of protection wanted at home. Offering additional security and control features around DNS resolution due to jurisdictional differences represents a clear advantage that ISPs might not be able to compete with.

ISPs can also team up with public resolver operators to escape the obligation of network blocking. Some ISPs and mobile operators have configured Google's Public DNS 8.8.8.8 via DHCP on the mobile subscribers' devices. While there are multiple reasons to configure public resolvers instead of ISPs-run ones, it is possible to identify instances in which a public DNS was introduced close to the date around which network blocking laws would come into effect. Salt, a mobile operator in Switzerland, switched to Google's 8.8.8.8 in early 2019, while the Swiss gambling law that required the blocking of unlicensed gambling sites came into effect on 1st July 2019. This example shows that network-blocking can influence the use of public DNS resolvers, leading, at least in part, to a loss of control points that can be regulated by national law.

Consolidation research

DNS resolvers have a high commercial value. Moves toward consolidation in this market started early, when UltraDNS was acquired by Neustar. The recent acquisitions of alternative DNS resolvers by big technology companies show that interest has continued to grow over the years. Cisco bought OpenDNS in 2015 for $635 million (Wilder 2015). It currently has over 90 million users and continues to operate under the same name for home use and as Cisco Umbrella for enterprises (OpenDNS 2019). It is presumed that Oracle bought Dyn in 2016 for more than $600 million, but the terms of the deal remained confidential (Business Insider 2016). In this space, only two DNS resolvers function as not-for-profits: OpenNic is user-owned and controlled; Quad9 is operated by a not-for-profit and it was founded by IBM, Packet Clearing House and the Global Cyber Alliance. Other models include sponsorship structures, such as for DNS.Watch which operates out of Germany, mainly backed by the German company IP-Projects. DNS.Watch also stands out as an exception for jurisdictional reasons, the majority of popular public DNS resolvers belonging to US-based companies.[3] This has consequences for the regulatory measures and safeguards that can be imposed, for example for users' privacy and security.

Ongoing work in the IETF Measurements and Analysis for Protocols Research Group and recent discussions in the IRTF Applied Networking Research Workshop and at the ACM Internet Measurement Conference show that the usage of public DNS resolvers has started to be closely watched. Most measurements of this usage, however, are done with web browsers or authoritative DNS servers, not on dedicated vantage points on mobile platforms. The latter are particularly relevant in this discussion, given the growing importance of mobile devices in accessing the internet. Our research covers

this gap, adding empirical evidence to the comparison of local DNS resolvers with third party resolvers.

Operators of public resolvers do not publish data regarding their number of users, but they might refer to the total number of queries handled daily when they introduce a new service. This limitation notwithstanding, there are different ways to estimate the overall market share of public resolvers. Measurements can be made passively by evaluating resolver queries on authoritative DNS Servers like the 'DNS Market Share Analysis' on Medium (Nykolas 2018b). Another method is active measurement by drafting special DNS queries to determine the upstream IP address of the query that indicates the resolver operator. This method is more accurate than using data from authoritative DNS servers where caching influences query numbers, but it is biased by the selection of the measurement points.

Measurement method

For this study we chose to evaluate publicly available data from the Open Observatory of Network Interference (OONI 2019a), a free TorProject software collecting and processing network measurements for the detection of network anomalies. OONI makes active measurements and stores the resolver configured on the system, as well as the upstream IP that effectively resolved the domain name. We evaluated 183,361,310 measurements from the OONI metadb (OONI 2019b) from 2016 to 2019 that had a valid 'dns_a.client_resolver' IP that was determined using a query to whoami.akamai.net. The measurements are global, but not evenly distributed.[4] The measurement is not representative for all DNS resolutions on the internet as it is limited to measurements from mobile devices and OONI probes. OONI users are tech-savvy and focused on measuring network interference and censorship, which makes the measurements biased as they have the know-how to change their DNS resolver. Even though the measurement is biased and the total numbers are not representative for all internet users, we see no evidence that the trend in the DNS resolver market is different for this user group. OONI provides us with a longitudinal perspective, analysing data over a longer period of time (2016–2019).

Findings

Our research questions revolved around how much market concentration there is, how fast it evolved and whether such a trend would be dangerous for the internet ecosystem. This section analyses our findings and it is split as follows: to answer the first two questions, we took into account the use of public resolvers versus DNS resolution provided by ISPs based on a comparative analysis of the data for 2016 and mid-2019. The risks triggered by the market trends observed warranted a separate discussion, presented in the second part of this section.

The DNS resolver market: public and highly concentrated

Based on measurements from 100,000 users of the OONI application at two different points in time, the popularity of public DNS resolvers increased tremendously from 2016 to 2019. Our analysis shows that, on mobile platforms, more than half of all

queries were handled by alternative DNS services in the first half of 2019. At that point, Google and Cloudflare answered 49.7% of the DNS queries from our measurement.

Compared to 2016, public resolvers appear to be the preferred way to handle DNS queries (see Table 1) across the world, even if providers like Yandex and OpenDNS have less than 0.1 per cent of the market. Three years ago, Google and OpenDNS ranked the highest among public resolvers, but their maximum market share was 15.4 per cent. Looking at the numbers for 2019, the leader of the market is Google Public DNS. The top alternative DNS providers all operate from the US, with the exception of Russia's Yandex, which comes fourth in our analysis. Comparing the market by entry year, we note that longevity does not necessarily make a big difference to this market, since resolvers introduced after 2016, such as the ones operated by Cloudflare and Quad9, rank second and third, respectively, in terms of use.

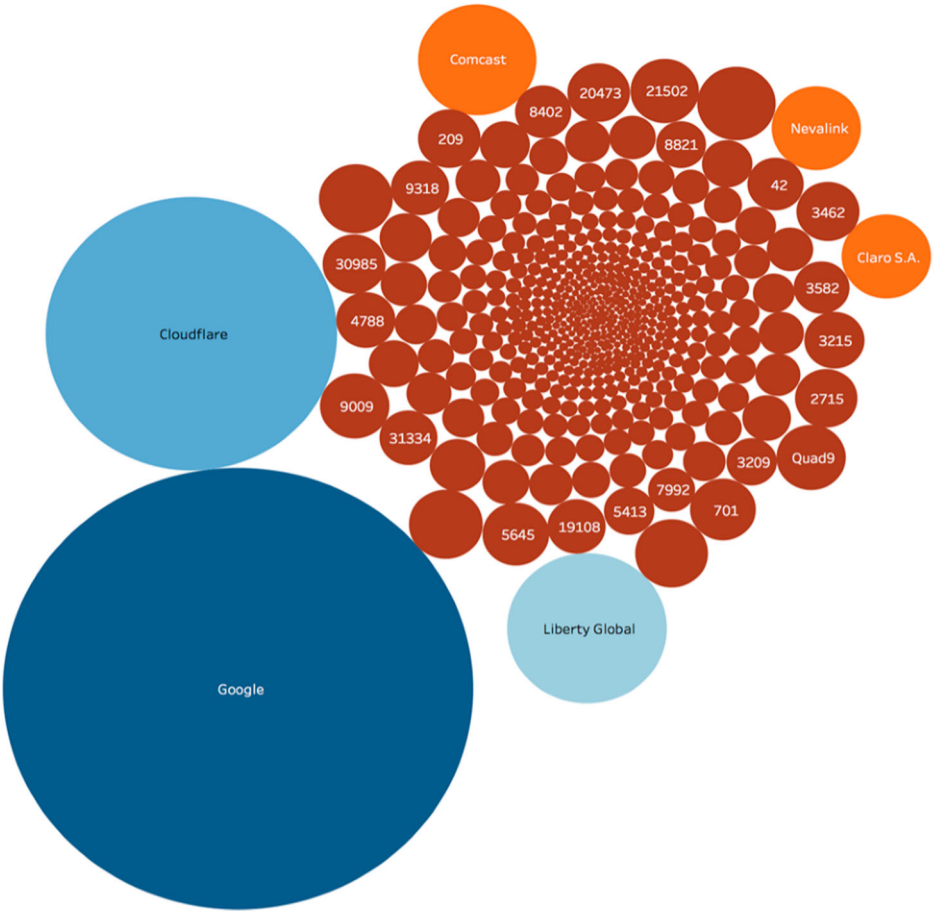
But how did we get here in three years? Rather than a majority of individual tech-savvy users manually configuring their systems to operate alternative DNS, we can assume that this shift in the market results from ISPs increasingly outsourcing DNS resolution to public providers, like Salt did in Switzerland in early 2019. As discussed above, the reasons for the *en masse* uptake of public resolvers include increased security, optimised speed and efficiency, the possibility of circumventing DNS-level censorship regimes, etc. If users decide to switch to other DNS resolvers themselves, for example following a local outage, the manual configurations remain in place long-term. A recent analysis (de Vries et al. 2019) showed that individuals switching to Google's Public DNS in the Netherlands following an outage tended to stay with that choice even after the service had been restored on their local ISP, Ziggo.

Consistent with earlier studies (Kesavan 2017; Nykolas 2018b), we find that the overall recursive DNS market is solidifying around Google's Public DNS. Their number of users continues to grow from year to year. Google was already the market leader in 2016, with 15.42 per cent of the market. Three years later, its market share grew 2.33 times, placing their DNS resolver in a dominant position. Its next competitor in 2019, with 13.80 per cent of the market, was Cloudflare's 1.1.1.1, which entered the market in April 2018. Built on the open-source Knot Resolver from CZ NIC, Cloudflare introduced this service as its first consumer-focused one (Guðmundsson 2018). Its impressive growth in a little over a year is linked to the strong reputation of Cloudflare in security and web performance services. If Google's coverage grew by 20.52 per cent between January 2016 and mid-2019, Cloudflare's evolution is equally impressive: almost 14 per cent of all measurements used Cloudflare's resolver in a little over a year since its release.

Our data allows us to compare alternative and ISP-based DNS services. As Graph 1 below shows, Liberty Global ranked the highest among ISPs with 4.16 per cent of the market in the first half of 2019, followed by Comcast and several other ISPs.

Table 1. Top open DNS resolver networks in first half of 2019.

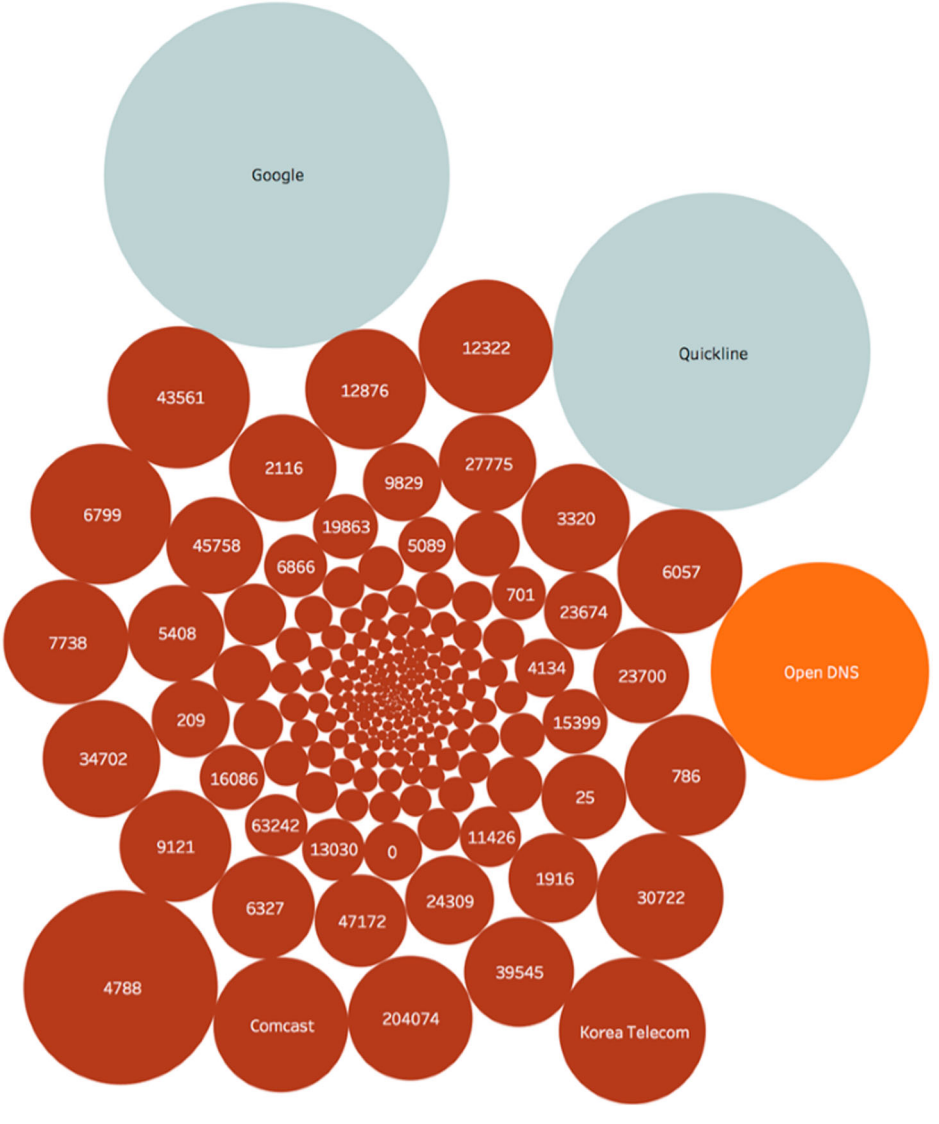
ASN	Name	Market entry	Share
15169	Google	2009	35.94%
13335	Cloudflare	2018	13.80%
715	Quad9	2017	0.78%
13238	Yandex	2013	0.09%
36692	OpenDNS	2006	0.03%
Total share of public resolvers			**50.64%**



Graph 1. Number of queries answered in the first half of 2019 by a resolver with an upstream IP from these ASNs.

Since 2016, the market has shifted significantly. Graph 2 shows us a fragmented picture of recursive DNS, in which a large number of players were competing for smaller portions of the market. Of these, about 5 had around 2.2 per cent of users, similar to Comcast, a long-standing American ISP providing broadband internet, cable television and telephone services, regularly enmeshed in scandals over its entertainment industry acquisitions and raising antitrust concerns (US Department of Justice 2015; Robertson 2018). As the largest provider of home internet in the US, it is interesting to note that their market share on mobile platforms remained constant over time.

In contrast to 2016, only 7 networks had a market share above 1 per cent by mid-2019. Whereas the majority of these are ISPs, their market share is low, ranging between 1 and 4.2 per cent, at a significant distance from public resolvers. Among ISPs, there is minimal variation in the share of DNS resolution over time: Claro increased from 0.54 per cent in 2016–1.29 per cent in 2019, while Korea Telecom dropped by 1.79 per cent from 2016. An interesting case is that of Liberty Global, whose presence increased significantly over time. A multinational operating in and outside the US, Liberty Global is known for its



Graph 2. Number of queries answered in 2016 by a resolver with an upstream IP from these ASNs.

broadband, cable and entertainment industry, following the acquisition of Virgin Media, Lionsgate and Cable & Wireless (Chuang 2016) between 2013 and 2016. By 2019, they served more than 10 million subscribers, of which 6 million were mobile customers. In our analysis, their increased market position represents an exception to the trends noted (Table 2).

Based on the data from the OONI, we see an indication of an ongoing consolidation between 2016 and mid-2019. However, as the measurements might be influenced by the mobility and the selection of networks by OONI users, changes in the measurements themselves and other unknown factors, we think that there is a need for more research to identify methods to accurately measure the absolute market share of DNS resolver

Table 2. DNS resolver top 10 networks in the first half of 2019 compared to 2016.

#	ASN	Name	2019	2016
1	**15169**	**Google**	**35.94%**	**15.42%**
2	**13335**	**Cloudflare**	**13.80%**	**0.00%**
3	6830	Liberty Global	4.16%	0.08%
4	7922	Comcast	2.28%	2.36%
5	42668	Nevalink	1.30%	0.00%
6	28573	Claro S.A.	1.29%	0.54%
7	4766	Korea Telecom	1.00%	2.79%
8	3356	Century Link	0.89%	0.51%
9	8447	Telekom Austria	0.88%	0.13%
10	45595	Pakistan Telekom	0.86%	0.00%
Total Market Share of Top 10			62.40%	
Total public resolvers in top 10			**49.74%**	

operators. Competition can change in nature and degree according to the extent of centralisation and concentration in the market, but such dynamics are difficult to capture with limited public statistics. Questions about the solidification of market positions around resolution services have only recently started to be asked, in part due to the absence of data and evidence, therefore regular, comparable measurements would go a long way in better understanding and addressing the trends we have observed here.

How dangerous?

The consolidation trends observed in our analysis and the insights from previous studies warrant a discussion of short- and long-term effects on the DNS resolution market. A first issue when studying centralisation in the DNS market is grasping the extent to which the resolver activities of internet giants such as Google remain separate or are integrated into its other services. As Geoff Huston (cited in Internet Society 2019, 19) puts it, 'the issue with consolidation is whether these activities remain discrete activities or whether they are being consolidated into a single service'. Sharing across platforms would constitute a competitive advantage likely to skew the market in favour of those holding leading positions and able to collect more data and monetise it. Looking at the publicly available information about the Google Public DNS, the only specification in regard to data-sharing refers to a commitment not to link the data to personal accounts and not to share outside Google services, unless asked by law enforcement authorities to do so. Sharing across Google platforms is, however, not at all addressed in the company's terms of service. According to its developers.google.com (2018), Google Public DNS stores temporary logs with the full IP address of the machine used for 24–48 hours and permanent logs for two weeks, with subsamples for indefinite time.

Beyond the punctual analysis of immediate outcomes, the long-term effects of these market dynamics are likely to manifest at different levels, from the configuration of the device itself to the overall internet ecosystem. The very robustness of the DNS system comes under challenge, as consolidation leads to a clustering of multiple risks, from technical to economic and political (jurisdiction, sovereignty, etc.). Moreover, if a public resolver fails or is inaccessible, the effects go beyond a single ISP. Trust in online services is thus a key component of the development and expansion of the internet. Ensuring a solid and competitive foundation for basic technical functions will matter when connecting the next billion users. Similarly to other network infrastructure sub-markets, the first-mover

advantage will count in the provision of recursive DNS services, with ISPs in developing countries less likely to compete directly with major alternative DNS providers.

Changes in user protection and in regulatory approaches

The biggest change in DNS resolution services is the amount of choice offered to internet users, whether mediated by an ISP, a browser or independently configured. Most public resolvers offer protection of privacy and enhanced security with DNS over TLS (DoT) and DNS over HTTP (DoH). A large number of top DNS resolvers present themselves as privacy-adherent. All public resolvers that stick to Mozilla's Security/DoH-resolver-policy (2019) have to offer QName Minimization and also protect their clients with DNSSEC validation from manipulated DNS responses, which is done by less than 25 per cent of all resolvers globally, according to the 'Use of DNSSEC Validation for World' by APNIC (2019). Many public resolvers like Quad9 or OpenDNS offer protection against malware and phishing.

On the other hand, users of public DNS resolver services need to trust the operator as there is less protection over what can be done with the users' data. The most popular public resolvers are operated by US companies and the users' data is often collected and processed outside the jurisdiction of the user. As these public DNS services are free for the end user, operators generate revenue from the collected data, which is a considerable risk for the privacy of the user. The move from an indirectly regulated market to an unregulated one is likely to reinforce the trends of continuous data collection and power concentration in the hands of a few companies.

Whereas ISPs had many obligations towards their clients under telecommunications and contract law (e.g. respecting the confidentiality of their clients' communication), the lack of oversight for alternative DNS services results in a shift towards a two-sided, unregulated market in which user privacy and the decentralised internet as a whole might be at stake. The global service providers of public DNS resolution services are not restricted in their practices by regulatory provisions, national control points or self-imposed codes of conduct and might respond to internal and external pressures in unpredictable ways.

At the other end of the spectrum, national regulators have mandated network-blocking at the DNS level to limit access to particular websites. The implementation of such a ban is delegated to local ISPs. Such a restriction may be circumvented by relying on public resolvers, at least until a ban or a technical manipulation occurs. Governments have made use of that in response to the redirection of traffic to Google's Public DNS. There are at least two instances of this: in 2017, the Taiwanese authorities threatened to impose a ban on Google's Public DNS for government operations on cybersecurity grounds (McCarthy 2007). In 2014, a political ban was imposed by the Turkish government, blocking access to the Google Public DNS around a Twitter ban ahead of municipal elections (Mihalcik 2014).

During the evaluation of the DNS data, we noted some irregularities for measurements that had configured Google's Public DNS (8.8.8.8) as a resolver. For these measurements the ASN of the upstream resolver was not always as expected in Google's AS15169. There were indications that in at least 230 networks, traffic to Google's Public DNS was redirected and answers were given from a resolver within the network. One effect of this redirection is that users who try to bypass network-blocking by using Google's DNS

resolver will not succeed and will get possibly filtered answers from a different resolver. This kind of redirection is no longer possible with DoH and DoT, as the transport mechanism is TCP and there is an authentication of the DNS resolver.

Changes in technology

When the DNS was developed there were almost no privacy considerations included in its design. Requests from clients to the resolver are still unauthenticated and unencrypted and can be surveilled to monitor the online activities of the users. This part of the DNS is also subject to interception and man-in-the-middle attacks, which can route users to fake websites for phishing or malware distribution. In recent years two different DNS protocol extensions tried to improve DNS privacy and security between the user and the resolver. The big public resolver operators have been the first to implement these technologies and we see that this is a strong motivation for users to switch to a public resolver.

DNS over TLS (DoT)

The first DNS privacy extension that was standardised in 2016 was DNS over TLS (DoT). The trigger was the disclosure of surveillance by state actors through the documents leaked by Edward Snowden. DoT introduced Transport Layer Security (TLS) for DNS running on port 853, encrypting the DNS queries and answers. The first global implementers were Cloudflare and Quad9.

DNS over HTTP (DoH)

The second DNS privacy extension, which was introduced by Google Public DNS in 2016 and standardised in 2018, was DNS over HTTP. DoH sends DNS queries and answers over HTTP using the Transport Layer Security of HTTPS to enable authentication and encryption. DoH makes it extremely difficult to filter DNS requests. With TLS 1.3 and encrypted Server Name Indication (SNI) the DNS traffic cannot be identified anymore and the only way to filter DoH is to block all HTTPS traffic on port 443. The collateral damage is that all web traffic to that operator is also blocked.

Applications doing DNS

DOH is not directly related, but goes along with applications, especially browsers, to circumvent the system stub resolver and send DNS queries directly from the application to a recursive resolver. This is also possible with plain DNS over UDP, but that can easily be detected and prevented on the network level. Applications that use a resolver other than the system stub resolver may cause inconsistency in DNS resolving and bypass security controls at the DNS level (DNS firewalls, DNS monitoring). While there are proposals to signal applications not to use an alternative resolver (Grover 2019), there is no easy way to enforce such behaviour at the moment.

DNS in the browser

The implementation of DoH at the application layer is still under discussion, but companies operating browsers have started taking action on it recently. Microsoft announced the use of DoH from the operating system without changing the server (Microsoft 2019), while Mozilla (in the US for now at least) changes the default resolver. Google's Chrome

upgrades to an encrypted protocol, but keeps the configured resolver (Google Chrome 2019). In effect, these elements are connected: the DNS third party ecosystem that evolved in recent years cannot be disconnected from consolidation in related markets – browsers and data centres.

For the last three years, Google's Chrome has been by far the global market leader for web browsing, followed by Apple's Safari, Ali Baba's UC Browser and Opera (StatCounter 2019). Just as with DNS resolution, Google has been able to deliver low latency services because of its wide network of locations from which it serves queries across its many data centres around the world, as close to the end user as possible.

With the introduction of the DoH and the new dynamics in the resolver market, the role of the ISPs is changing in a few respects. First, blocking at the level of the ISP becomes redundant – if the choice is with the browsers, their parent company and the jurisdiction they are incorporated in might be determinant factors for the action taken.[5] According to StatCounter's browser market share study from April 2019, Chrome is the global leader (63 per cent), followed by Safari (16 per cent), Firefox (5 per cent) and Samsung Internet (4 per cent). All other players own a maximum of 3 per cent of the market, pointing to the fact that most decisions are taken by resolvers that are US-based and would follow their own internal rules when confronted with legislative and jurisdictional pressures (Hoffmann 2019).

The daily operation of the ISP might be limited by the specific policies of the browsers. For example, Mozilla (primarily relying on Cloudflare) champions DoH by encrypting DNS requests over HTTPS for privacy reasons and approves the list of resolvers before proposing them to users. In a future market we could envision a situation in which a single, preferred DoH provider is pre-configured as the default one, running the risk of giving all data about the browser's users to one provider. The Internet Society warned that such a scenario would happen without user intervention and, if it was the case for a highly popular browser, 'it could change the effective privacy properties of a large fraction of global DNS requests, while changing the trust model of the DNS itself' (Internet Society 2019, 42). Moreover, measurements from browser-based DoH are difficult to take due to the HTTPS traffic being hidden and this might further obscure related research investigating consolidation in the near future.

Changes in the internet ecosystem

Studying consolidation requires looking beyond the direct effects in the market affected. The popularity of public DNS services has consequences beyond the recursive DNS, affecting the operation of other internet markets. For example, alternative DNS has introduced some disruptions for content delivery networks, hosting content in multiple locations, some of which may be very far from the user and affect the speed and performance of the services. To address the problem of suboptimal end-point selection, an extension known as *GeoDNS* has been introduced by Google developers in 2016, proposing to partially reveal a client's IP address to authoritative name servers (Open Rights Group 2019).

At the level of the internet ecosystem, a few dominant players come close to replacing the distributed resolver market previously managed by ISPs. When global outages happen – like the one of Cloudflare on 2 July 2019 (Graham-Cummings 2019) – many more services

are disrupted in a highly centralised market. The move away from a distributed recursive DNS follows other broader concentration trends characterising the current internet. Google leads the advertising services market and increasingly invests in infrastructure, continuously improving access to servers and ownership in submarine cables. This dynamic is replicated by other global service operators that, just like Google, have diversified the markets they participate in and have continued to acquire competitive start-ups to expand and improve their services.

Concentrating the recursive DNS services in the hands of one or a few companies could also put the whole domain name system at risk. As their user base grows fast, these players acquire new capabilities derived from mapping global internet usage and changes in DNS resolution in real time. They also have an advantage in extracting real-time threat intelligence data out of the DNS. In the absence of limitations for sharing across platforms, this can lead to leveraging a competitive advantage in other markets, for example by implementing features for protecting email users from spam or email-based attacks. Unfortunately, this would not benefit the health of the overall internet, since such information would continue to constitute a trade secret, heavily guarded by the market leaders, or a premium service.

Moreover, a larger user base also allows the introduction of new value-added services to the DNS that pertain to one specific resolver, leveraging the network effect with existing users. For example, dominant players can create their own namespace that does not require ICANN's multi-stakeholder processes. Market leaders would have the power to preconfigure their resolvers on billions of devices or applications, creating an additional incentive for users to switch to a particular service, but also raising the market entry barriers. A recursive DNS service was open to anyone to implement, but with the diversification of related services and the increased expectations of the users, that may no longer be the case in the near future.

Conclusion

Since its introduction 36 years ago, the DNS has been operated in a highly decentralised manner. Originally, that meant thousands of ISPs set up their own DNS resolver servers and provided the DNS resolution for their customers. By the end of the 2000s, experimentation with the first alternative DNS services (UltraDNS and OpenDNS) opened the door for a real transformation of the market and its dominant business model. The growing popularity of the public resolvers resulted in a shift towards a two-sided market in which two groups of interest (users and enterprises) are served (bundled) services on differentiated pricing model: users get the DNS lookup for free via public resolvers, while enterprises pay for the advanced threat intelligence and analysis that comes with the significant amounts of traffic data collected.

Our analysis of the recursive resolver usage in the first half of 2019 shows a clear reliance on public resolvers, as more than 50 per cent of DNS queries go through them. Apart from offering improved speed and security, the alternative DNS providers are also able to circumvent local DNS-based censorship regimes and might be preferred in countries that impose network-blocking. Active measurements from 100,000 users' mobile platforms and OONI probes show that there is a high concentration of power in the hands of Google and Cloudflare, which control half of the overall market. The

prospects of DNS in the browser point in a similar direction, consolidating the position of the first company and limiting the opportunities for market entry and for competition. Long-term, innovation might no longer arise on the 'edges' of the network, but rather surface where value and data are readily available and constantly invested in.

Contributing to narrowing the gap between empirical research and DNS market trends, this study shows the concentration is related to an existing or future dominant position in other markets and discusses how dangerous the observed trends are. While public resolvers deliver a better service for the user, with improved speed, security and privacy, they are transforming this unregulated environment by introducing more centralisation, new standards and higher entry costs.

The market-driven approach that characterised the development of the internet in the early 1990s has come under sharp criticism in recent years and we are yet to see the extent to which this will apply to less visible sub-markets, such as that of DNS resolution. Given the rapid changes in the market, our research is necessarily a snapshot in time of a portion of the global DNS resolution. This continuously-evolving market would benefit from regular, accurate and comparable measurements that capture the share of various DNS resolver operators. Quantifying consolidation is increasingly important for unregulated markets such as recursive DNS services.

Notes

1. The DHCP is a protocol used to provide a quick, automatic and centralised distribution of IP addresses within a network, as well as to configure DNS server information on a device, among other functions (Fisher 2019).
2. These include: Domain Name System Security Extensions (DNSSEC), DNS over HTTPS (DoH), DNS over TLS (DoT), DNSCrypt, DNS Over Quic (DoQ), Query Name Minimization, etc. While protocols like DoT and DoQ bring a number of improvements to the DNS transport layer, we see no evidence that their deployment changes the key trends in the consolidation of the DNS resolver market.
3. An exception is the Russian company Yandex, a leader in the search engine market in former USSR states, which launched its own public DNS resolver in 2013.
4. An overview of all measurements is available at the OONI Explorer: https://explorer.ooni.io/world/
5. However, governments can still request DoT and DoH providers to block particular domains from responding accurately to queries (Open Rights Group 2019, 19).

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

Roxana Radu gratefully acknowledges support by the Swiss National Science Foundation under Grant P2GEP1_178007.

Notes on contributors

Roxana Radu is a Postdoctoral Researcher at the University of Oxford's Programme in Comparative Media Law and Policy, working on internet regulation, algorithms and knowledge production in the

public sphere. She is also a Research Associate at the Global Governance Centre, Graduate Institute in Geneva and a non-residential fellow at the Centre for Media, Data and Society, Central European University. Her interdisciplinary research and publications focus on international governance and global internet policy-making.

Michael Hausding is an Internet- and DNS-Security Specialist. He works as the Competence Lead DNS & Domain Abuse for SWITCH, the ccTLD registry for.ch and.li. His main task is preventing internet crime on and with.ch &.li domains. He has been working on internet security for most of his career as an incident handler and programme manager. He is currently the Chair of the Internet Society Switzerland Chapter and a board member of the Swiss Internet Security Alliance. Michael holds a Masters degree in computer science from the University of Darmstadt and a MAS in management, technology and economics from ETH Zürich. He is currently working on a Postgraduate Diploma in Contemporary Diplomacy / Internet Governance with Diplo Foundation and the University of Malta.

References

APNIC. 2019. "Use of DNSSEC Validation for World." Accessed 14 August 2019. https://stats.labs.apnic.net/dnssec/.

Borgolte, Kevin, Tithi Chattopadhyay, Nick Feamster, Mihir Kshirsagar, Justin Holland, Austin Hounsel, and Paul Schmitt. 2019. "How DNS over HTTPS is Reshaping Privacy, Performance, and Policy in the Internet Ecosystem." *SSRN*. 27 July. Accessed 15 December 2019. https://ssrn.com/abstract=3427563.

Broadband Now. 2019. "The Complete List of Internet Providers in the US." Accessed 14 August 2019. https://broadbandnow.com/All-Providers.

Business Insider. 2016. "This 35-Year-Old Grew a College Dorm Project into a Business that Sold to Oracle for More Than $600 million." Accessed 15 December 2019. http://linkis.com/businessinsider.com/TRf2s.

Chuang, Tamara. 2016. "Why Liberty Global Moved to Denver." *Denver Post*. 20 May. https://www.denverpost.com/2016/05/20/the-liberty-global-you-dont-know/.

de Vries, Wouter B, van Rijswijk-Deij, Roland, de Boer, Pieter-There, and Aiko Pras. 2019. "Passive Observations of a Large DNS Service: 2.5 Years in the Life of Google." *IEEE Transactions on Network and Service Management*. doi:10.1109/TNSM.2019.2936031

developers.google.com. 2018. "Your Privacy". Accessed 14 August 2019. https://developers.google.com/speed/public-dns/privacy.

DNS.Watch. 2019. Homepage. https://dns.watch

EuroISPA. 2019. "Who We Are." Accessed 15 December 2019. http://www.euroispa.org/about/who-we-are/.

Fisher, T. 2019. "What is DHCP?" *Lifewire*. 1 July. https://www.lifewire.com/what-is-dhcp-2625848.

Google Chrome. 2019. "DNS-over-HTTPS Setting." Chrome Browser Enterprise Community Announcement. 22 July. https://support.google.com/chrome/a/thread/10152459?hl=en.

Google Security Blog. 2018. "Google Public DNS Turns 8.8.8.8 Years Old." 10 August. https://security.googleblog.com/2018/08/google-public-dns-turns-8888-years-old.html.

Graham-Cummings, J. 2019. "Details of the Cloudflare outage on July 2, 2019." *Cloudflare Blog*. 17 July. https://blog.cloudflare.com/details-of-the-cloudflare-outage-on-july-2-2019/.

Grover, A. 2019. "DNS Resolver-Based Policy Detection Domain." Accessed 15 December 2019. https://datatracker.ietf.org/doc/draft-grover-add-policy-detection/.

Guðmundsson, Ólafur. 2018. "Introducing DNS Resolver 1.1.1.1. (Not a Joke)." *Cloudflare Blog*. 1 April. https://new.blog.cloudflare.com/dns-resolver-1-1-1-1/.

Hoffmann, Stacie. 2019. "Understanding DNS over HTTPS – DoH." *Oxford Information Labs Blog*. 19 August. https://oxil.uk/blog/understanding-dns-over-https-doh/.

Huston, G. 2019. "DNS Resolver Centrality.2." *APNIC Blogpost*. 23 September. https://blog.apnic.net/2019/09/23/dns-resolver-centrality/.

ICANN. 2012. "Ten Million DNS Resolvers on the Internet." 22 March. https://www.icann.org/news/blog/ten-million-dns-resolvers-on-the-internet.

Internet Society. 2019. *Global Internet Report: Consolidation in the Internet Economy*. https://future.internetsociety.org/2019/wp-content/uploads/sites/2/2019/04/InternetSociety-GlobalInternetReport-ConsolidationintheInternetEconomy.pdf.

Kesavan, Archana. 2017. "Comparing the Performance of Popular Public DNS Providers." *NetworkWorld*. 10 May. https://www.networkworld.com/article/3194890/comparing-the-performance-of-popular-public-dns-providers.html.

McCarthy, Kieren. 2007. "Taiwan Government to Block Google's Public DNS in Favor of HiNet's." *The Register*. 11 May. https://www.theregister.co.uk/2017/05/11/taiwan_gov_blocks_googles_public_dns/

Microsoft. 2019. "Windows Will Improve User Privacy with DNS over HTTPS." 17 November. https://techcommunity.microsoft.com/t5/Networking-Blog/Windows-will-improve-user-privacy-with-DNS-over-HTTPS/ba-p/1014229.

Mihalcik, Carrie. 2014. "Google: Turkey is Blocking Our DNS Service." *CNET*. 30 March. https://www.cnet.com/news/google-confirms-turkey-is-blocking-its-dns-service/.

Mozilla. 2019. "Security/DoH-Resolver-Policy." Accessed 14 August 2019. https://wiki.mozilla.org/Security/DOH-resolver-policy.

Mueller, M. 2004. *Ruling the Root: Internet Governance and the Taming of Cyberspace*. Cambridge, MA: MIT Press.

Nykolas, Z. 2018a. "DNS Resolvers Performance Compared: CloudFlare x Google x Quad9 x OpenDNS." *Medium*. 2 April. https://medium.com/@nykolas.z/dns-resolvers-performance-compared-cloudflare-x-google-x-quad9-x-opendns-149e803734e5.

Nykolas, Z. 2018b. "DNS Market Share Analysis – Identifying the Most Popular DNS Providers." *Medium*. 9 April. https://medium.com/@nykolas.z/dns-market-share-analysis-identifying-the-most-popular-dns-providers-80fefb2cfd05.

OECD. 2004. *Access Pricing in Telecommunications*. Glossary of Terms. Paris: OECD.

OECD. 2010. *The Economic and Social Role of Internet Intermediaries*. Report by the Directorate for Science Technology and Industry. Paris: OECD.

OONI (Open Observatory of Network Interference). 2019a. Accessed 15 July 2019. https://ooni.torproject.org/.

OONI (Open Observatory of Network Interference). 2019b. MetaDB. Accessed 15 July 2019. https://github.com/ooni/sysadmin/blob/master/docs/metadb-sharing.md.

Open Rights Group. 2019. *DNS Security – Getting It Right: Recommendations for Policy Makers and Technologists*. London: Open Rights Group. 24 June. https://www.openrightsgroup.org/assets/files/reports/report_pdfs/ORG_DNS_Security_Report_.pdf.

Radu, Roxana. 2019. *Negotiating Internet Governance*. Oxford: Oxford University Press.

Robertson, A. 2018. "Comcast Should Be Investigated for Antitrust Violations, Say Small Cable Companies." *The Verge*. 12 November. https://www.theverge.com/2018/11/12/18088846/comcast-nbcuniversal-american-cable-doj-antitrust-investigation-letter-trump-tweet.

StatCounter. 2019. "Browser Market Share Dynamics Between December 2016 and May 2019." Accessed 15 December. https://gs.statcounter.com/browser-market-share.

Statista. 2019. "Global Digital Population as of October 2019 (in Millions)." Accessed 12 December. https://www.statista.com/statistics/617136/digital-population-worldwide/.

Singel, Ryan. 2009. "Geez, Google Wants to Take Over DNS, Too." *Wired*. 12 March. https://www.wired.com/2009/12/geez-google-wants-to-take-over-dns-too/

US Department of Justice. 2015. "Comcast Corporation Abandons Proposed Acquisition of Time Warner after Justice Department and the Federal Communications Commission Inform Parties of Concerns." Press Release, 24 April. https://www.justice.gov/opa/pr/comcast-corporation-abandons-proposed-acquisition-time-warner-cable-after-justice-department.

Wilder, Christopher. 2015. "Moor to the Story: Quicktake on Cisco's Acquisition of OpenDNS." *Forbes*. 2 July. https://www.forbes.com/sites/moorinsights/2015/07/02/moor-to-the-story-quicktake-on-ciscos-acquisition-of-opendns/#5379a07113b5.

Zetter, Kim. 2008. "OpenDNS Wildly Popular after Kaminsky Flaw Disclosure." *Wired*. 8 June. https://www.wired.com/2008/08/opendns-wildly/.