DNS Resolvers Used in the EU

ICANN Office of the Chief Technology Officer

Alain Durand
OCTO-032
1 March 2022

TABLE OF CONTENTS

This document is part of ICANN's Office of the Chief Technical Officer (OCTO) document series. Please see the OCTO publication page for a list of documents in the series. If you have questions or suggestions on any of these documents, please send them to octo@icann.org.

This document supports ICANN's strategic goal to improve assessment of, and responsiveness to, new technologies which impact the security, stability, and resiliency of the Internet's unique identifier systems by greater engagement with relevant parties. It is part of ICANN's strategic objective to evolve the unique identifier systems in coordination and collaboration with relevant parties to continue to serve the needs of the global Internet user base.

Executive Summary

DNS resolution is typically done either by Internet service provider (ISP) resolvers or by public resolvers. In January 2022, ICANN's Office of the Chief Technical Officer (OCTO) observed that 95% of consumers served by large European Union (EU) consumer ISPs are using their ISP-provided Domain Name System (DNS) resolvers. Only about 4% of consumers served by large EU consumer ISPs are using public resolvers such as Google Public DNS (3%), Cloudflare (0.6%), and Cisco OpenDNS (0.4%). (The remaining users are using non-public resolvers inside or outside the EU.)

Across all EU consumers and business users of ISPs of various sizes, the numbers are different: 86.7% of those users used the DNS resolvers managed by their ISPs in their countries, 12.2% of them used public resolvers (such as Google Public DNS (9.4%), Cloudflare (1.9%), and Cisco OpenDNS (0.8%)), and the remainder using other resolvers. These numbers are also different from what is observed worldwide: about 80% of all users use their ISPs' DNS resolvers and about 20% use public resolvers such as Google Public DNS (17.1%) , Cloudflare (1.8%), and Cisco OpenDNS (0.7%).

Within the EU, there is a very distinct difference between consumer and enterprise patterns. Enterprise users use public resolvers in large numbers (39.3%). This is in contrast to consumer use of DNS resolvers in the EU across all ISP sizes: 90.8% of consumers used the DNS resolvers managed by their ISPs in their countries and only 8.5% of them use public resolvers. There is also a noticeable difference between consumer ISPs depending on the number of users that the ISP has.

Changing DNS resolvers is too complex for the vast majority of consumers: they mostly use the DNS resolvers provided by their ISPs. When measurements detect a large amount of public resolver usage at an ISP, it is likely due to the ISP choosing to either configure the recursive resolvers they operate to forward all queries to one or more public resolvers, or simply to configure their subscribers to use a public resolver. This use of public resolvers resulting from ISP configuration appears to be more often the case for small consumer ISPs (36.2% using a public resolver) than for large consumer ISPs (4.0%).

1 A DNS "Black Box" Measurement System

Public resolver operators do not publish data on the number of users they serve, and it is impossible to determine the number of unique users at any point in time. An evaluation of resolvers used can only be done via a statistical approach relying on sampling, looking at the DNS resolution system from the outside. This method is often referred to as a "black box" measurement. The principle of operation is simple. First, induce a large number of users to send DNS queries for a specific domain name. Then observe the IP addresses of the DNS recursive resolvers querying the authoritative name servers for the experiment's domain name. In case of a chain of DNS recursive resolvers, the DNS authoritative server will only see the last one.

A sampling-based measurement system produces the best data if it uses a large enough sampling size of unbiased users and runs continuously.

This system needs to be large enough to have a comprehensive view of the overall picture and for the measurements to be statistically relevant. If there are only a few thousand samples per day scattered across the EU, the results do not represent the actual use of them. Also, it must not be a one-off experiment, ideally running every day for at least a month to take weekly usage patterns into account.

The selection of samples must be unbiased. For example, a system that relies on the participation of technically competent users will have a self-selection bias, because such users are capable of configuring their resolvers.

When using sampling techniques, it is easy to lose track of the original goal of the experiment. For example, when discussing the overall share, which is X% of operator Y, one needs to keep in mind what is the total population size. In this particular case, the question is X% of what, exactly?

To better understand this issue, one needs to review the typical operation of a DNS resolution in a web browser. When a user clicks on a URL, the browser asks the operating system to look up the IP address of the hostname in the URL, and the operating system's stub resolver sends a DNS query to its configured recursive resolver. The recursive resolver then finds the answer to the query by sending queries to various authoritative servers.

But what if the device's stub resolver is configured with multiple recursive resolvers? What if that recursive resolver forwards the stub resolver's query to other recursive resolvers? Or what if one of the recursive resolver's queries fails for some reason and it retries using a different forwarder? DNS queries and answers are most often performed over the UDP protocol. UDP packets can be lost and not retransmitted. In the IP stack, retries are left to the applications. In such scenarios, instead of a single query arriving at the authoritative server for the domain name in the URL, a multitude of queries could potentially be observed, all of them deriving from that initial click. Which one should be counted? The first one? All of them? Or only a fraction of each of them?

These questions might seem like a purely intellectual exercise, but in fact, the answers depend on the problem one is trying to solve when asking, What is the share of Y? Is the research question which DNS resolvers see what users do in the DNS, or is it which DNS resolvers send answers that users are actually using? In other words, is the desire to know more about the issue of privacy and monetization of user metadata, or to understand the actual usage of the DNS service? Sometimes the measurements will be similar and sometimes they will be different. When interpreting measurements, one must always keep in mind the original question.

And last but not least, when answering the question "X% of what exactly?", one needs to decide which user population to focus on: businesses, consumers, or a mix of both?

2 Methodology

2.1 Partnership

The analysis presented in this paper uses data from research conducted by Asia Pacific Network Information Centre (APNIC) Labs as part of its measurement campaigns. APNIC Labs

run large scale experiments, on a continuous basis, making over 10 million measurements per day around the world. This activity translates to over 20,000 measurements per day in large ISPs in the EU and typically a few hundred measurements per day for small ISPs (except for the very smallest ISPs). We decided to aggregate results from 31 days in January 2022 to smooth out the weekday/weekend patterns. The APNIC system is based on browser-based ads, thus no user intervention is required to run those probes: they all occur silently after the user is served an invisible ad that causes measurements to occur. This ad-based technique eliminates user selection bias, since any user's device can make measurements. Those two characteristics – the large number of measurements and the lack of user selection bias – give us confidence in the data.

Note that this paper is likely to be updated in the future as OCTO performs more analysis on the data.

2.2 Counting

That leaves the question of what to count. We decided to focus this paper on the question, "Which resolvers are people actually using?", leaving the other question ("Which resolvers see the users queries") for another study. Thus, as the original query coming from a single measurement may result in multiple DNS queries coming from different resolvers on the authoritative DNS server, we decided to only count the resolver associated with the first DNS query arriving at an authoritative server for a given domain name. The rationale is that the inbound and the outbound network path will likely be similar, and it is the response to that query that will reach the user first and will most likely be used.

Public resolvers typically operate globally. They use the same anycast IP address for all their instances, regardless of a specific instance's location in a country (anycast is described in RFC 7094).[1] In this study, we decided to count those public resolvers first, then count the recursive resolvers in the same country as the users, then those in a different EU country, and finally those outside of the EU, the total adding to 100%. That way, we can separate the use of public resolvers from the use of other resolvers located inside or outside of the EU. In this document, we use the term "EU ISP" to mean an ISP operating in one of the 27 European Union countries.

The APNIC Labs measurement system includes a list of 29 public resolvers:

- 114 DNS[2]
- AliDNS[3]
- Alternate DNS[4]
- Baidu DNS[5]
- CleanBrowsing[6]
- Cloudflare (commonly called 1.1.1.1)[7]

[1] See https://datatracker.ietf.org/doc/rfc7094/
[2] See https://www.114dns.com/
[3] See http://www.alidns.com
[4] See https://alternate-dns.com/
[5] See https://dudns.baidu.com/support/localdns/Address/index.html
[6] See https://cleanbrowsing.org/
[7] See https://1.1.1.1/dns/

- Comodo Secure DNS[8]
- CNNIC SDNS[9]
- DNS PAI[10]
- DNSPod[11]
- DNS.Watch[12]
- Oracle Dyn[13]
- Free DNS[14]
- Freenom World[15]
- Google Public DNS (commonly called 8.8.8.8)[16]
- Green Team DNS[17]
- Hurricane Electric DNS[18]
- Level 3[19]
- Neustar[20]
- One DNS[21]
- OpenDNS[22]
- Open NIC[23]
- puntCAT[24]
- Quad9[25]
- SafeDNS[26]
- TWNIC Quad 101 (101.101.101.101)[27]
- Uncensored DNS[28]
- Verisign Open DNS[29]
- Yandex DNS[30]

To establish a baseline, we looked first at the worldwide usage of public resolvers, then focused on the EU alone based on the geo-localization of the users.

---

[8] See https://www.comodo.com/secure-dns/
[9] See http://www.sdns.cn
[10] See http://www.dnspai.com/public.html
[11] See https://www.dnspod.cn/products/public.dns
[12] See https://dns.watch
[13] See https://help.dyn.com/internet-guide-setup/
[14] See https://freedns.zone/en/
[15] See http://www.freenom.world/
[16] See https://developers.google.com/speed/public-dns/
[17] See http://www.greentm.co.uk/
[18] See https://dns.he.net
[19] See http://www.level3.com/en/
[20] See https://www.security.neustar/dns-services/free-recursive-dns-service
[21] See https://www.onedns.net
[22] See https://www.opendns.com
[23] See https://www.opennic.org/
[24] See http://www.servidordenoms.cat/
[25] See https://www.quad9.net
[26] See https://www.safedns.com
[27] See https://101.101.101.101/index_en.html
[28] See https://blog.uncensoreddns.org/
[29] See https://www.verisign.com/en_US/security-services/public-dns/index.xhtml
[30] See https://dns.yandex.com/

The IP address of end-user devices, which generate the measurements, are mapped to the Autonomous System Number (ASN) of their ISP. Although ISPs may use multiple ASNs for different technical or business purposes, we use the terms ISP and ASN interchangeably in this document. In this study, we categorized EU-based ISPs into those serving businesses (business-to-business (B2B)) and those serving consumers (business-to-consumers (B2C)). This categorization is based on publicly available data, such as the RIPE Whois database,[31] the RIPE Stat application[32] and the web pages of the ISPs. (RIPE is the Regional Internet Registry (RIR) serving the European region.) This categorization is done for the top 10 ISPs per country, as defined by the number of measurements in the experiment. This categorization process is done manually, so there is room for human interpretation and possibly human error.

We then further zoomed in to look at the differences between small, medium, and large B2C ISPs in the EU. We defined "small" as ISPs with less than a thousand measurements per day, "medium" as those with between 1,000 and 10,000 measurements per day, and "large" those with over 10,000 measurements per day. The largest average number of measurements for an EU ISP was 76,500 per day during that period.

2.3 Limitations of the Methodology

The categorization B2B/B2C was not done for the entire set of ASNs, but only for the top 10 per country. This, compounded by the fact that the larger the number of measurements, the more confidence we have in them, makes that the results for small B2B and small B2C ISPs less reliable than measurements for medium and large ISPs.

Lastly, we compared the results with the measurements from a year earlier (January 2021). Note: the geolocation of IP addresses and the categorization between B2B and B2C was made according to 2022 data. Although there is typically relatively little variation in these data, some changes might have occurred that could influence the reliability of the 2021 results.

[31] See https://apps.db.ripe.net/db-web-ui/query
[32] See https://stat.ripe.net/

3 Results and Interpretations

3.1 World

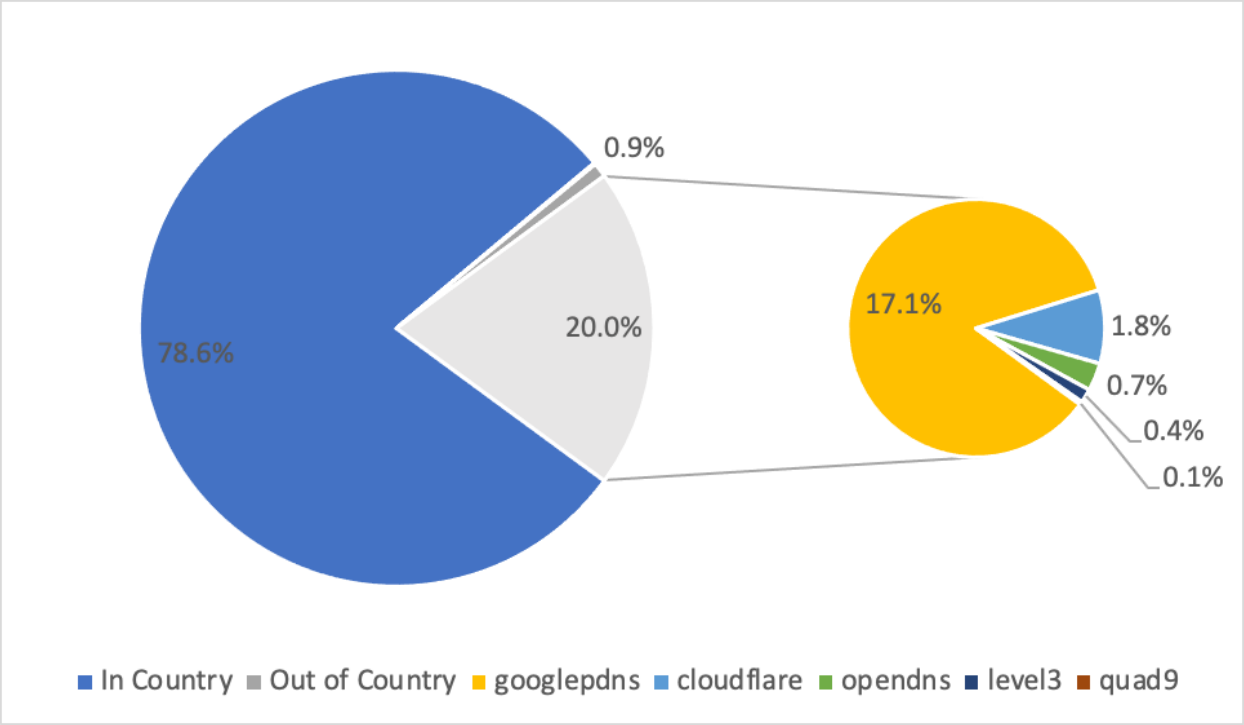

Diagram 3.1 aggregates results from all samples around the world in January 2022.

Worldwide, in January 2022, 78.6% of users used their ISP DNS resolvers and 20% used public resolvers, such as Google Public DNS (17.1%), Cloudflare (1.8%), and Cisco OpenDNS (0.7%). The rest, 0.9%, are queries sent out-of-country to non-public resolvers.

3.2 EU

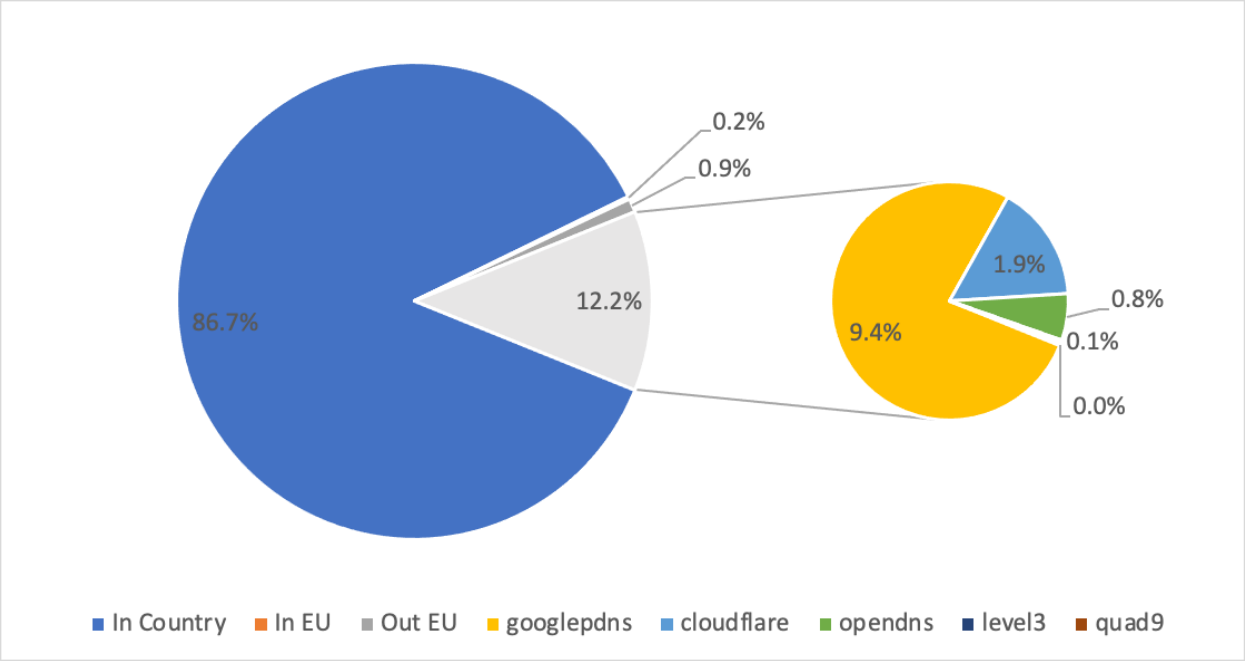

Diagram 3.2 zooms in to all samples collected from EU-geolocated IP addresses for January 2022.

The aggregate EU picture is different from the aggregate world picture. In January 2022, 86.7% of users across the EU used the DNS resolvers managed by their ISPs in their respective countries. About 12.2% of them use public resolvers such as Google Public DNS (9.4%), Cloudflare (1.9%), and Cisco OpenDNS (0.8%). The rest of the data consisted of 0.2% of queries, which were sent to non-public resolvers from outside of the country, but in the EU and 0.9% of queries, which were sent to non-public resolvers located outside of the EU.

3.3 EU B2B

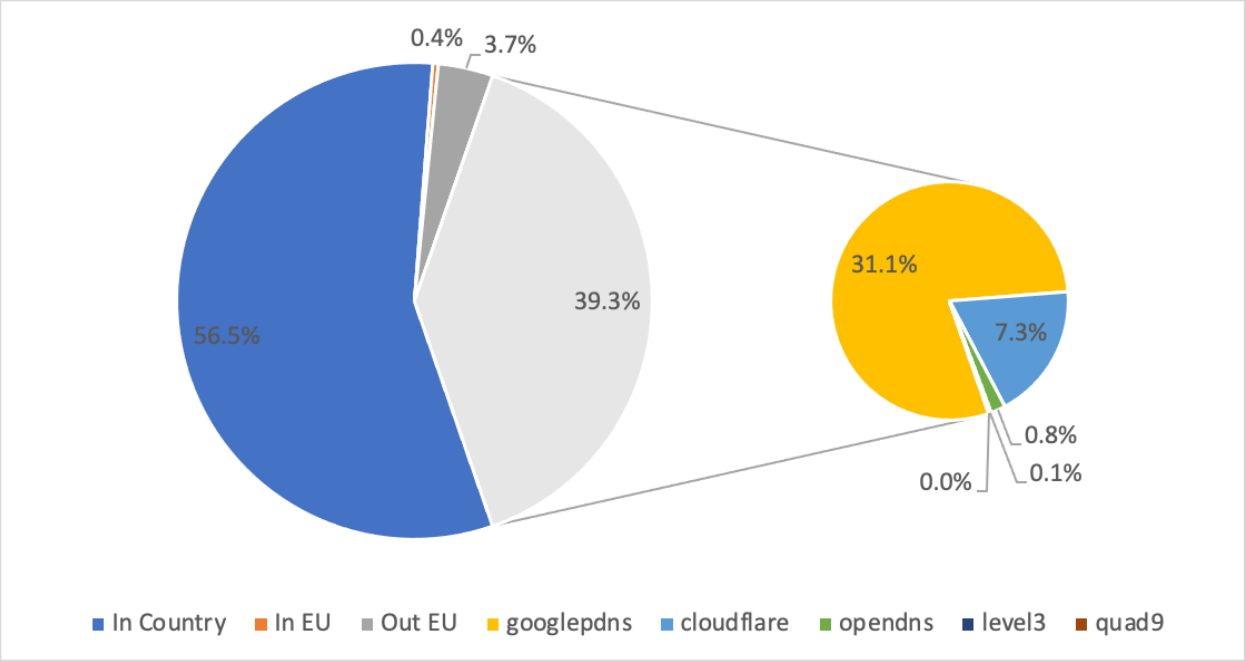

Diagram 3.3 only shows IP addresses geolocated in the EU that are part of ASNs corresponding to B2B ISPs for January 2022.

Samples from B2B ISPs' users show a very different pattern of reliance on public resolvers than the general EU ones: 39.3% of B2B ISP users relied on public resolvers, i.e., Google Public DNS (31.1%), Cloudflare (7.3%), and Cisco OpenDNS (0.8%). It would appear that a large number of enterprises have made the conscious choice to configure their DNS to use public resolvers. B2B users' reliance on their ISP-managed resolvers is only about 32%. We considered two possible explanations: a) some enterprises outsource their DNS resolution to public resolvers for cost reasons (similar to small consumer ISPs, as will be discussed in section 3.5) or b) they do that because they subscribe to DNS-managed services (such as DNS filtering or optimization), which may include access to an open resolver.

3.4 EU B2C

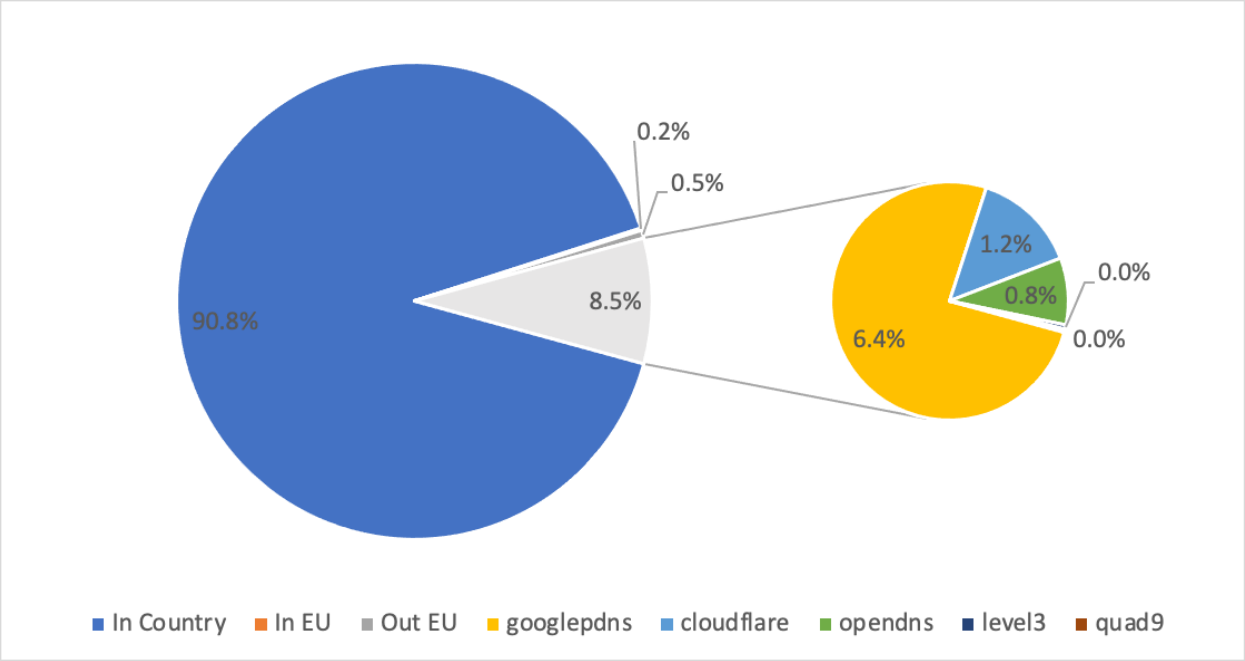

Diagram 3.4 only shows IP addresses geolocated in the EU and that are part of ASNs affiliated to B2C ISPs for January 2022.

The picture is dramatically different for measurements from B2C ISPs' users. In January 2022, 90.8% of consumers across the EU used the DNS resolvers managed by their ISPs in their respective countries. Only about 8.5% of them used public resolvers such as Google Public DNS (6.4%), Cloudflare (1.2%), and Cisco OpenDNS (0.8%).

Those numbers support our hypothesis that changing DNS configuration is too complex for the vast majority of consumers.

3.5 EU Small B2C

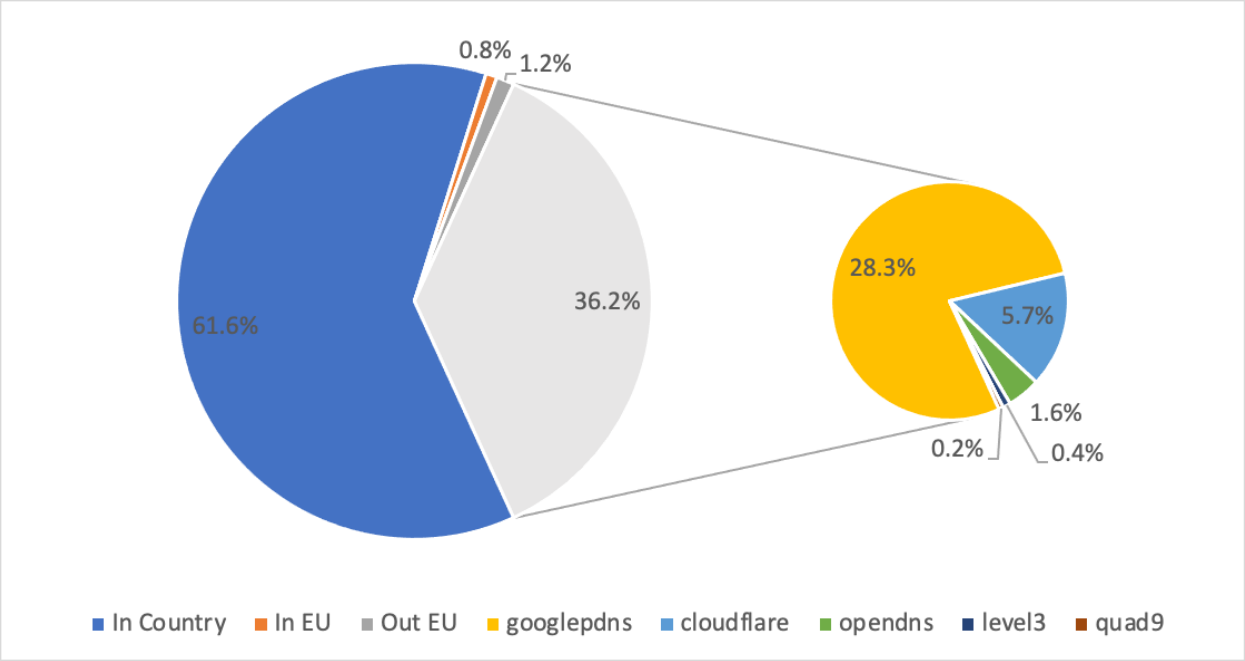

Diagram 3.5 only shows IP addresses geolocated in the EU that are part of ASNs affiliated to small B2C ISPs for January 2022.

The level of reliance on DNS public resolvers is not uniform in the EU. We see large differences based on the apparent size of the ISP. As mentioned in the methodology section, we characterize “small ISPs” as the ones being covered by fewer than 1,000 measurements per day.

In January 2022, 61.6% of customers of “small” consumer ISPs across the EU used the DNS resolvers managed by their ISPs in their countries; and 36.2% of them used public resolvers such as Google Public DNS (28.3%), Cloudflare (5.7%), and Cisco OpenDNS (1.6%).

When measurements detect a non-trivial amount of public resolver usage at an ISP, we feel that it is likely the case that the ISP made the choice to either configure the recursive resolvers they operate to forward all queries to one or more public resolvers or simply to direct their subscribers to use a public resolver via configuration methods. This configuration uses methods such as DHCP options in IPv4 (RFC 2937), DHCPv6 options for IPv6 (RFC 3646) and Router Advertisement options in IPv6 (RFC 8106), or similar mechanisms in cellular environments.[33,34,35]

[33] See https://datatracker.ietf.org/doc/rfc2937/
[34] See https://datatracker.ietf.org/doc/rfc3646/
[35] See https://datatracker.ietf.org/doc/rfc8106/

3.6 EU Medium B2C

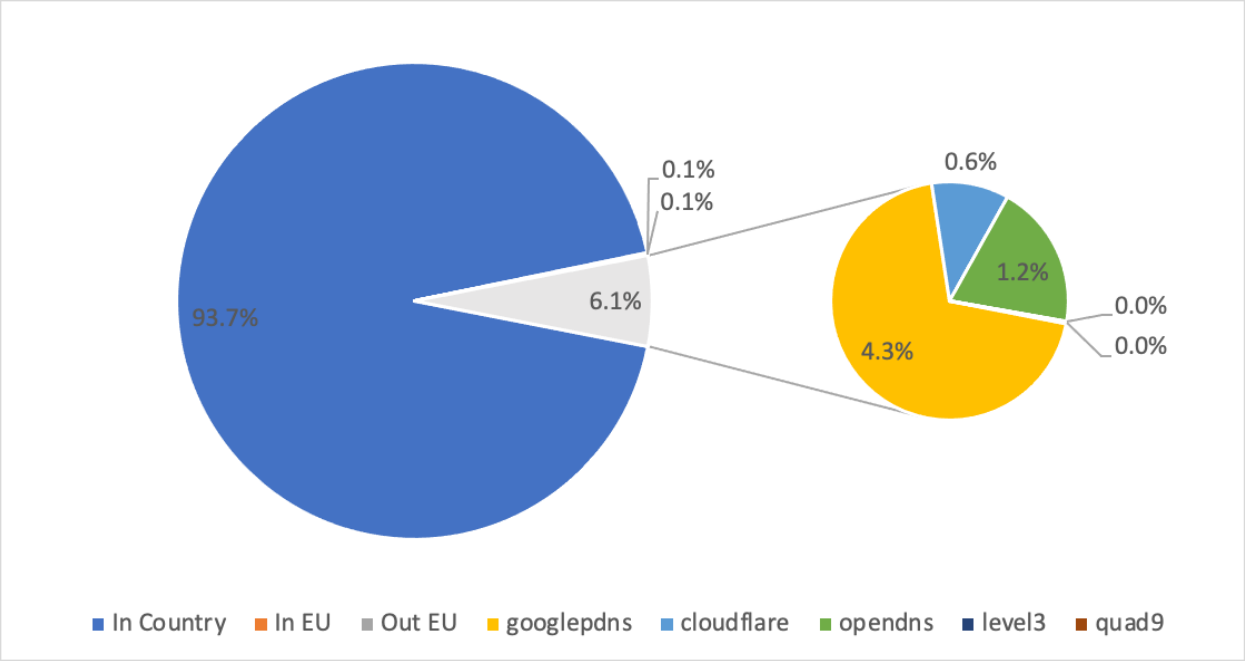

Diagram 3.6 only selects IP addresses geolocated in the EU and that are part of ASNs affiliated to medium B2C ISPs for January 2022.

As mentioned in the methodology section, we characterized “medium ISPs” as those that received more than 1,000 but less than 10,000 measurements per day.

In January 2022, 93.7% of customers of ”medium” consumer ISPs across the EU used the DNS resolvers managed by their ISPs in their countries; and 6.1% of them used public resolvers such as Google Public DNS (4.3%), Cisco OpenDNS (1.2%), and Cloudflare (0.6%).

3.7 EU Large B2C

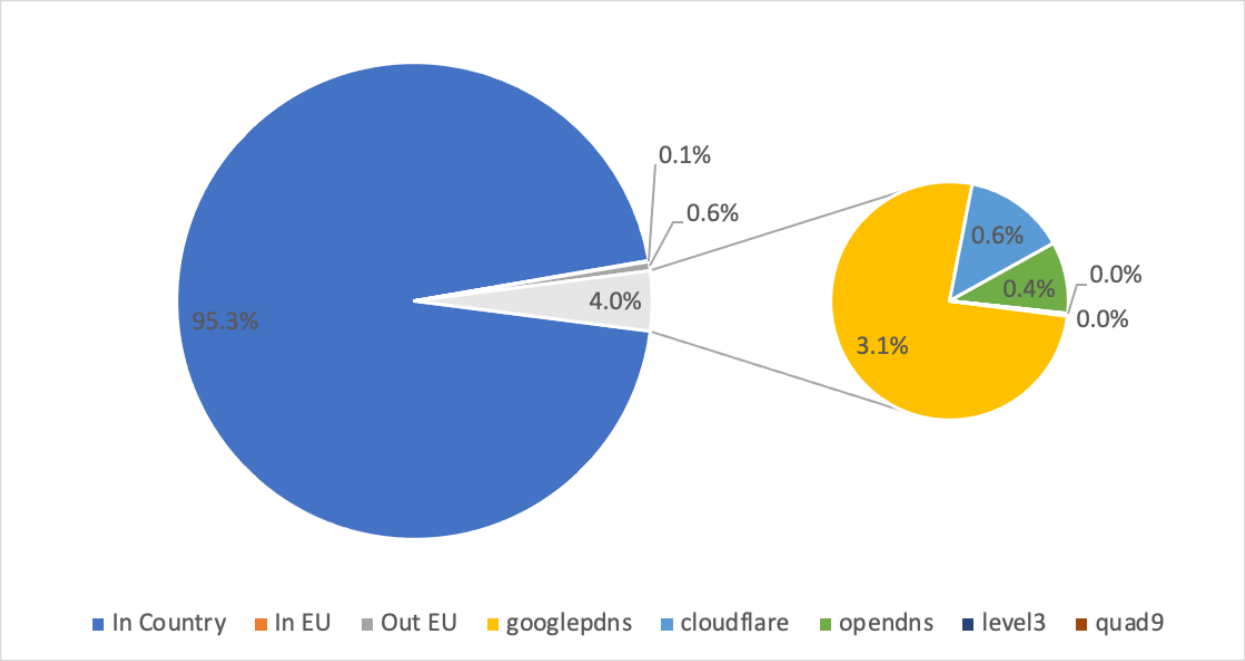

Diagram 3.7 shows IP addresses geolocated in the EU and that are part of ASNss affiliated to large B2C ISPs for January 2022.

As mentioned in the methodology section, we characterized “large ISPs” as those that received more than 10,000 measurements per day, the average maximum observed number being 76,500.

In January 2022, 95.3% of customers of ”large” consumer ISPs across the EU used the DNS resolvers managed by their ISPs in their countries; and 4% of them used public resolvers such as Google Public DNS (3.1%), Cloudflare (0.6%), and Cisco OpenDNS (0.4%). However, the smaller the ISP, the larger its reliance on public resolvers: 36.2% of customers for small ISPs use public resolvers, while 6% of medium-sized ISPs, and 4% of large ISPs use public resolvers.

DNS resolver data can be leveraged by network analytics to improve network management; it can also be directly monetized. OCTO hypothesizes that many ISPs still consider DNS service as a cost center, not a profit center. Large ISPs have entire teams of engineers specialized in managing their DNS resolvers. Small ISPs very often cannot (or don’t want to) afford it. In many cases, small ISPs may simply decide to forward the DNS queries to public resolvers.

The EU is a set of comparable developed countries with many large ISPs, proportionally more than in the world at large. As seen above, large ISPs tend to not outsource or forward DNS queries to public resolvers. This is a possible explanation why the measurements for the EU show a lower reliance on public resolvers than the measurements for the whole world.

3.8 In EU / Out of EU DNS Traffic

Excluding the aforementioned public resolvers, the amount of DNS traffic sent outside of the EU is minimal for the B2C environment, less than 1%. It is higher in the B2B environment at 3.7%. This can potentially be explained by non-EU, large multinational companies sending their DNS traffic via VPN back to their country of origin.

We also observed that the amount of out-of-country but intra-EU DNS resolution is very low, less than 1%. A higher number would have potentially indicated a situation where large pan-European ISPs perform DNS resolution in their country of origin. This is not the case, as most DNS resolution, except for those sent to public resolvers, is performed in the country.

3.9 Public Resolver Distribution

As seen in Section 2, we took into account a list of 29 public resolvers based in various countries around the world..

Cloudflare, Google Public DNS, and Cisco OpenDNS are the only three public resolvers used by more than 1% of users in any of the EU scenarios we studied. A second tier used by less than 1% but more than 0.1% of users includes Level3, Neustar, Quad9, and Yandex. All the other public resolvers are used by less than 0.1% of users in any of the EU scenarios we studied.

4 Comparison with 2021

We are seeing an overall increase in the amount of public resolver usage from 2021 to 2022.

4.1 World

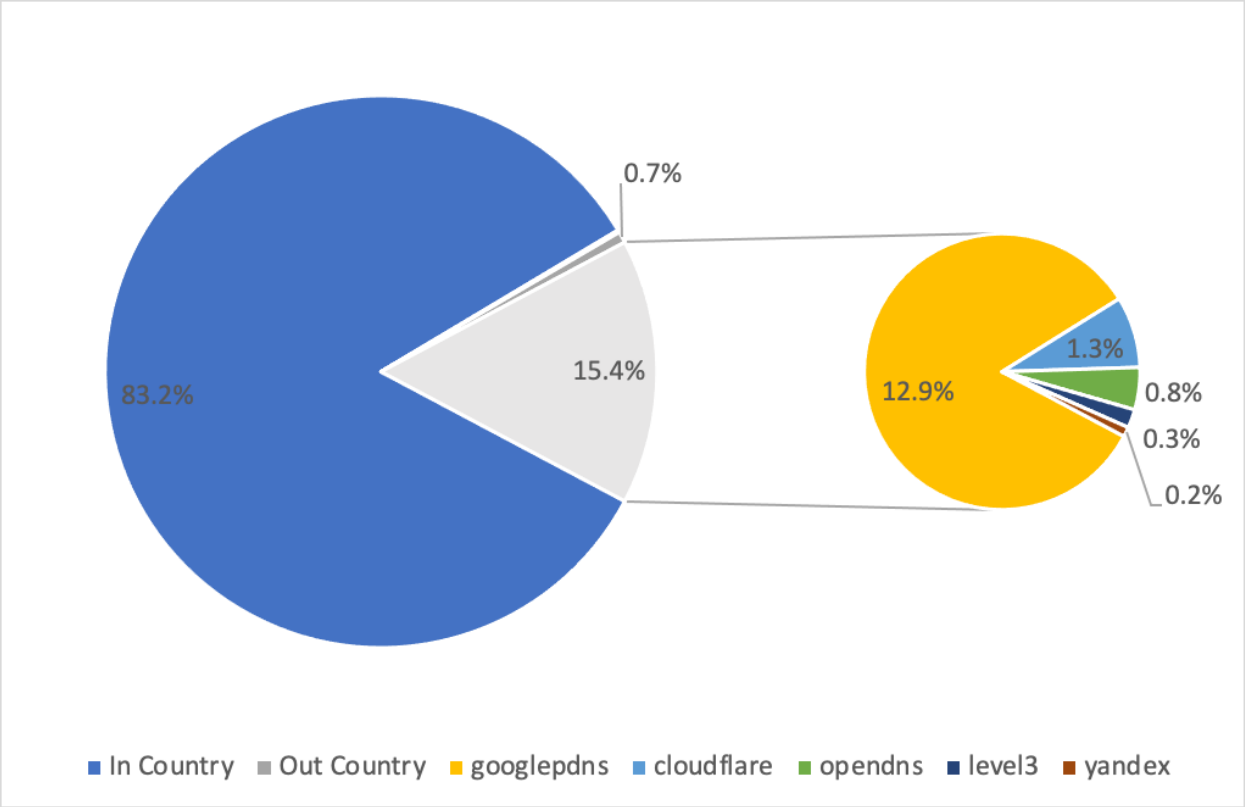

Diagram 4.1 aggregates results from all samples around the world in January 2021.

For the world, the share of DNS public resolvers went up 4.6% from 15.4% to 20%.

4.2 EU B2C

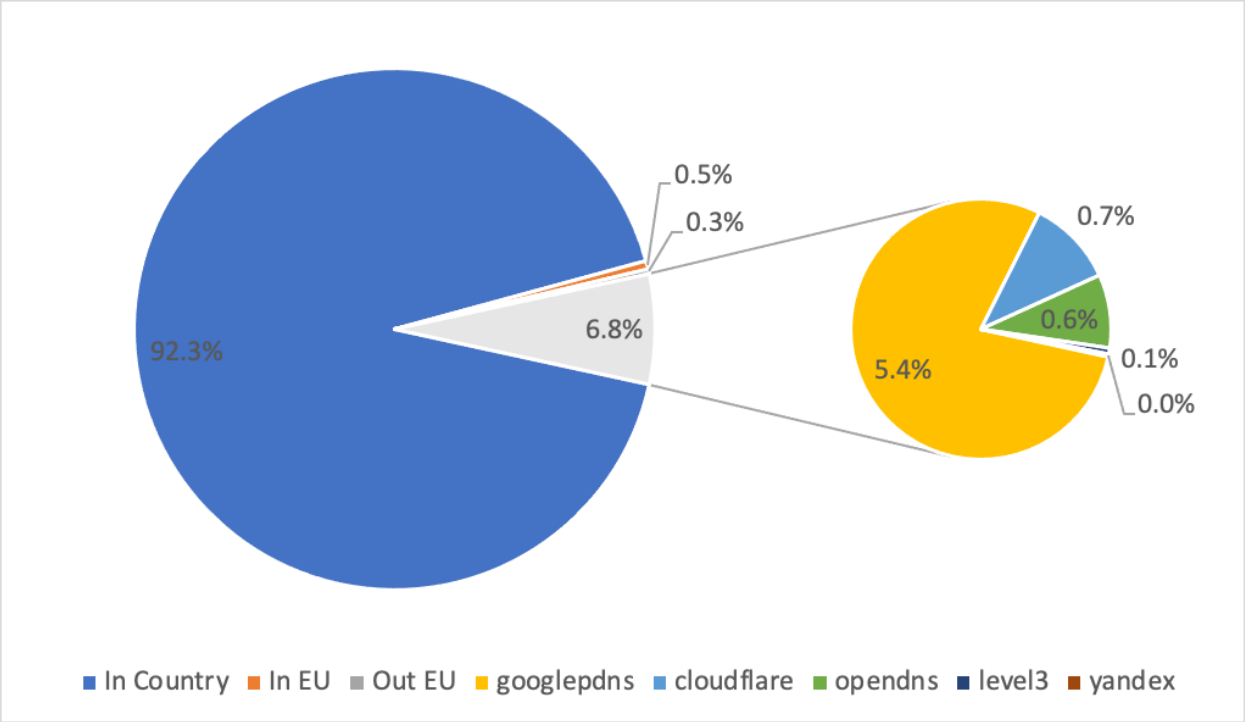

Diagram 4.2 zooms in on all samples collected from EU-geolocated IP addresses in January 2021 for B2C ISPs.

For the EU B2C totals, public DNS usage went up by 1.7% from 6.8% in 2021 to 8.5% in 2022. The major open DNS providers remain the same, and their relative proportions also remain stable.

We see similar increases in all three sizes of B2C ISPs.

5 Analysis of the Distribution of ISP Choices for January 2022

To better understand the picture behind the average numbers presented in Section 3, we looked at the distribution of open resolver usage per ISP for small, medium and large B2B and B2C ISPs. For this, we considered all ISPs in the category, sorted them by the percentage of open resolver usage and plotted the graph showing the breakdown of public resolver usage for all those ISPs. Each vertical line represents an ISP. We decided to remove the actual Autonomous System number on the horizontal axis.

When we zoom in to individual ISPs, some of them are served by few measurements. We consider a minimum of 100 measurements per day a minimum threshold to have confidence in the data. As such, we decided to remove from the list the ISPs served by fewer than 100 measurements on average per day, i.e. 3,100 measurements in January 2022.

5.1 Small B2B

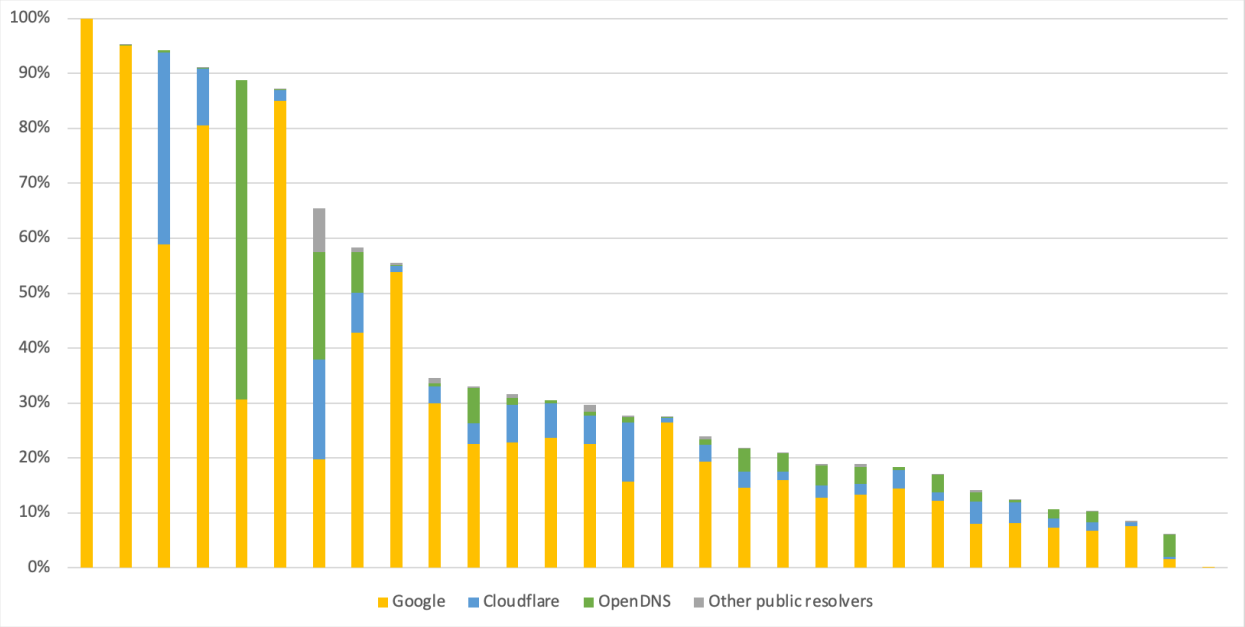

Diagram 5.1 looks at the variations in open resolver usage among small B2B ISPs.

About one third of small B2B ISPs show a high use of public resolvers (>50%). The rest, two thirds of them, show a significant use of public resolvers (>10%).

5.2 Medium B2B

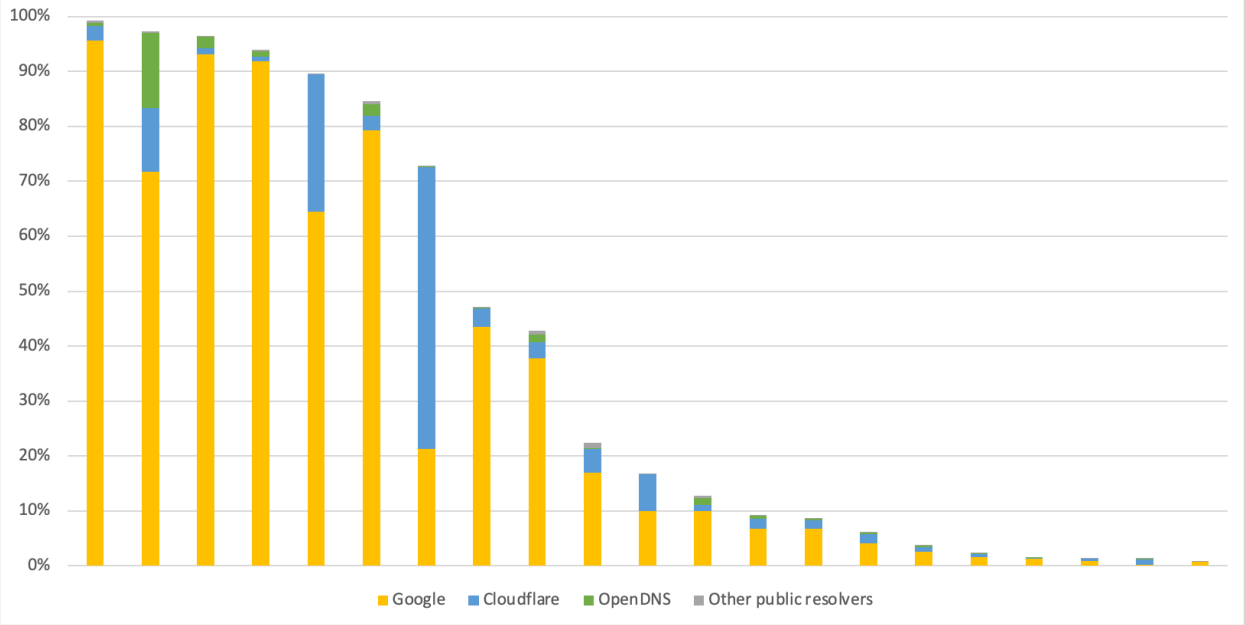

Diagram 5.2 looks at the variations in open resolver usage among medium B2B ISPs

We see an almost even split between the ISPs whose users use public resolvers (> 40%) and those who do not use public resolvers (< 10%).

5.3 Large B2B

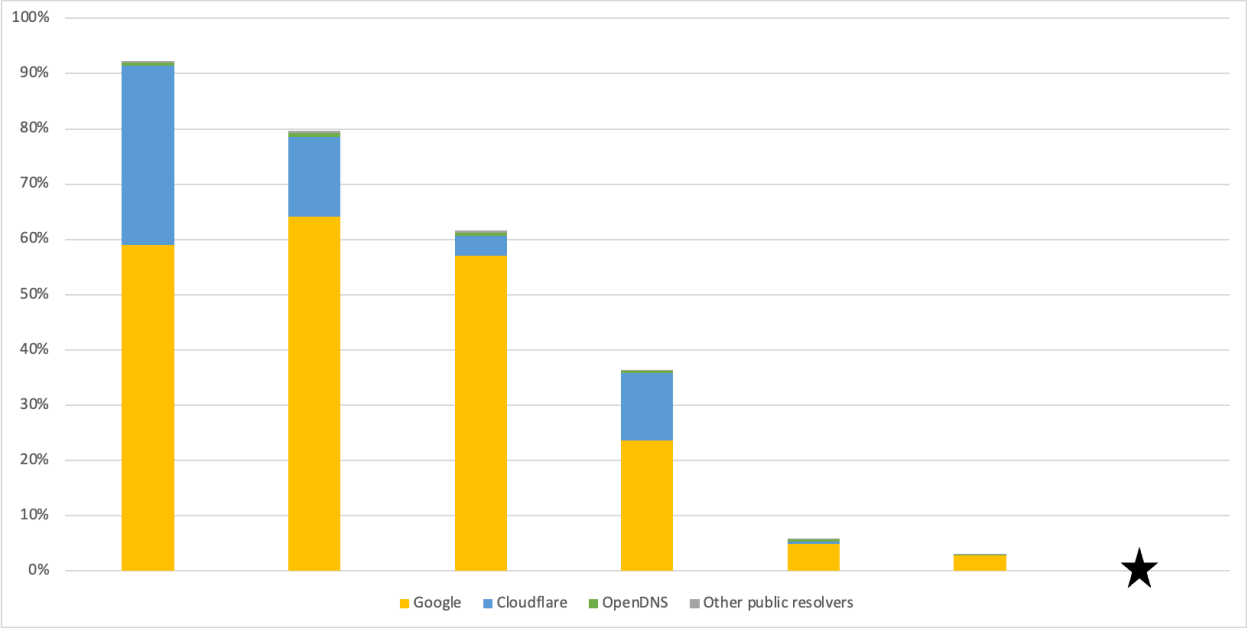

Diagram 5.3 looks at the variations in open resolver usage among large B2B ISPs. Note, on the far right of the graph, there are ISPs which show 0% usage of a public resolver.

About half of ISPs display a large use of public DNS (>50%), the other half shows very little public DNS usage (<10%) .

5.4 Small B2C

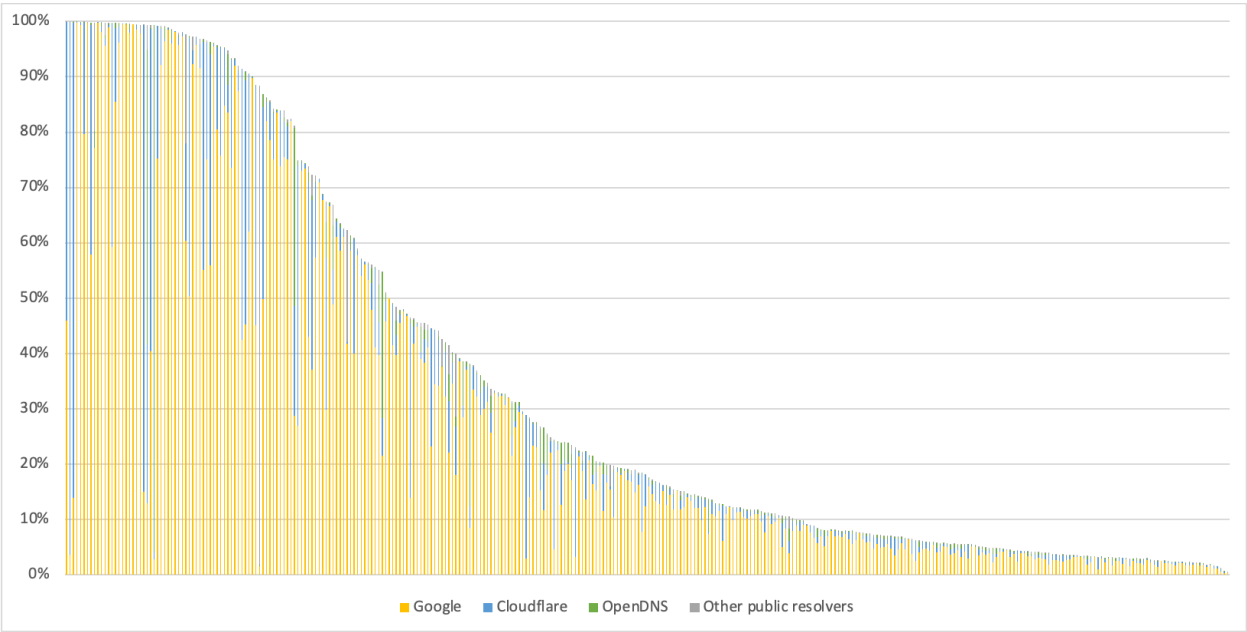

Diagram 5.4 looks at the variations in open resolver usage among small B2C ISPs.

This diagram shows a similar pattern as in diagram 3.10 for small B2B ISPs, with a large number of ISPs showing heavy public resolvers usage (>80%). The values on the tail end of the graph are higher than expected.

5.5 Medium B2C

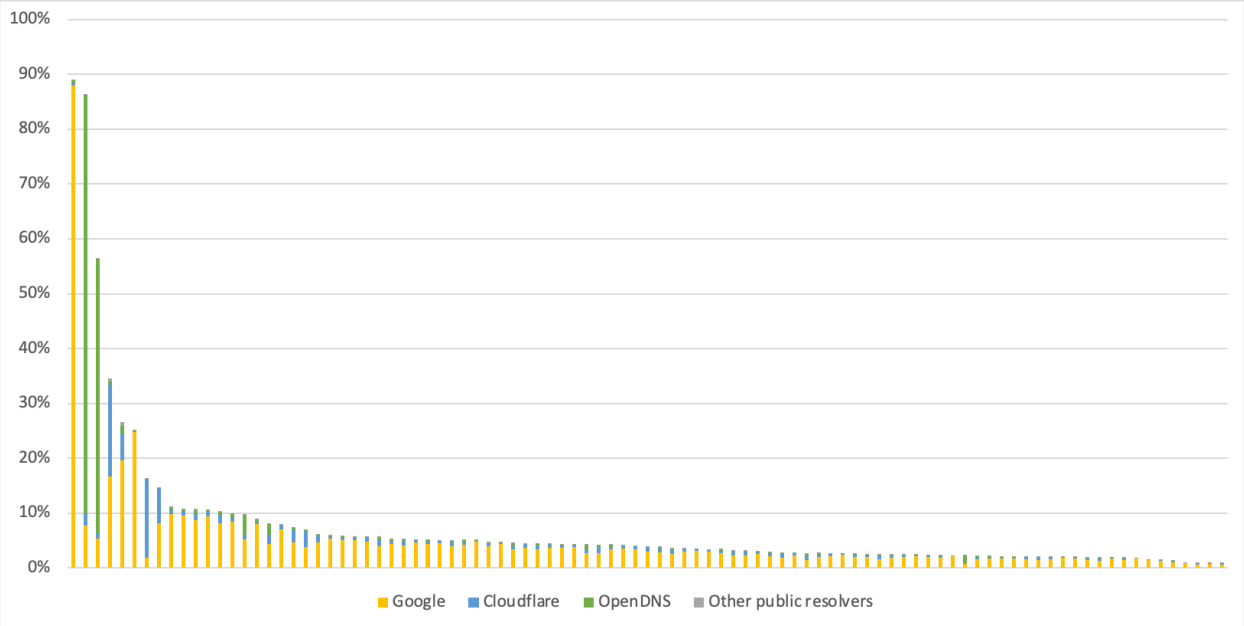

Diagram 5.5 looks at the variations in open resolver usage among medium B2C ISPs.

We see a small number of medium B2C ISPs showing heavy public resolver usage (>50%) and a very long tail of ISPs apparently doing DNS resolution themselves, with just a few percent of users using public resolvers.

5.6 Large B2C

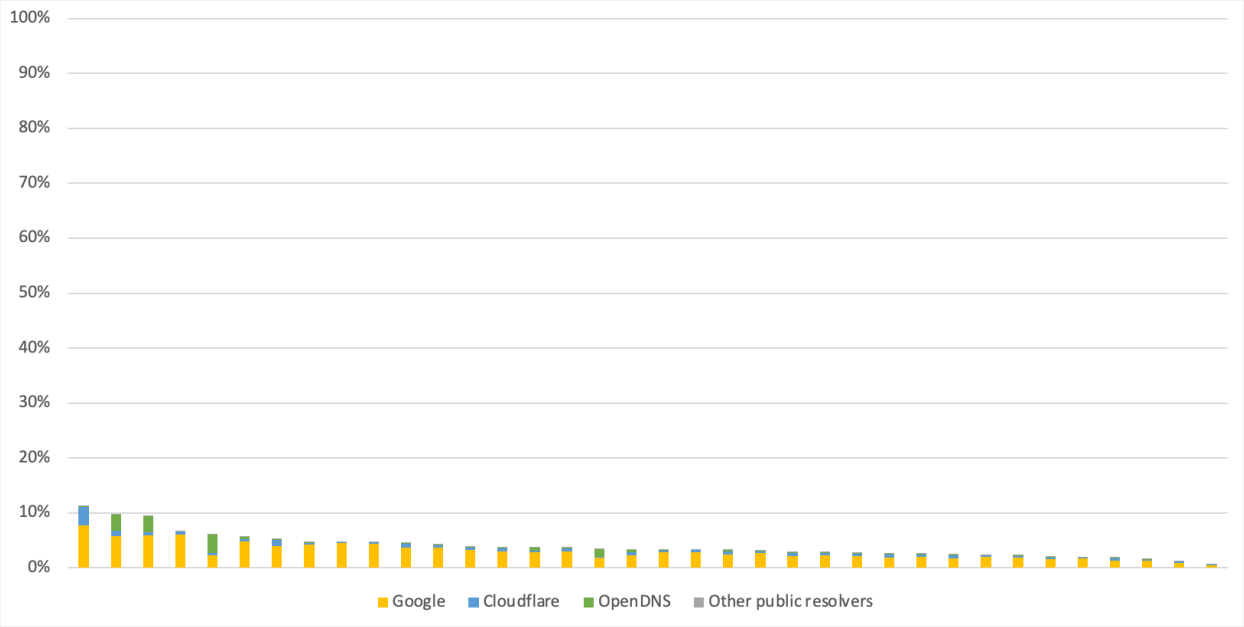

Diagram 5.6 looks at the variations in open resolver usage among medium B2B ISPs.

Most large B2C ISPs users seem to use their ISP-provided DNS resolvers. Similar to medium B2C ISPs, we see a background measurement of a few percent of users using public resolvers.

5.7 B2B vs B2C

In small ISPs, we see a similar pattern in B2B (diagram 5.1 and B2C (diagram 5.4 of heavy usage of public resolvers by users of several ISPs. This pattern repeats for medium and large B2B ISPs.

However, when we compare diagrams for medium B2B ISPs 5.2 and medium B2C ISPs 5.5, and then large B2B ISPs 5.3 and large B2C ISPs 5.6, we see a very clear distinction between B2B and B2C environments for medium and large ISPs. We see there a much lower usage of public resolvers.

It would appear that B2B ISPs (and/or their enterprise customers) make similar decisions when it comes to DNS resolution, regardless of size. This is not the case for B2C, where we see a clear difference between ISP sizes.

5.8 Choice of Public Resolver

Looking at all diagrams in section 5, we see different ISPs in the same categories making different choices for public resolvers. We see a combination of the most popular public resolvers used: Google, Cloudflare, and Cisco OpenDNS. In most cases, Google has the largest share, but not always. We see cases of individual ISPs choosing primarily Cloudflare or Cisco OpenDNS.

6 Conclusion

This study demonstrates a clear difference between enterprise and consumer behavior when it comes to DNS recursive resolver choice in the EU. Our analysis shows that different sized consumer ISPs serving different customer segments make different choices for DNS resolution. In this paper we have proposed a few possible reasons for these variations.

The numbers are changing over time. We did see an increase in the proportion of public resolvers used by consumers from 2021 to 2022. The ICANN OCTO Identifier Technology Health Indicators (ITHI) will define and track new metrics based on this study.[36]

7 Acknowledgements

The author would like to acknowledge the contributions of Joao Damas and Geoff Huston from the APNIC Labs and David Huberman from ICANN OCTO.

[36] See https://ithi.research.icann.org