



Stranger VPNs: Investigating the Geo-Unblocking Capabilities of Commercial VPN Providers

Etienne Khan^{1(✉)}, Anna Sperotto¹, Jeroen van der Ham^{1,2},
and Roland van Rijswijk-Deij¹

¹ Faculty of Electrical Engineering, Mathematics and Computer Science,
University of Twente, Enschede, The Netherlands

{e.khan,a.sperotto,j.vanderham,r.m.vanrijswijk}@utwente.nl

² National Cyber Security Centre, The Hague, The Netherlands

Abstract. Commercial Virtual Private Network (VPN) providers have steadily increased their presence in Internet culture. Their most advertised use cases are preserving the user's privacy, or circumventing censorship. However, a number of VPN providers nowadays have added what they call a *streaming unblocking service*. In practice, such VPN providers allow their users to access streaming content that Video-on-Demand (VOD) providers do not provide in a specific geographical region.

In this work, we investigate the mechanisms by which commercial VPN providers facilitate access to geo-restricted content, de-facto bypassing VPN-detection countermeasures by VOD providers (blocklists). We actively measure the geo-unblocking capabilities of 6 commercial VPN providers in 4 different geographical regions during two measurements periods of 7 and 4 months respectively. Our results identify two methods to circumvent the geo-restriction mechanisms. These methods consist of: (1) specialized ISPs/hosting providers which do not appear on the blocklists used by content providers to geo-restrict content and (2) the use of residential proxies, which due to their nature also do not appear in those blocklists. Our analysis shows that the ecosystem of the geo-unblocking VPN providers is highly dynamic, adapting their chosen geo-unblocking mechanisms not only over time, but also according to different geographical regions.

1 Introduction

Virtual Private Networks (VPN) allow us to act as part of a specific network even from a physically remote location, with the added advantage of doing so in a secure and private manner. As a consequence of this, not only are we able to access our work environment while working from home, but users all over the world benefit from better privacy or, for example, have the ability to circumvent censorship [26]. Acting as part of a physically remote network, however, also means that a user will appear to be in a different physical location than their real one, thus allowing them access to content and services that are instead typically bound to a specific geographic region. VPN providers have recently

added one more service to their repertoire that allows them to capitalize on this, namely a so-called *streaming unblocking service*.

VPN streaming services are born in the context of the arms race that seems to exist between VPN providers and Video-on-Demand (VOD) providers. As a consequence of non-technical constraints such as copyright negotiations, licensing and business models, VOD providers typically use geolocation mechanisms to identify if a user is allowed access to certain content. This phenomenon is known as *geo-blocking* or *geo-fencing*, and it is often negatively perceived by end users. Think about not being able to watch the new season of your favorite series that is already streaming in the US, but that lengthy copyright negotiations are holding back in other parts of the world. Since VPNs have the ability to let a user’s request originate from a different geographical location, VOD providers have developed methods to detect if a user connects to their service using a VPN, and can block the request. Despite these countermeasures, VPN providers claim to be able - and we can confirm that they succeed - to bypass VOD geo-blocking and VPN detection mechanisms.

This paper investigates how VPN providers are able to bypass geo-blocking and VPN detection. We refer to this as *geo-unblocking*. The challenge in this is that VPN providers act as “black boxes”, hiding from the end-user how geo-unblocking is achieved. This calls for an in-depth analysis of the VPN geo-unblocking ecosystem.

The contributions of this paper are that:

- We empirically infer a model of the VPN geo-unblocking ecosystem and identify a methodology that gives us visibility into the population of proxy hosts used to bypass geo-unblocking;
- We identify two distinct methods used by VPN providers to circumvent VOD geo-blocking and VPN-detection mechanisms;
- We characterize these methods at the network-level, shedding light on how VPN providers implement these methods and how their strategies adapt over time and over different regions.

The remainder of this paper is organized as follows. In Sect. 2 we present the relevant related work and background information. In Sect. 3 we describe the VPN ecosystem in relation to geo-unblocking. We then describe how we select relevant VPN providers in Sect. 4. In Sect. 5 we explain our methodology to identify VPN exit nodes used for geo-unblocking, and we explain how we collected our data set. Section 6 presents our results. We discuss ethical concerns regarding our study in Sect. 7. Finally, we present our conclusions in Sect. 8.

2 Background and Related Work

2.1 Background

Geo-blocking and Geolocation. Geo-blocking is the term for the procedure of prohibiting access to online resources based on the user’s geographical location [27]. VOD providers make use of this, because they often do not possess

the licensing rights to broadcast their content globally [11,19]. Therefore, they have to ensure that only subscribers from regions for which the license has been acquired may access the resource. In order to accurately do so, VOD providers make use of geolocation databases to map users' traffic to its geographical origin. Such geolocation databases are often maintained by commercial parties and strive to have a high accuracy, but research has shown that this data is mostly only accurate and consistent at a country level, compared to a more fine-grained province or city level [24].

Proxy/VPN Detection at VOD Providers. VOD providers are aware that their users circumvent the geographical restrictions put in place by using proxies or VPNs [4,8,10,13,15]. To deter the use of these proxies and VPNs, the VOD provider has to reliably detect their use. VOD providers do not disclose their detection methods, but we suspect that IP geolocation services are used at least partially for this [2,9,14]. Nowadays, many IP geolocation providers, e.g. NetAcuity, Maxmind, IP2Location or IPInfo offer more data than just geographical information. For example, they provide publicly available information such as the *AS number*, *ISP name*, or *reverse DNS* entry of the IP in question, but some providers are even classifying IP ranges by their usage. In those cases they provide information such as if the IP address is located at a data center or at a consumer's household as well as if the IP address is being used for proxy purposes (such as an open proxy or Tor exit node) or if it belongs to a commercial VPN service including the name of the VPN provider. We call these databases *enhanced geolocation databases*, as they provide metadata which cannot be inferred from public databases (i.e. from national or regional Internet registries). This information may allow VOD providers to more easily identify users circumventing geoblocking.

2.2 Related Work

Researching commercial VPN providers is a relatively new direction in the Internet measurement community and most current work focuses on privacy and security aspects.

In 2015, Perta et al. manually analyzed 14 providers on their privacy and security claims, and concluded that almost all providers are vulnerable to IPv6 leakage [29]. A follow-up study by Ikram et al., one year later, extended this previous work, by analyzing 283 Android VPN apps [25]. Even though the Android apps benefit from a standardized networking interface, many of the apps came with embedded malware, ad-trackers, JavaScript injection, ad-redirections and even TLS interception. Work by Khan et al. from 2018 presented a more comprehensive view of the commercial VPN ecosystem as a whole [26]. This work not only includes the previously mentioned privacy and security issues, but also investigates the VPN providers' claims regarding the physical location of the VPN servers. In their results the authors show that 5-30% (depending on the geolocation database used) of all servers are located in a different country than

what is advertised and in one extreme case a provider claimed to have 190 distinct locations, but ultimately only 10 different data centers were responsible for the hosting of the servers.

Similar research has been conducted by Weinberg et al., who tried to verify advertised proxy locations with the help of geolocation [32]. They conclude that one third of all proxies are definitely not in the advertised location and another third might not be. A different study by Winter et al. tried to geolocate BGP prefixes, in order to better understand routing anomalies, outages and more [33]. One of their data points showed that a /23 network geolocated to 127 different countries (including Vatican City and North Korea). This is of course highly unlikely and only after consulting WHOIS data, it became clear that this was an IP range owned by a commercial VPN provider¹. The most recent paper on the commercial VPN ecosystem from Ramesh et al. presents measurement software called *VPNalyzer* which can run on end-user devices to “collect 15 distinct measurements that test for aspects of service, security and privacy essentials, misconfigurations, and leakages” [30]. Their system allows for a systematic analysis of key security and privacy issues in VPN implementations in the wild.

All previously mentioned studies highlight the usage of VPNs (or proxies) to circumvent geo-blocking. Yet to the best of our knowledge, there has not been any study so far that investigated the unblocking methodologies of these providers, which we instead cover in this paper. There has been an assumption that geo-unblocking can be facilitated through the sheer amount of servers operated². Our contribution to this field presents new insights, by showing that this is not necessarily the case.

3 Ecosystem

When analyzing the geo-unblocking ecosystem, the first step is to understand how geo-unblocking is carried out. In this section, we reason about how geo-unblocking can be achieved, we test our assumptions and derive a model of the geo-unblocking ecosystem.

If we consider that VOD providers use enhanced geolocation databases to detect the use of proxies or VPNs by looking at IP addresses, but also that streaming unblocking services do work, then it stands to reason that commercial VPN providers claiming to be able to bypass geolocation must use IPs which are not marked as proxy or VPN in geolocation databases.

This helps us shape a view of the geo-unblocking VPN ecosystem, and leads to the assumption that traffic to VOD providers may be routed differently via the VPN server than traffic to non VOD providers.

¹ The provider in question is the same provider who claimed to operate 190 distinct locations from the Khan et al. study [26].

² Some commercial VPN providers claim to run between 2,000 and 4,000 servers [26].

```

traceroute to example.com (93.184.216.34), 64 hops max, 72 byte packets
 1  10.8.0.1
 2  cs0-evo.nl.as25369.net
 3  ae2.10.rt0-evo.nl.as25369.net
 4  adm-b3-link.ip.twelve99.net
 5  adm-bb4-link.ip.twelve99.net
 6  prs-bb2-link.ip.twelve99.net
 7  rest-bb1-link.ip.twelve99.net
 8  ash-b2-link.ip.twelve99.net
 9  verizon-ic342246-ash-b2.ip.twelve99.net
10  ae-65.core1.dcb.edgecastcdn.net
11  93.184.216.34

```

Fig. 1. ICMP traceroute to `example.com` while being connected to NordVPN. RTTs have been omitted for readability.

We investigated this assumption by purchasing multiple subscriptions to common commercial VPN providers that advertise with geo-unblocking capabilities. During the setup phase for these providers we were asked to use their custom connection clients, which featured simple menus through which we could choose our VPN server’s location. The source code for these applications is not made available though, so we cannot reason about the inner workings of the programs without reverse engineering. Luckily, all the providers we considered offer OpenVPN configuration files as well, meaning that we can access and investigate the exact parameters with which the OpenVPN tunnel is established. The systematic analysis of the configuration files, however, did not show anything out of the ordinary with respect to geo-unblocking, which led us to believe that the geo-unblocking mechanism must be located on the server side. We therefore used `traceroute` to get a first impression of the paths the traffic to the VOD providers could take.

Our test led to unexpected results, which were instrumental for defining a model of the VPN ecosystem. Ordinarily, one would expect that `traceroute` would trace a route from the VPN server to the VOD’s homepage, likely with multiple hops depending on the relative location of the source and end point. This is the case, for example, when we issue a request to `example.com` while using a geo-unblocking VPN service (NordVPN), as shown in Fig. 1. However, when contacting a streaming provider (in this case `www.netflix.com`) using the same VPN service, we observe only a single hop as seen in Fig. 2.

From this we can draw two conclusions. Firstly, the IP address the `traceroute` terminates at clearly does not belong to the VOD provider, as the address falls in a prefix that is reserved for IETF Protocol Assignments³. Secondly, as a consequence of receiving these IP addresses, we infer that the commercial VPN providers are manipulating the proper DNS resolution for URLs

³ <https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml>.

Table 1. Manipulated DNS requests from NordVPN’s DNS servers for requests to Netflix’s and Disney+’s homepage and CDN.

| VOD Provider | VPN DNS | Cloudflare DNS |
|------------------------------------------|------------|----------------|
| <code>www.netflix.com</code> | 192.0.0.69 | 54.246.79.9 |
| <code>nflxvideo.net</code> | 192.0.0.69 | 54.155.178.5 |
| <code>www.disneyplus.com</code> | 192.0.0.56 | 23.206.113.15 |
| <code>disney.api.edge.bamgrid.com</code> | 192.0.0.56 | 18.65.39.3 |

belonging to VOD providers by returning IP addresses under their control. This mode of operation closely resembles what is often called a “smart” DNS Service [23]. Table 1 shows a sample of the returned IP addresses when requesting the A records for Netflix’s and Disney+’s landing page and CDN network through NordVPN’s DNS servers. For comparison, Table 1 also shows the expected A records for those domains when connected to NordVPN but forcing the use of Cloudflare’s DNS server, thus showing that DNS manipulation is carried out.

Figure 3 shows a shortened log of trying to fetch Netflix’s homepage via *curl* while being connected to NordVPN. The log shows the connection to 192.0.0.69, and also presents some rudimentary information on Netflix’s TLS certificate. From this log, we inferred the following observation. If the certificate had been self-signed or expired then *curl* would have presented a warning and would not have continued unless instructed to do so. As this was not the case, and considering that the commercial VPN providers cannot terminate the TLS connection, we conclude that our connection to Netflix has been forwarded opaquely. We call these opaque forwarders *TLS forwarding proxies*.

Figure 4 depicts the principal building blocks of the geo-unblocking VPN mechanism that we identified based on our experiments so far. The figure shows the VPN user, who wants to perform geo-unblocking, on the left. The user connects to the VPN provider’s gateway. The configuration of the provider then tells the client to use the VPN provider’s DNS resolver. When the user connects to a streaming service, the VPN provider’s resolver returns an internal IP address that presents as a transparent TLS proxy. The remainder of this paper will focus on what happens to traffic after the TLS forwarding proxies, shedding light on how VPN providers manage to achieve geo-unblocking.

```
tracert to netflix.com (192.0.0.69), 64 hops max, 72 byte packets
1 192.0.0.69
```

Fig. 2. ICMP traceroute to Netflix.com while being connected to NordVPN. RTTs have been omitted for readability.

4 Commercial VPN Provider Selection

The commercial VPN ecosystem is ever-changing, with some providers going out of business [1], or being shut down by law enforcement due to almost exclusively offering their services for criminal purposes [3]. To fill this void, new providers take their places. Some providers stand the test of time and are a stable presence in the industry. In 2018, Khan et al. [26] identified 200 unique commercial VPN providers through three selection methods, namely: popular review site, Reddit crawl and personal recommendation. The fact that neither an exhaustive nor a more systematic approach for selection exists, highlights the size and dynamicity of this industry and also the lack of academic overview.

In this paper, we only consider commercial VPN providers that explicitly offer geo-unblocking. This requirement drastically reduces the set of possible providers. Our selection methodology takes inspiration from the methodology in [26], but rather than focusing on identifying a large number of VPN providers, we focus on building a sample among VPN providers bearing in mind the following guidelines:

- the VPN providers should appear in popular review sites;
- the VPN providers should have geo-unblocking capabilities;
- the selected VPN providers should be representative of different market shares.

With these guidelines in place we were able to execute a more targeted search for providers. We first identify a comprehensive review of existing VPN providers, namely the “VPN TIER LIST” [18]. Similarly to the popular review sites, which were used by Khan et al., the “VPN TIER LIST” maintains a ranking of commercial VPN providers, based on criteria such as pricing or if the user can

```

$ curl https://www.netflix.com -v

* Trying 192.0.0.69:443...
* Connected to www.netflix.com (192.0.0.69) \
port 443 (#0)
...
* Server certificate:
* subject: C=US; ST=California; L=Los Gatos; \
O=Netflix, Inc.; CN=www.netflix.com
* start date: Dec 14 00:00:00 2021 GMT
* expire date: Jan 14 23:59:59 2023 GMT
* subjectAltName: host "www.netflix.com" \
matched cert's "www.netflix.com"
* issuer: C=US; O=DigiCert Inc; CN=DigiCert \
TLS RSA SHA256 2020 CA1
* SSL certificate verify ok.
...

```

Fig. 3. Private IP returns valid certificate for www.netflix.com

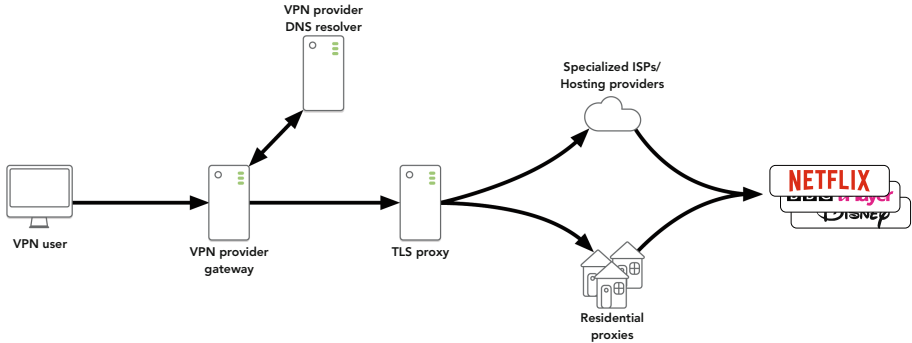


Fig. 4. Inferred geo-unblocking system

fully utilize the promised bandwidth without being throttled. The main difference though is the presence of a “streaming” criterion. This criterion rates the compatibility of a commercial VPN provider to flawlessly work with VOD providers. If we remember that VOD providers usually prohibit the use of VPNs, this compatibility rating is an indication of whether VPN providers are capable of deploying geo-unblocking methods that successfully circumvent blocking by VOD providers. Among the geo-unblocking VPN providers, we select six commercial providers that occupy different roles in the market. In particular, ExpressVPN [6] and NordVPN have been selected because they are established providers with a large market share, as can be inferred by the fact that they are able to allocate significant resources to marketing [7, 21]. WeVPN, on the contrary, is a recent up-and-coming provider, which we expect to still have a limited market share. Manual investigation of CyberGhost, PrivateVPN and Surfshark places those instead as medium-sized providers. Finally, we also checked that all the selected providers actually succeed in geo-unblocking content. To do so, we followed the geo-unblocking instructions from each VPN provider as a regular user would, and tried streaming content that would otherwise be not available in our geographical area.

5 Methodology

In this section, we describe our measurement methodology, which focuses on gaining visibility behind the TLS forwarding proxies we identified in Sect. 3.

5.1 Geo-Unblocking IP Retrieval

The use of TLS forwarding proxies at most commercial VPN providers means that network path information is not available for the entire route from client to VOD CDN endpoint. Instead, we can only observe the path from our client to the host on which the proxy is running, as demonstrated in Sect. 3. To understand


```

Response
HTTP/1.1 403 Forbidden
Content-Type: application/octet-stream
...
Server: nginx
X-TCP-Info: addr=<Our Public IP>;port=58219;

```

Fig. 5. Shortened response of a GET request to Netflix’s video CDN, showing the populated *X-TCP-Info* header.

how geo-unblocking takes place in VPN providers, we need a way to retrieve which IP address the VPN provider uses to connect to the VOD provider.

The analysis of the HTTP header for connections towards Netflix’s CDN provided valuable information in this respect. When a connection request is issued to a Netflix CDN edge server (e.g. *ipv4-c139-ams001-ix.1.oa.netflixvideo.net*), we observed that a custom header (*X-TCP-Info*), likely set by the Netflix CDN itself, is returned. This header contains an IP address. Our hypothesis is that this IP address is actually the IP address of the host initiating the connection to the Netflix CDN.

To verify this hypothesis, we accessed Netflix’s CDN from multiple vantage points under our control, such as residential wired and mobile connections, cloud providers, as well as from workstations at our institute. To simulate a VPN connection we also setup a VPN on a cloud-hosted machine under our control. In all cases, *X-TCP-Info* contains either the IP address of the host we were using for the test, or the external-facing IP of the VPN server, proving that this header contains information about the host initiating the VOD request. In addition, once connected to a geo-unblocking VPN host, we observe that the IP address returned in this header is no longer our own machine’s address, but instead belongs to an unrelated autonomous system. We therefore consider this field as ground truth for the exit-node accessing Netflix, making it an invaluable source of information to map the ecosystem behind the TLS proxy (see Fig. 4).

We have also looked for this kind of header at other popular streaming providers at the time that data collection started, but we were not able to find any. Therefore, in the remainder of the paper, we will focus on Netflix as VOD service at which to direct our requests during our data collection.

Figure 5 shows a snippet of the HTTP response containing the populated *X-TCP-Info* field. Notice also, that the HTTP status code in Fig. 5 is “403 Forbidden”. This is because we accessed Netflix’s CDN node without providing prior authorization on purpose (i.e., without being logged in with a Netflix account). Logging in changes the HTTP status code to “200 OK”, but the returned header fields are the same, including *X-TCP-Info*. We therefore strongly believe our method to be log-in status agnostic.

5.2 Testbed

To automate the retrieval of the header and the extraction of the *X-TCP-Info* field, we set up a testbed in the Netherlands which can support many concurrent VPN connections. A previous study [26] has used virtual machines for this purpose to maintain isolation between the VPNs, but this is not feasible for dozens of concurrent measurements. As a consequence we opted for a more lightweight solution, by using containers with segregated network namespaces. Within each container we establish an OpenVPN connection to a desired geographical unblocking region for every commercial VPN provider we consider. Once the VPN connection is established, we send a single HTTPS request at an interval of 30s to Netflix’s video CDN. For each request we save the following information: the time of the request, the status code of the request (i.e., OK or timeout) and the IP address of the exit-node. We then enrich the collected IP address with AS and (enhanced) geolocation information.

5.3 Geo-Unblocking Regions

Most VPN providers limit the amount of concurrent connections per account. As a result we cannot measure all geo-unblocking regions of a given VPN provider. Instead, we focused on a limited number of regions making sure that these regions are mostly supported by all chosen providers. We have selected the following four regions: USA, Japan, Germany and the Netherlands. The rationale behind these choices is as follows. We chose the USA because US-based VOD providers usually offer a larger content library for their internal market (while rights need to be negotiated for other countries), so we expect that this will draw the attention of geo-unblocking services. Japan has instead been chosen because it is a content creator for niche content, such as Anime, which could also be a reason to trigger geo-unblocking requests. Finally, Germany and the Netherlands are chosen for geographical diversity. In addition, the Netherlands has been chosen because it is known to have a generally good Internet infrastructure, both for consumers as well as for hosting. Table 2 shows that all chosen providers support these regions except CyberGhost, who do not offer geo-unblocking in the Netherlands.

Most VPN providers support at least five concurrent connections, which is why we chose to limit our vantage points to four, leaving one free connection as buffer for timed-out sessions or for debugging purposes.

6 Results

In this section, we discuss the results of the two measurement campaigns we ran. These measurement campaigns, both executed in 2022, are summarised in Table 3. We start with a general overview of our measurements, and then dig deeper into two particular mechanisms that VPN providers use to provide geo-unblocking for their customers. We end the section with an analysis of potential overlap in the backend infrastructures of VPN providers.

Table 2. Matrix showing the availability of measurements of a region per provider.





| Provider | Vantage Point | | | |
|------------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| |  |  |  |  |
| CyberGhost | ✓ | ✓ | ✓ | ✗ |
| ExpressVPN | ✓ | ✓ | ✓ | ✓ |
| NordVPN | ✓ | ✓ | ✓ | ✓ |
| PrivateVPN | ✓ | ✓ | ✓ | ✓ |
| Surfshark | ✓ | ✓ | ✓ | ✓ |
| WeVPN | ✓ | ✓ | ✓ | ✓ |

Table 3. Data set overview

| Measurement | Start date | End date | # samples |
|-------------|------------------|-----------------|-----------|
| #1 | 24 February 2022 | 15 May 2022 | 3,810,624 |
| #2 | 1 July 2022 | 29 October 2022 | 7,059,110 |

6.1 General Characterization of the Geo-Unblocking Ecosystem

We start with a general overview of our two main measurement campaigns as shown in Fig. 6. The graphs are arranged in a matrix where each row represents one of our six measured commercial VPN providers and the columns are the four distinct regions in which we measured. Each element of this matrix consists of two bar charts. The top chart represents the amount of unique IP addresses seen per day, where the bars are color-coded for IP versions, green for IPv4 and pink for IPv6. The overlaying black line visualizes the perceived IP churn, measured as the number of new IP addresses seen each day.

The bottom graphs, which are often more colorful, show a normalized view of the different autonomous systems we encountered per day. Each color represents a distinct AS and the colors are consistent across all graphs. We observed a total of 2,059 distinct ASNs and were therefore not able to give all of them a unique color. To account for this we gave the top 50 ASNs by observations in our data set a unique color, while the remaining ASNs have been colored black.

Based on these plots, we can see a few different geo-unblocking patterns. To start, we focus on the ASN usage. Some providers, for example NordVPN, PrivateVPN and Surfshark in Germany, Japan and the Netherlands, select their VPN exit nodes from a pool belonging to one or at maximum a few ASNs. Differently, providers such as Cyberghost in Germany or ExpressVPN in Germany and Japan, select their IP addresses from a large pool of ASNs.

These patterns are by no means stable over time though, nor are they the same for the same provider in different regions. For example, at CyberGhost in Japan we see their unblocking strategy switch from multiple ASNs to a single one, yet in the United States their strategy changes from a few ASNs to many. We can also see both of these behaviors occur in a single region, for example

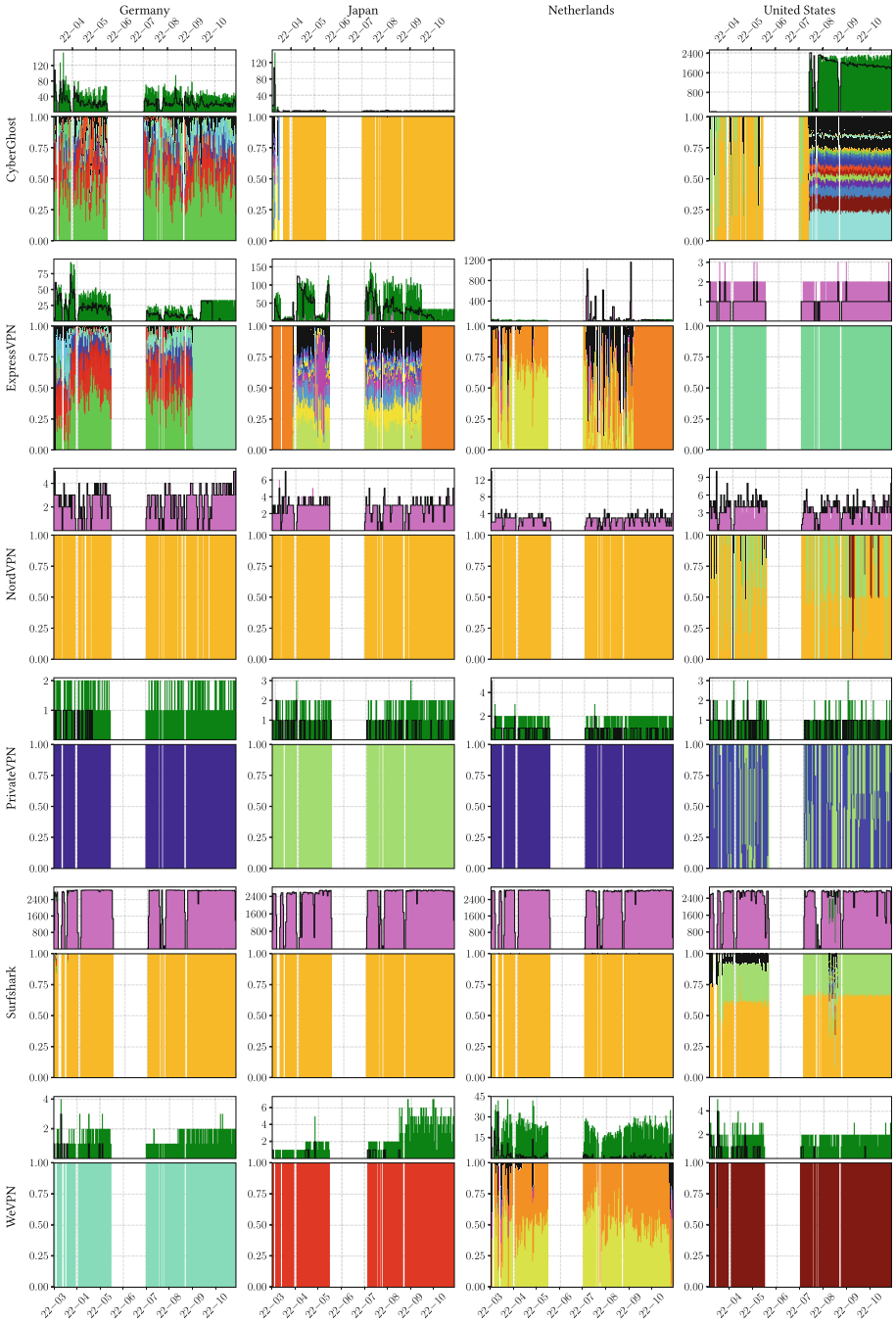


Fig. 6. Bird's view of the geo-unblocking ecosystem

ExpressVPN in Japan, where their unblocking strategy changes from one ASN to many and then reverts back to one.

The difference in ASN usage is not the only noteworthy observation. We now look at the IPv4/v6 usage and churn. Also in this case, the ecosystem shows several different approaches. In the US, CyberGhost relies on many thousands of distinct IPv4 addresses over the entire measurement period, many hundreds of which also seem to be repeating between August and November. Differently, PrivateVPN in Germany uses only 29 IPv4 addresses. These approaches are in sharp contrast to Surfshark’s geo-unblocking solution. Instead of using IPv4, their preferred method is IPv6. Additionally, for every HTTPS request we sent we retrieved a unique IPv6 address, which is indicated by our churn-graph sitting on top of the unique IP graph peaks.

Lastly, we sometimes seem to observe the VPN providers “experimenting” with their settings. For example, Surfshark in the US has four distinct short-lived periods in August, during which we recorded many different ASNs mixed in with their “regulars”. The IP graph in the top plot also indicates the inclusion of IPv4 addresses during these periods. Similarly, ExpressVPN in the Netherlands displays several periods during which the amount of unique IPs spikes above what is generally observed for that provider/region pairing.

These observations raise the question: *Can the different patterns be explained by VPN providers using different mechanisms to facilitate geo-unblocking?* To answer this question, we performed a detailed inspection of the IPs and ASNs we observe for each provider in each region.

For each ASN with a substantial presence in our data set, we manually obtained information on the type of service these ASNs provide, classifying these into two groups: Specialized networks or hosting providers and (apparent) residential Internet service providers.

Specialized Networks/Hosting Providers—The first mechanism we identify is the use of what we call “Specialized Networks” or “Hosting Providers”. This category can be characterized as typically using a small number of ASNs (often, but not always a single one) and a small number of IPs, and the ASNs are characterized – at first glance, e.g., by inspecting their website – as residential access networks. Deeper inspection of these networks, however, reveals that they are in fact not residential access providers, but only masquerade as such. An especially interesting case in this category is PrivateVPN, which is the only provider in our set that does not use TLS proxies. Instead, it entirely relies on the specialized ISP model. We discuss this category in more detail in Sect. 6.2.

Residential ISPs – The second mechanism we identify is the use of proxies located at residential ISPs. VPN providers and regions that use this mechanism can be characterized by the use of a large(r) number of ASNs and larger numbers of unique IP addresses. The ASNs can all be categorized as legitimate ISPs that provide residential and/or business services, and the IP addresses reflect this as well (based on reverse DNS entries and geolocation). We discuss this category in more detail in Sect. 6.3.

Table 4. Unblocking behavior for each provider region

| | Germany | Japan | Netherlands | United States |
|------------|---------|-------|-------------|---------------|
| CyberGhost | R | R→H | <i>n/a</i> | H→R |
| ExpressVPN | R→H | H→R→H | R→(R+H)→H | R |
| NordVPN | H | H | H | H→(H+R) |
| PrivateVPN | H | H | H | H |
| Surfshark | H | H | H | H→(H+R)→H |
| WeVPN | H | H | R | R |

(R = Residential, H = Specialized ISP/Hosting Provider)

Figure 6 shows that the geo-unblocking ecosystem is highly dynamic, suggesting that VPN providers are willing to put considerable effort into enabling their unblocking mechanisms. To further highlight this dynamicity, Table 4 summarizes our results in terms of the changes we observe in behavioral patterns among the considered providers and geographic regions. In the table, we indicate with H a provider unblocking strategy based on the use of specialized networks/hosting providers, and with R a strategy based on residential ISPs. An arrow indicates a change in strategy. The table shows a variety of mechanism dynamics per region. What really stands out is the lack of a clear trend or overall strategy, even for each provider separately. In this, a few examples stand out. In Fig. 6 we see that ExpressVPN in the US makes use of a single ASN, which would typically indicate that this provider relies on a specialized network/hosting provider. However, in this case we were able to verify (by asking the ASN operator, a large US ISP, directly), that the IPs used for ExpressVPN operations were actually all allocated for residential use. We also observe that the same operator can choose a completely different approach in different geographical zones. This is for example the case of NordVPN in the US (hosting) compared to the other zones. PrivateVPN seems to use the same mechanism. However, this is a particular case that we will discuss in more detail in Sect. 6.2. Finally, Surfshark in the US shows only a temporary switch from a hosting mechanism, to residential and back to hosting. We speculate, given how stable their behavior in the US zone has been throughout the entire measurement, this is rather a fluke in their infrastructure than a real behavioral change.

Not only do geo-unblocking mechanisms change drastically within the same provider from measurement #1 to measurement #2, but within that same provider they are also substantially different from region to region. Such observations clearly provide hints that providers are willing to tailor their unblocking mechanisms to what works best at a specific moment in time and in a specific region. While it is hard to substantiate this without insider knowledge on how the VPN providers run their operation, we speculate that these changes are evidence of the arms race between VPN providers that want to offer geo-unblocking

to their customers, and streaming providers that want to stop viewers from circumventing geo-fencing of content [5].

In the remainder of our analysis, we will provide more details on the categories of “Specialized Networks/Hosting Providers” and “Residential ISPs” in Sects. 6.2 and 6.3 respectively. The dynamics we observe suggest that the VPN provider ecosystem w.r.t. geo-unblocking is in constant evolution, probably because providers constantly look for IPs that do not appear in blocklists. This brings forward the question if providers also share these resources, or if they differentiate their infrastructure. We will look into this in Sect. 6.4.

Key Takeaways: *Analysis of regional Internet registry data for the IP addresses involved in geo-unblocking indicates that there are two main approaches to geo-unblocking: specialized networks and residential ISPs. Furthermore, we see strong indications that VPN providers adapt their behavior. This may be driven by attempts of the VOD providers to block them, or alternatively, the change in behavior may also be a result of a need to have more bandwidth available to satisfy the demand of their customers. As an external observer, however, we cannot ascertain whether either of these two is the case or not.*

6.2 Specialized Networks/Hosting Providers

We now take a deeper look at the specialized networks/hosting provider category we identified as being used by VPN providers to facilitate geo-unblocking earlier. We first look at hosting providers, in particular what we consider *non top-tier hosting providers*. These providers offer all of the services one might expect from a hosting provider, such as virtual private servers (VPS), dedicated servers or rack space to retail customers. Yet they are not one of the well-known major international players in the hosting business. The combination of these two attributes gives the VPN providers ample bandwidth to power their geo-unblocking network while also staying under the radar of enhanced geolocation database providers. Examples of these providers are Inter Connex (AS13737 INCX Global, LLC), which operates from two data centers in the US (Detroit, MI and Kansas City, MO), and Starry DNS, which is a service provider based in Hong Kong with a small presence in the EU and US as well (AS134835 Starry Network Limited).

Key Takeaway: *It is possible for VPN providers to find lesser known hosting providers that are not listed in enhanced geolocation databases. However, this reveals an intrinsic fragility in the ecosystem as such hosting providers could be listed in those databases at any moment.*

The other subclass, *specialized ISPs*, can generally be described as IP space brokers. They often directly advertise that they monetize unused IP addresses, by renting them to interested parties or have a certain quantity of IP ranges on lease. Examples are IPXO [12] or Xantho UAB [20]. In some cases only a cryptic static landing page (if at all) informs potential customers of their services. This is the case, for example, for Trafficforce UAB (<https://trafficforce.lt/>), which has a very minimalist Web presence, but their IP addresses are in use in no fewer than four different VPN providers (Surfshark, NordVPN, ExpressVPN and CyberGhost).

Table 5. Matrix of PVDDataNet AB and Telia Company AB’s ASes and IPs per vantage point and the corresponding maintainer according to RIPE. IPs are represented by their network prefix.

| Country | AS | IP | RIPE Maintainer |
|---------------|-----------------------------|------------------|---------------------------------|
| Germany | Telia Company AB (AS1299) | 193.104.198.0/24 | Nordic Internet Service AB |
| | | 80.239.128.0/19 | Privat Kommunikation Sverige AB |
| Japan | Datacamp Limited (AS212238) | 193.234.55.0/24 | PVDDataNet AB |
| Netherlands | Telia Company AB (AS1299) | 80.239.128.0/19 | Privat Kommunikation Sverige AB |
| United States | Telia Company AB (AS1299) | 193.104.198.0/24 | Nordic Internet Service AB |
| | PVDDataNet AB (AS42201) | 45.130.86.0/24 | PVDDataNet AB |

What differentiates this subclass from non top-tier hosting providers is that the organisations in this category generally do not service any retail customers and have optimized their business model to monetize IP addresses.

Key Takeaway: *The use of specialised ISPs, especially those that are used by multiple VPN providers, suggests that there may exist a specialised market that caters to the needs of VPN providers for the combination of sufficient bandwidth coupled with IP addresses that are not blocked by VOD providers.*

Finally, we want to highlight one particular model that does not fit well into either category. In particular we want to spotlight a company that appears to be wholly owned and operated by PrivateVPN, for the sole purpose of appearing to be a consumer ISP. This company, called Nordic Internet Service AB came to light when we performed further investigation of the IP ranges we collected during our measurement. In particular, this concerns IP ranges that belong to either Telia Company AB (AS1299), Datacamp Limited (AS212238) or PVDDataNet AB (AS42201). Looking at the administrative information in the RIPE database, the so-called maintainer object of these IP ranges shows that they are delegated to either Nordic Internet Service AB, Privat Kommunikation Sverige AB or PVDDataNet AB as shown in Table 5.⁴

We consulted the Swedish companies registration office (Bolagsverket) for additional information on the companies listed as RIPE maintainers, due to their similarity in name. What we found is that the CEO for PrivateVPN Global AB and Nordic Internet Service AB is the same person. Furthermore, this person also acts as ordinary board member for PVDDataNet AB. We therefore conclude that PVDDataNet AB, Nordic Internet Service AB and PrivateVPN Global AB, are essentially the same entity.

⁴ Note that, at the time of writing, some IP ranges have already been re-allocated to different providers and current RIR data might not reflect the data of this table.

Table 6. Residential ISPs with the largest amount of unique IPs per core unblocking region.

| Country | AS | n |
|---------------|-----------------------------|--------|
| Germany | Deutsche Telekom (AS3320) | 2,412 |
| | Vodafone (AS3209) | 1,143 |
| Japan | NTT (AS4713) | 1,052 |
| | Softbank (AS17676) | 724 |
| Netherlands | Vodafone Libertel (AS33915) | 347 |
| | KPN (AS1136) | 319 |
| United States | Comcast (AS7922) | 48,288 |
| | AT&T (AS7018) | 24,306 |

PVDataNet AB and Nordic Internet Service AB are also both registered local Internet registries (LIR) with RIPE, meaning that they can get IP address ranges assigned to them by an RIR, or have their own AS. From this publicly available information we conclude that PrivateVPN is using shell companies under their control for two specific goals. Firstly, by being a registered LIR they can easily enter the commercial Internet transit market to buy transit and IP addresses in a region they would like to geo-unblock. And secondly, by creating the impression of being a consumer ISP, they evade classification by enhanced geolocation databases, which in turn allows for geo-unblocking.

Key Takeaway: *Some VPN providers are willing to go the extra mile by seriously investing in their own dedicated infrastructure in order to circumvent VPN detection.*

6.3 Residential Proxies

The second class of geo-unblockers are residential proxies. Residential proxies, as the name suggests, run on hardware which is connected via consumer ISPs to the Internet. More research into this area is needed to understand the nature of these proxies, although other studies suggest that these proxies sometimes consist of compromised devices [22, 28, 31]. Residential Internet connections in general still have asymmetric network speeds, making them a sub-par solution compared to data center connectivity, which is what the first geo-unblocking solution would provide. On top of that, residential proxies might be less stable since they might be hosted on devices which are regularly turned off.

And yet, in all of our measurement regions we have identified major residential ISPs. Table 6 shows the unique IPs we identified per major residential ISP. Despite the intuition that residential proxies may be less reliable than specialized ISPs or hosting, we observe very large numbers of residential addresses being used in geo-unblocking, take for example the tens of thousands of IPs observed in two large US ISPs as shown in Table 6.

Table 7. Appearance of unique IPs which can be described as belonging to educational institutes (measurement campaign #1 and #2 combined).

| Region | VPN Provider | n |
|---------------|--------------|-----|
| Germany | ExpressVPN | 17 |
| Germany | Surfshark | 2 |
| Japan | ExpressVPN | 3 |
| United States | CyberGhost | 95 |
| United States | Surfshark | 17 |

We not only see classic residential ISPs though. As a consequence of the fact that those proxies run on user computers, we have noticed that some geo-unblocking exit points appear in a variety of networks, even some where VOD streaming traffic might be odd. For example, we identified a residential proxy running on an IP belonging to the address space of the Ministry of Defense of a European country (which we have duly notified). Educational institutions are another example of networks where we observe VPN proxies, as we have detailed in Table 7. Those examples suggest that there are not only a few major players in the field of residential connection providers hosting VPN proxies, but that there is also a long tail of exit nodes distributed over numerous other networks.

We have been in contact with several operators of residential ISPs as well as educational networks to confirm our hypothesis that our recorded IPs largely belong to residential end-users and are not freely available to rent. The two residential ISP operators from two different countries (the US and Japan) provided us with ground truth that shows that the overwhelming majority of IPs belong to residential connections. In one case the operators indicated the occurrence of their commercial cloud in our data set ($\sim 3.7\%$).

In the case of the educational institutes we contacted (in two countries), we received confirmation that all but one IP were used by students or belonged to student housing, while the remaining IP belonged to the workstation of a university employee.

Key Takeaway: *The fact that VPN providers are willing to use “unreliable” residential connections means that this is still a mechanism that pays off, most likely w.r.t. evading VPN detection mechanisms.*

6.4 VPN Infrastructure Overlap

The availability of IP space that has not yet been tagged by an enhanced geolocation database (and thus aids in evading VOD VPN detection mechanisms) could be considered a precious, if not rare, commodity. This therefore brings about the question if VPN providers share their underlying unblocking infrastructure. We have investigated this by first looking into the number of unblocking IP addresses that occur at multiple VPN providers. From a total of 214,993 unique IPv4 and 1,925,327 unique IPv6 addresses, we only found an overlap of 273 IPv4 addresses

Table 8. Amount of ASNs shared between distinct number of VPN providers

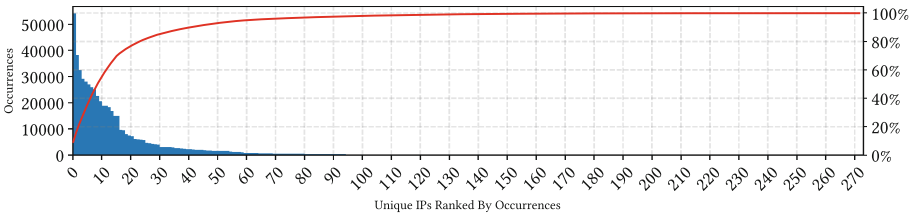
| | | | | | |
|-------------------------|---|---|----|-----|------|
| Distinct ASNs | 2 | 8 | 40 | 414 | 1582 |
| Shared by N Providers | 5 | 4 | 3 | 2 | 1 |

($\sim 0.1\%$) and no IPv6 addresses. These 273 IPv4 addresses in turn account for only $\sim 5.8\%$ of all observations (580,360 of 9,987,688). Even within this set of IPv4 addresses, the distribution is not uniform. As Fig. 7 shows, roughly 10 IPs make up half and about 40 IPs are responsible for 90% of our overlapping observations. In other words, based on these numbers we assume that it is highly unlikely that the VPN providers share a common geo-unblocking platform.

Taking a step back though and looking at a coarser-grained set of data, namely ASNs, we can see a different picture. In total, we observed 2,046 distinct ASNs of which 464 ($\sim 22.7\%$) have been found to overlap between the different VPN providers. Table 8 shows how often ASNs that overlap occur in our dataset.

Generally speaking the amount of shared ASNs resembles a heavy-tailed distribution and can be seen in Fig. 8. Just two ASNs (AS212144 (45.3%) and AS212238 (11.1%)) make up 56.4% of all overlapping observations. More importantly, though, they make up 48.8% of *all* observations in our data set. The first ASN, AS212144, Trafficforce UAB (which we discussed previously in Sect. 6.2) is shared among four of the VPN providers (NordVPN, Surfshark, CyberGhost, ExpressVPN) and the latter, AS212238, Datacamp Ltd. (which announces IP space for Trafficforce) is shared among five (PrivateVPN, CyberGhost, Surfshark, NordVPN, ExpressVPN). This can also be noticed in Fig. 6 by keeping in mind that the same ASN is plotted in the same color throughout the picture.

Key Takeaway: *The majority of overlap in infrastructure between VPN providers lies with just a few distinct ASNs that seemingly belong to a class of service provider that caters well to the need of VPN providers that want to perform geo-unblocking. Nevertheless, we also still see evidence of overlap in residential connections*

**Fig. 7.** Number of overlapping IPv4 addresses and amount of occurrences in our data set

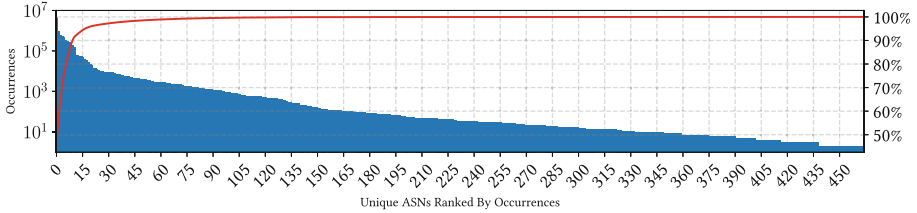


Fig. 8. Number of overlapping ASNs and amount of occurrences in our data set

7 Ethical Considerations

The work described in this paper has presented us with several different ethical dilemmas that affect many of the different stakeholders in this context. In this section we aim to provide an overview of the ethical challenges that we identified and explain how we handled them to minimize impact on the relevant stakeholders.

7.1 Ecosystem

The ecosystem of VPN providers in the context of geo-unblocking and Video-on-Demand (VOD) providers creates tensions. As described in Sect. 3 VOD providers put measures in place to restrict material due to distribution right restrictions. VPN providers in contrast advertise with geo-unblocking capabilities to allow VPN users to circumvent the restrictions put in place by the VOD providers. VOD providers in turn aim to detect the circumvention methods, which causes VPN providers to come up with alternative ways to route traffic and evade this detection.

This context presents ethical tensions:

- Users may use the VPN services to circumvent the geo-blocking measures of VOD providers, which breaks the terms of service of most of these services, and may even be illegal in some jurisdictions.
- VOD providers currently restrict content due to licensing agreements, and have put detection capabilities in place to prevent geo-unblocking. Research into this context provides them with additional information on the practices, allowing (or perhaps even forcing) them to improve their detection capabilities.
- VPN providers on the other hand advertise with the geo-unblocking capability. Our research into this practice may hurt their business practices.

7.2 VPN Provider Selection

As described in Sect. 4 the VPN ecosystem is ever-changing, in part due to catering to the criminal market. For this reason we limited our research to long-lived commercial providers that presented geo-unblocking capabilities.

While the practice of geo-unblocking in the context of VOD may be breaking terms of service, we are aware that there might also be legitimate uses of geo-unblocking.

7.3 Methodology and Results

While designing our measurement system and exploring the systems and capabilities of the VPN providers, we discovered that routes could also include personal networks. This meant that we would record personally identifiable information in recording traffic routes.

It was impossible for us to request informed consent from the users of the residential IP addresses, as there was no way for us to contact them directly. To mitigate impact on these individuals we secured our testbed which we described in Sect. 5. We secured this testbed so that only the researchers had access to the data, and further restricted access to just our university's network.

In the paper we only use aggregated results that do not identify specific users, and we will not voluntarily share the data with others. Furthermore, the recording of this personal data has been registered at the university following the official processes required by the GDPR.

An approval record from our institution's ethics board is available under registration number *redacted*.

8 Conclusion

Both streaming and VPNs are multi-billion dollar industries [16, 17]. The two are constantly locked in an arms race where VPN providers are trying to offer geo-unblocking to their customers and VOD providers are trying to enforce restrictions on the content delivery to certain regions to enforce licensing agreements.

In this paper we shed first light on how VPN providers circumvent geo-blocking restrictions. Our main findings are three-fold. Firstly, VPN providers use different mechanisms for bypassing geo-blocking, making use of specialized networks/hosting providers and residential ISPs. Secondly, VPN providers use different mechanisms in different geographical regions, thus adapting their behavior to what best ensures escaping VOD detection mechanisms. Finally there are also temporal dynamics, i.e., the approaches change at different moments in time, even within the same provider. These findings paint a picture of the geo-unblocking VPN providers' ecosystem as highly dynamic and adaptable. Given the value of the market we expect this arms race to continue in a future where we might see even *Stranger VPNs*.

References

1. Tunnelr - maintenance mode - we'll be right back! (2018). <https://www.tunnelr.com/>
2. Digital element commemorates 20th anniversary (2019). https://www.digitalelement.com/digital_element_20th_anniversary/

3. Cybercriminals' favourite VPN taken down in global action (2020). <https://www.europol.europa.eu/media-press/newsroom/news/cybercriminals'-favourite-vpn-taken-down-in-global-action>
4. Hulu help center - i'm getting an anonymous proxy error (2021). <https://www.help.hulu.com/s/article/anonymous-proxy-error>
5. Netflix intensifies 'VPN Ban' and targets residential IP-addresses too (Updated) * TorrentFreak (2021). <https://www.torrentfreak.com/netflix-intensifies-vpn-ban-and-targets-residential-ip-addresses-too-210811/>
6. Top podcast advertisers USA 2021 (2021). <https://www.statista.com/statistics/1273734/podcast-advertisers-usa/>
7. Brands with highest youtube influencer marketing spend 2020 (2022). <https://www.statista.com/statistics/1267365/youtube-influencer-marketing-spenders/>
8. Error code 73: 'Disney+ is only available in certain regions...' (2022). https://www.help.disneyplus.com/csp?id=csp_article_content&sys_kb_id=bd59d944db08d9943142eb2ed396199a
9. Geo-blocking security & filtering — Video streaming with geo blocking (2022). <https://www.streamingvideoprovider.com/secure-streaming/geo-blocking-restrcitions/>
10. HBO Max — Find out what to do if you're getting an 'HBO Max isn't available in your region' message. (2022). <https://www.help.hbomax.com/us/Answer/Detail/000001252>
11. How Netflix licenses TV shows and movies (2022). <https://www.help.netflix.com/en/node/4976>
12. Monetize the Unused IPv4 Space. Quick Setup & Easy-to-Use (2022). <https://www.ipxo.com/monetize-ips/>
13. Netflix says 'You seem to be using an unblocker or proxy'. (2022). <https://www.help.netflix.com/en/node/277>
14. Netflix thinks I'm in a different country (2022). <https://www.help.netflix.com/en/node/26100>
15. Prime video: help (2022). https://www.primevideo.com/help/ref=atv_hp_nd_cnt?nodeId=GU85HKX66NVFNQ9Y
16. Streaming worldwide (2022). <https://www.statista.com/study/112979/streaming-worldwide/>
17. VPN market size worldwide 2027 (2022). <https://www.statista.com/statistics/542817/worldwide-virtual-private-network-market/>
18. VPN tier list 2022 (2022). <https://www.vpntierlist.com/vpn-tier-list-2022>
19. Where is Disney+ available? (2022). https://www.help.disneyplus.com/csp?id=csp_article_content&sys_kb_id=27544637dbb23894ac7ceacb1396197e
20. Xantho IP space lease (2022). <https://www.xantho.lt/>
21. Akgul, O., Roberts, R., Namara, M., Levin, D., Mazurek, M.L.: Investigating influencer VPN Ads on YouTube. In: 2022 IEEE Symposium on Security and Privacy (SP), pp. 876–892. IEEE, San Francisco, CA, USA (2022). <https://doi.org/10.1109/SP46214.2022.9833633>
22. Chung, T., Choffnes, D., Mislove, A.: Tunneling for transparency: a large-scale analysis of end-to-end violations in the internet. In: Proceedings of the 2016 Internet Measurement Conference, pp. 199–213. ACM, Santa Monica California USA (2016). <https://doi.org/10.1145/2987443.2987455>
23. Fainchtein, R.A., Aviv, A.J., Sherr, M., Ribaldo, S., Khullar, A.: Holes in the geofence: privacy vulnerabilities in "Smart" DNS services. *Proceed. Priv. Enhanc. Technol.* **2021**(2), 151–172 (2021). <https://doi.org/10.2478/popets-2021-0022>

24. Huffaker, B., Fomenkov, M., claffy, k.: Geocompare: a comparison of public and commercial geolocation databases. Tech. Rep. (2011)
25. Ikram, M., Vallina-Rodriguez, N., Seneviratne, S., Kaafar, M.A., Paxson, V.: An analysis of the privacy and security risks of android VPN permission-enabled apps. In: Proceedings of the 2016 Internet Measurement Conference, pp. 349–364. ACM, Santa Monica California USA (2016). <https://doi.org/10.1145/2987443.2987471>
26. Khan, M.T., DeBlasio, J., Voelker, G.M., Snoeren, A.C., Kanich, C., Vallina-Rodriguez, N.: An empirical analysis of the commercial VPN ecosystem. In: Proceedings of the Internet Measurement Conference 2018, pp. 443–456. ACM, Boston MA USA (2018). <https://doi.org/10.1145/3278532.3278570>
27. McDonald, A., et al.: 403 forbidden: a global view of CDN geoblocking. In: Proceedings of the Internet Measurement Conference 2018, pp. 218–230. IMC 2018, Association for Computing Machinery, New York, NY, USA (2018). <https://doi.org/10.1145/3278532.3278552>
28. Mi, X., et al.: Resident evil: understanding residential IP proxy as a dark service. In: 2019 IEEE Symposium on Security and Privacy (SP), pp. 1185–1201. IEEE, San Francisco, CA, USA (2019). <https://doi.org/10.1109/SP.2019.00011>
29. Perta, V.C., Barbera, M.V., Tyson, G., Haddadi, H., Mei, A.: A glance through the VPN looking glass: IPv6 leakage and DNS Hijacking in commercial VPN clients. *Proceed. Priv. Enhanc. Technol.* **2015**(1), 77–91 (2015). <https://doi.org/10.1515/popets-2015-0006>
30. Ramesh, R., Evdokimov, L., Xue, D., Ensafi, R.: VPNalyzer: systematic investigation of the VPN ecosystem. In: Proceedings 2022 Network and Distributed System Security Symposium. Internet Society, San Diego, CA, USA (2022). <https://doi.org/10.14722/ndss.2022.24285>
31. Tosun, A., De Donno, M., Dragoni, N., Fafoutis, X.: RESIP host detection: identification of malicious residential IP proxy flows. In: 2021 IEEE International Conference on Consumer Electronics (ICCE). pp. 1–6. IEEE, Las Vegas, NV, USA (2021). <https://doi.org/10.1109/ICCE50685.2021.9427688>
32. Weinberg, Z., Cho, S., Christin, N., Sekar, V., Gill, P.: How to catch when proxies lie: verifying the physical locations of network proxies with active geolocation. In: Proceedings of the Internet Measurement Conference 2018, pp. 203–217. ACM, Boston MA USA (2018). <https://doi.org/10.1145/3278532.3278551>
33. Winter, P., Padmanabhan, R., King, A., Dainotti, A.: Geo-locating BGP prefixes. In: 2019 Network Traffic Measurement and Analysis Conference (TMA), pp. 9–16. IEEE, Paris, France (2019). <https://doi.org/10.23919/TMA.2019.8784509>