Why E.T. Can't Phone Home: A Global View on IP-based Geoblocking at VoWiFi

Gabriel K. Gegenhuber
gabriel.gegenhuber@univie.ac.at
University of Vienna
Faculty of Computer Science
Doctoral School Computer Science
Vienna, Austria

Philipp É. Frenzel
pfrenzel@sba-research.org
SBA Research
Vienna, Austria

Edgar Weippl
edgar.weippl@univie.ac.at
University of Vienna
Faculty of Computer Science
Vienna, Austria

ABSTRACT

In current cellular network generations (4G, 5G) the IMS (IP Multimedia Subsystem) plays an integral role in terminating voice calls and short messages. Many operators use VoWiFi (Voice over Wi-Fi, also Wi-Fi calling) as an alternative network access technology to complement their cellular coverage in areas where no radio signal is available (e.g., rural territories or shielded buildings). In a mobile world where customers regularly traverse national borders, this can be used to avoid expensive international roaming fees while journeying overseas, since VoWiFi calls are usually invoiced at domestic rates. To not lose this revenue stream, some operators block access to the IMS for customers staying abroad.

This work evaluates the current deployment status of VoWiFi among worldwide operators and analyzes existing geoblocking measures on the IP layer by measuring connectivity from over 200 countries. We show that a substantial share (IPv4: 14.6%, IPv6: 65.2%) of operators implement geoblocking at the DNS- or VoWiFi protocol level, and highlight severe drawbacks in terms of emergency calling service availability.

CCS CONCEPTS

• **Networks** → **Mobile networks**; *Network management*; • **Security and privacy** → *Mobile and wireless security*.

KEYWORDS

geoblocking, telecommunication, roaming, cellular networks, mobile networks, VoWiFi, Wi-Fi calling, IMS, net neutrality, censorship, network measurements

ACM Reference Format:
Gabriel K. Gegenhuber, Philipp É. Frenzel, and Edgar Weippl. 2024. Why E.T. Can't Phone Home: A Global View on IP-based Geoblocking at VoWiFi . In *The 22nd Annual International Conference on Mobile Systems, Applications and Services (MOBISYS '24), June 3–7, 2024, Minato-ku, Tokyo, Japan.* ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3643832.3661883

MOBISYS '24, June 3–7, 2024, Minato-ku, Tokyo, Japan

ACM ISBN 979-8-4007-0581-6/24/06.
https://doi.org/10.1145/3643832.3661883

1 INTRODUCTION

Mobile network services are a crucial lifeline in today's society, given that in 2023 over 5.4 billion people relied on cellular networks for connectivity and communication [44]. With 4G currently being the most used wireless standard and 5G rapidly gaining penetration, numerous operators are actively decommissioning older legacy networks (2G and 3G), marking the completion of the shift from circuit-switched to a comprehensive packet-switched network paradigm.

In the packet-switched domain, operators use VoIP (Voice over IP) based technology to terminate voice calls and messages. Additionally to the VoLTE (Voice over LTE) standard, VoWiFi (Voice over Wi-Fi, also known as Wi-Fi calling) was introduced. While VoLTE uses the traditional radio infrastructure that is provided by the operator as its access medium, VoWiFi is a complementary solution that allows the use of third-party wireless networks as an alternative uplink to the operator. Consequently, customers can leverage existing Wi-Fi access points (APs) and continue utilizing their mobile phones for voice calls in areas with poor or no cellular reception.

To support this functionality, operators need to expose parts of their infrastructure to the public Internet. This opens new possibilities for active measurement studies since it allows the investigation of exposed parts of a mobile network without requiring any radio equipment. Moreover, it allows measuring a huge number of international operators, without the need for sophisticated measurement hardware at the target locations.

Presumably, the general idea behind VoWiFi is to expand the cellular coverage to allow uninterrupted service e.g., in rural areas with weak reception. Thereby, a voice call can be handed over from VoLTE to VoWiFi, and vice versa, on the fly. However, VoWiFi can also be used completely independent from VoLTE, i.e., it requires no radio signal at all and also works e.g., when the mobile phone is in airplane mode but has Wi-Fi connectivity. In a mobile world that facilitates seamless transitions across national borders, it thereby can also be used overseas, possibly allowing customers to escape from

Figure 1: An Indian operator states in the FAQs [2] that VoWiFi cannot be used during international roaming.

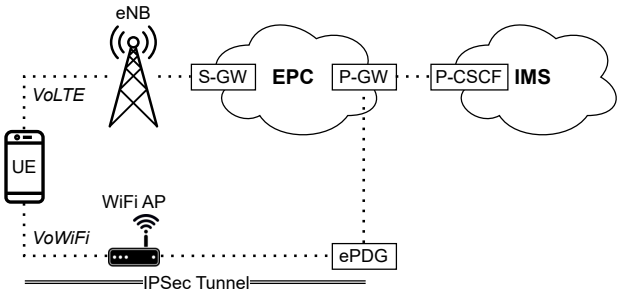

Figure 2: (Simplified) LTE network architecture for VoLTE and VoWiFi.

expensive roaming fees. In practice, some operators are actively denying their customers access to VoWiFi from foreign countries, as the screenshot in Figure 1 shows.

This paper aims to offer a comprehensive overview of the global deployment of VoWiFi and analyzes geoblocking measures of worldwide operators. More specifically, we use commercial VPN- and cloud services to simulate customers connecting from a diverse set of distinct foreign locations and to thereby determine geoblocking measures.

In summary, the main contributions of this paper are as follows:

- We propose a methodological approach to discover existing VoWiFi deployments and to probe them for IP-based geoblocking measures.
- We map the current VoWiFi support at worldwide operators, analyze the used infrastructure and give an overview of the latest global market penetration.
- We probe worldwide operators for IP-based geoblocking both at the DNS- and VoWiFi-protocol levels and provide an overview of current practices.

The remainder of the paper is organized as follows. Section 2 introduces the topic by providing background knowledge on the architecture and implementation of VoWiFi. In Section 3, we describe our methodological approach to discover and probe the VoWiFi infrastructure of global operators. Section 4 presents the results that were collected throughout this study and Section 5 briefly outlines related studies. Finally, we discuss our results and limitations in Section 6 and draw final conclusions in Section 7.

2 BACKGROUND

Figure 2 compares VoLTE and VoWiFi within a simplified cellular network architecture. For the sake of clarity, we've excluded several nonsubstantial components. Furthermore, we stick to the terminology that was specified in LTE, while later generations often introduced new names for similar components or services (e.g., VoLTE is called Voice over New Radio (VoNR) or Voice over 5G (Vo5G) in the fifth network generation).

***3GPP Access*, Voice over LTE (VoLTE).** As shown in the upper path of Figure 2, the User Equipment (UE) attaches to a base station (Evolved Node B (eNB) in LTE) via the Radio Acces Network (RAN). The Serving Gateway (S-GW) and the Packet Data Network Gateway (P-GW) within the Evolved Packet Core (EPC) system are responsible for assigning IP addresses to Access Point Names (APNs) and for routing and forwarding the traffic to external Packet Data Networks (PDNs). Finally, the Proxy Call Session Control Function (P-CSCF) acts as a Session Initiation Protocol (SIP) proxy and is the ingress point to the IP Multimedia Subsystem (IMS). All data traffic between the UE and the P-CSCF is encapsulated in an IPsec tunnel. The UE can then directly send SIP messages, e.g., after successful establishment of the IPSec tunnel it can send a *SIP REGISTER* request to the IMS core network. While SIP is used for signaling, the actual audio stream of a call is transferred via the Real-Time Transport Protocol (RTP).

***Non 3GPP Access*, Voice over WiFi (VoWiFi, Wi-Fi Calling).** In this scenario (lower path of Figure 2), the UE does not use the operator's RAN, but connects via an *untrusted* Wi-Fi Access Point (AP). More specifically, it establishes another IPsec tunnel to an Evolved Packet Data Gateway (ePDG) that is accessible via the public Internet. After successful authentication of the UE (via its IMSI and the cryptographic keys that are saved on the SIM card) and establishment of the IPSec tunnel between UE and ePDG, all traffic is forwarded to the IMS via the P-GW. Note that for VoWiFi, the SIP traffic is actually wrapped within two different IPSec tunnels (i.e., the first between the UE and ePDG, and the second between the UE and P-CSCF).

Internet Protocol Security (IPsec). As described above, VoLTE and VoWiFi heavily rely on IPSec [16] for authentication and traffic encapsulation. To set up a Security Association (SA) it uses the Internet Key Exchange (IKE) protocol. More specifically it uses IKEv2 [26, 27] with EAP-AKA [4] (Authentication and Key Agreement) for key derivation and thereby leverages the SIM card's secret keys to obtain a new session key. The negotiation can be divided into two phases: `IKE_SA_INIT` that negotiates the ciphering suite and other security parameters, and `IKE_AUTH` where the SIM card authenticates by solving a random challenge using its secret keys.

3 METHODOLOGY

VoWiFi calls are usually issued via domestic Wi-Fis, i.e., the customer's location can be inferred by looking at the client's IP address. For VoWiFi, the UE needs to communicate with at least two servers, as shown in Figure 3. After discovering the responsible ePDG IPs via DNS (1, 2), the UE establishes a secure connection to the ePDG (3, 4, 5) that will be used to terminate calls and messages.

There are multiple ways for an operator to block VoWiFi based on a subscriber's IP address:

DNS. Global companies often use GeoDNS (also GeoIP) to minimize network latency by pointing their clients to a geographically close server. Similarly, this can be used for geoblocking, by configuring the responsible DNS server to ignore queries that stem from unwanted client countries. Due to caching and the recursive manner of DNS, this method is relatively inaccurate and might nevertheless leak IP addresses. Finally, there are relatively easy anti-blocking techniques, e.g., skillful customers can use custom DNS servers or manually add host entries to circumvent geoblocking.

ePDG. To achieve more effective blocking, operators can also implement measures at the ePDG. As an example, an operator could

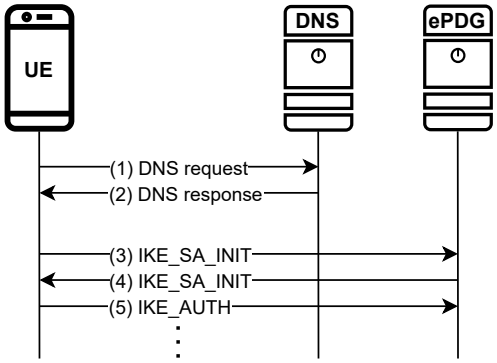

Figure 3: To connect via VoWiFi, the client fetches the ePDGs IP address via the DNS server and starts the IKE negotiation with the ePDG.

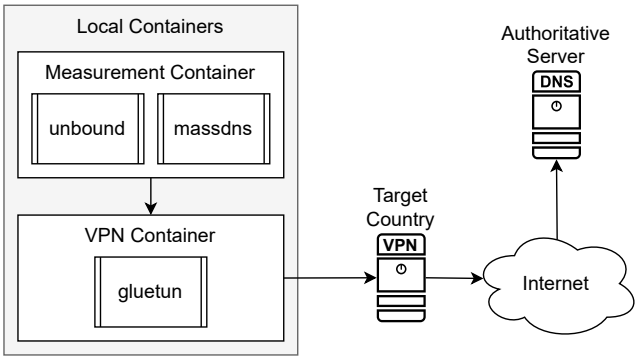

Figure 4: A containerized architecture isolates independent measurements and enables parallel execution for simple upscaling.

simply deploy firewall rules on their ePDGs to drop packets from IPs that do not belong to the domestic country. Additionally, operators could develop more complex rules that only permit specific *premium users* (identified by their IMSI), or also check the latest roaming status (via radio) of a subscriber before deciding whether to block the connection. To achieve worldwide coverage in our study, we decided to focus on straightforward IP-based rules because it does not require the acquisition of SIM cards of the tested operators.

To allow structured testing, our methodological approach is divided into two steps: (i) mapping DNS records and (ii) probing the actual servers.

3.1 Mapping DNS Records

The Fully Qualified Domain Name (FQDN) of an ePDG is specified in 3GPP TS 23.003 [12] and can be built from an operator's Mobile Country Code (MCC) and Mobile Network Code (MNC):

```
epdg.epc.mnc{y}.mcc{x}.pub.3gppnetwork.org
```

According to the specification, the MCC (x) always consists of three decimal digits, while the MNC (y) can be either two or three decimal digits. The first digit of the MCC is allocated according to the geographic region of the operator and thereby easily allows to differentiate operators based within different continents e.g., Europe or North America.

If we want to get an exhaustive list of ePDGs from all operators around the globe, requesting the IP addresses via normal (recursive) DNS requests (i.e., offloading them to popular DNS servers like Cloudflare or Google) from one central location does not work, or would at least yield imprecise or non-deterministic results (e.g., due to caching, Anycast routing, etc.). To make recursive DNS servers query for geographically close IP addresses, the eDNS Client Subnet (ECS) [7] mechanism allows propagating the client's IP address range (usually a `/24` subnet) to the authoritative DNS server. However, some DNS servers (e.g., Cloudflare [6]) do not enable ECS due to privacy concerns. Also, we found several operators' authoritative DNS servers do not support ECS and therefore solely use the request's IP address as baseline to build their responses. Addressing this requires a more complex approach, that uses different locations worldwide to issue DNS requests in an authoritative manner.

To cope with these needs we use a containerized infrastructure that leverages Virtual Private Networks (VPNs) for global distribution of DNS requests. Figure 4 describes the approach in detail: the VPN container connects to an existing VPN, providing Internet connectivity to the measurement container. The measurement container runs a local *unbound*[1] resolver that is configured to resolve DNS requests in an iterative manner (i.e., to get the IP addresses from the authoritative server). All DNS requests to the local server are issued with *massdns*[2].

The VPN container is built upon *gluetun*[3]. Thereby our setup works with any *OpenVPN* or *WireGuard* server and already implements native support for many consumer-grade VPN services (e.g., ProtonVPN, NordVPN, CyberGhost). To quickly achieve broad coverage, we purchase several VPN services and additionally use boto3[4] to implement automatic generation of ephemeral Amazon EC2 instances that are spawned in all available AWS Regions and act as WireGuard-based relays. Table 1 provides a summary of the utilized services along with the corresponding number of countries advertised by each service.

3.2 Discovering DNS Records

To discover existing ePDGs, we simply construct a list of all possible MCC and MNC combinations, resulting in 1.1 million domain names. We use the presented infrastructure to resolve these domain names (`A` and `AAAA` entries) from globally distributed vantage points. For all `CNAME` responses, we iteratively resolve the referenced domain until a final response is returned.

After retrieving the corresponding `A` and `AAAA` entries for a domain we can generate an exhaustive list of all ePDGs. For entries that only occur within specific client countries, we derive that the operator is possibly using DNS for load balancing, to reduce latency, or as a geoblocking measure.

[1] https://github.com/NLnetLabs/unbound
[2] https://github.com/blechschmidt/massdns
[3] https://github.com/qdm12/gluetun
[4] https://github.com/boto/boto3

Service	Countries[a]	IPv6 Support
Amazon EC2 (Cloud)	23	✓
Cloudflare WARP	120	✓
CyberGhost	91	×
hide.me	50	✓
HideMyAss	210	×
IVPN	36	✓
Mullvad	43	✓
NordVPN	60	×
Private Internet Access	84	×
ProtonVPN	68	×
Surfshark	100	×

[a] As advertised by the VPN/cloud service.

Table 1: Overview of VPN and cloud services that were used to distribute our measurements across the globe.

3.3 Probing Servers via IKE Initialization

To scan for IP-based geoblocking at the ePDG server, we can simply leverage the containerized infrastructure that was used to distribute our DNS requests in the previous section. Within the measurement container, we run a Python script that iterates over all IP addresses that were discovered in the previous step, trying to do an `IKE_SA_INIT` exchange (step 3, 4 in Figure 3). The script logs its current public IP address and whether the ePDG servers respond to the sent initialization packet. Any server that does not answer the first packet is probed repeatedly (i.e., five times) with an added back-off period. After querying a server's status from different source IP addresses we are able to determine whether the operator drops requests that are issued from unwanted countries.

The second phase (step 5 onwards in Figure 3) of the IKE protocol requires additional parameters like a subscriber's IMSI and cryptographically signed challenges that prove the identity of the customer. Since we want to get a big picture of global geoblocking practices and because it is not feasible to get access to SIM cards of a considerable amount of all worldwide operators we focus on detecting geoblocking relying on simple rules, such as dropping packets from unwanted IP addresses.

Therefore, the results of our methodology provide a lower bound on the number of operators that deploy geoblocking for VoWiFi. While our results in Section 4 show that we're able to detect a great share of blocking operators, we outline potential factors that restrict the detection capabilities of our method in Section 6.1.

4 RESULTS AND EVALUATION

We started with some preliminary exploratory measurements in May 2023 and subsequently improved our measurement methodology. The majority of our measurement results were obtained within a condensed measurement campaign during July and August 2023 (DNS discovery: Jul 13th to Aug 15th, IKE probing: Jul 13th to Aug 22th).

When citing a particular operator, we employ the notation $\texttt{CarrierName}_{[MCCMNC]}$.

As explained in Section 3.1, we issue DNS queries for all possible domain names from multiple clients distributed worldwide. From an abstract perspective, only a single DNS request is required to find the IP addresses that are currently associated with a domain name (from a particular location). In practice, however, this theoretical assumption does not hold. In fact, first of all, a client needs to find the responsible authoritative nameserver by querying the root and Top Level Domain (TLD) servers before the actual query is sent. Additionally, when asked for an `A` or `AAAA` record, the authoritative nameserver can refer to another domain by returning a `CNAME` entry. To cover this, we subsequently resolve `CNAME` chains until a final response (i.e., either `A`/`AAAA` or `NXDOMAIN`) is reached. Lastly, we enable rigorous caching at our local *unbound* instance, to prevent repeated queries and lower the amount of actual requests issued to external servers.

We experienced that most authoritative nameservers return a complete list of all IP addresses that are assigned to the requested domain name. In contrast, some nameservers only answer with a single IP and withhold the rest of the addresses that are also assigned to the requested domain name. While it is relatively easy to request all IP addresses for the first case, the latter complicates the matter and can only be tackled by querying the desired resource over and over again.

Lastly, some nameservers are configured to return IP addresses deterministically, depending on the source of the request.

In our approach, we split the requests into two phases (executed consecutively at every location), retrieving all available `A` and `AAAA` records respectively.

In addition to the original strategy where we query for all possible hostnames (*domain discovery*), we also ran some instances only querying domains already discovered in previous rounds. This was done to reduce the overall number of queries necessary to find all IP addresses (*IP discovery*) that exist for a single domain.

Overall, we ran 8,555 domain discovery and 47,902 IP discovery scans that were distributed across 219 countries.

Collected IP Addresses. Table 2 shows the amount of collected domains and (distinct) IP addresses. Overall, we collected 1,026 (`A`) and 66 (`AAAA`) domain-to-IP mappings. However, many IP addresses occur multiple times within one country, e.g., when an operator occupies multiple MNCs or when a Mobile Virtual Network Operator (MVNO) uses the ePDG of its parent provider, which reduces the set to 725 (`A`) and 40 (`AAAA`) unique ePDG IPs. About 7.3% of all domains support dual-stack (i.e., they have both an `A` and `AAAA` entry). For all found `AAAA` records, there is also a corresponding `A` entry, i.e., there is no operator that runs the ePDG via IPv6 only.

The vast majority of providers use three digits for the MNC in their ePDG domain, while $\texttt{Vodacom}_{[64004]}$ (Tanzania) is the only one that reserves an additional two-digit domain (i.e., `epdg.epc.mnc04.mcc640.pub.3gppnetwork.org`), serving the same IPs as its three digit counterpart.

Geographic Location of ePDGs. To determine the country of origin for an MNO (by its MCC), we rely on the most recent version of Android's MCC table [1], which is based on T-SP-E.212A [25] standardized by the International Telecommunication Union (ITU). To geolocate IP addresses we use the free MaxMind GeoLite2 database[5]. The MCC country of an ePDG and the location of an ePDG

[5] https://dev.maxmind.com/geoip/geolite2-free-geolocation-data

	IPv4			IPv6		
Region (via MCC) [a]	Countries [b]	Domains	IPs	Countries [b]	Domains	IPs
0 Test networks	0	0	0	0	0	0
2 Europe	41	148	311	8	9	16
3 North America & Caribbean	20	69	127	2	2	7
4 Asia, Middle East	21	133	164	3	17	11
5 Australia, Oceania	9	32	60	1	1	3
6 Africa	8	14	22	1	1	2
7 South- & Central America	9	26	40	1	1	1
9 Worldwide [c]	1	1	1	0	0	0
Total	109	423	725	16	31	40

[a] digits 1 and 8 are not specified. [b] according to the MCC. [c] Satellite, Air, Maritime, Antarctica.

Table 2: Encountered ePDGs via DNS discovery, grouped by MCC region. For *Test networks* we found no public DNS entries.

according to its IP addresses do not necessarily need to be identical. However, the majority of the operators use ePDGs that are hosted within their own network range and country. In most cases where the ePDG is not located within the MCC country, it is hosted within close proximity (i.e., in a neighbouring country). We noticed that this practice is especially popular with relatively small countries (e.g., `Tele2`$_{[24603,24702]}$ in Latvia and Lithuania via Sweden, `Orange`$_{[27099]}$ in Luxembourg via Belgium or `Claro`$_{[74810]}$ in Uruguay via Argentina) and in Caribbean island countries (e.g., `Flow`$_{[365840,364390]}$ in Anguilla and the Bahamas via Jamaica). An outlier with no geographical proximity of MCC and ePDG country is `Tata Communications`$_{[23427]}$ which is based in the United Kingdom but uses an ePDG located in the United States. `MTX Connect`$_{[90139]}$, the only operator we found within the "Worldwide" MCC range, is pointing to an ePDG IP hosted in Luxembourg. For IPv6 we do not see any divergences between MCC and ePDG country.

Non-Routable IP Addresses. While the majority of returned IP addresses lie within public address ranges, some results are not publicly routable. For example, German `Voiceworks`$_{[26220]}$ and Italian `Wind Tre`$_{[22288,22299]}$ return loopback IP addresses (`127.0.0.1` and `127.0.0.9`). Obviously, these addresses will not work in practice and were presumably just deployed as a placeholder or for internal testing purposes.

For IPv6, we see several providers referring to their IPv4 siblings. More specifically, `Three Mobile`$_{[23594]}$ (United Kingdom) and `Méditélécom`$_{[60400]}$ (Morocco) use the NAT64 IPv6 transition mechanism [38] via the `64:ff9b::/96` prefix and `Maxis`$_{[50212]}$ (Malaysia) refers to its IPv4 sibling via an IPv4-Compatible IPv6 address (deprecated in RFC4291 [9]).

4.1 Analyzing Differences in DNS Responses

We experience several cases where the returned DNS results deviate for repeated queries from different locations. For every IP address that is returned for a specific domain, we inspect the set of countries from which we were able to discover this IP address. Additionally, we also count the number of occurrences per country.

By inspecting these results, we can group the DNS servers according to their characteristic behavior:

(G1) *Returning Multiple IPs for Redundancy.* This group contains all domains where the DNS server directly returns all IP addresses that are associated with the queried hostname (without differentiating by the client's location). The vast majority of all domains (at least 78%[6] of all IPv4 domains) show this behavior. Responding with a greater set of IP addresses makes sense from an availability perspective: a client that wants to connect to a service can always switch to another IP address if something goes wrong when connecting to the first endpoint. Additionally, due to round-robin DNS [5], this will also enforce automatic load-balancing across all associated IP addresses.

While the median number of IP addresses that are returned is only two, some operators return a greater number of IPs. For instance, the maximum number that we discovered was `Telekom`$_{[26201]}$ (Germany) where all 12 IPs that exist for their ePDG domain are instantly returned by the responsible DNS server.

(G2) *Using DNS for targeted Load-balancing.* Some operators do not disclose all IP addresses in every DNS answer, but just return a subset (often just a single entry) of their responsible IP address pool. In this case, every request receives a partition of the address pool without any specific bias or determination (regarding the request's source location). Therefore, we assume that this is just used as a load-balancing measure, e.g., to balance clients among existing servers and that there is no intention to use this to block any resources. Additionally, the operator could use this for A/B testing or more fine-grained balancing based on the current network status, e.g., by purposefully forwarding clients to servers that currently have free resources.

`T-Mobile`$_{[310240,310260]}$ (United States) stands out as the primary example within this category, as they provide a total of 39 IP addresses for each of their domains. All ePDG servers were in deployment concurrently (i.e., discovered during various scans in the same time period) but their DNS server only answers with a single IP per request, as described above. Supposedly, the returned IP is selected randomly, as we do not see any location bias.

[6] According to our simple heuristic algorithm.

	IPv4		IPv6	
Service	Countries	Measurements	Countries	Measurements
Amazon EC2 (Cloud)	21	2,456	22	2,212
Cloudflare Warp	208	8,934	208	7,417
CyberGhost	90	4,025	0	0
hide.me	49	1,994	46	1,641
HideMyAss	207	2,969	0	0
IVPN	36	3,975	34	791
Mullvad	34	1,930	33	1,538
NordVPN	59	2,166	0	0
Private Internet Access	83	5,337	0	0
ProtonVPN	68	3,801	0	0
Surfshark	100	4,562	0	0
Total	219	42,149	208	13,599

Table 3: To achieve global coverage and to improve diversity of our client-side vantage points, we evenly distributed the IKE probing measurements to numerous VPN- and cloud services. Surprisingly, Cloudflare Warp provided far more countries than advertised in the service description (120 advertised vs. 208 actual countries). While they only list locations of their data centers the service presumably also uses smaller edge locations as exit points.

(G3) *Using DNS for Geolocational Grouping.* Again, only a single entry of a bigger address pool is returned. Additionally, the returned address is determined by the source IP address. Analyzing the IPs returned for specific countries, we see that the operator uses predetermined IP addresses to serve customers in different locations. For example, `Reliance Jio`$_{[405874]}$[7] (India) clearly separates their domestic and foreign users. All queries issued within India received IP addresses that never occurred within any other country. For their external customers, we could not see any further differentiation (i.e., customers in Europe usually get the same responses as customers in America or Africa). Additionally, we noticed that their DNS server does not support the eDNS Client Subnet (ECS) [7] mechanism. Therefore, the only way to discover their local IP addresses is to issue DNS queries from a location within India.

Regular use cases for this behaviour include its utilization for structural grouping of customers based on their location, or reducing latency by pointing to geolocationally close servers that are close to the customers (GeoDNS). Additionally, this behavior could be used to block the resource by returning an IP that does not accept any connections from the requester's location. To check whether this is the case, we need further analysis, i.e., we need to check whether the ePDG response differs between all returned IP addresses (cf. Section 4.2).

(G4) *Using DNS for Geoblocking.* Finally, operators could only answer local DNS queries and simply block or drop any external requests, to prohibit their customers from accessing the IMS via Wi-Fi when being abroad. In our results, we found that `Vodafone`$_{[26202]}$ (Germany) is only serving its ePDG IP addresses for DNS requests from appropriate client IPs. This was occasionally noticed by actual customers, as we also found anecdotal evidence [3, 53, 55, 45, 23, 52] within several posts on blogs and online forums. In contrast to `Jio`$_{[405874]}$ (see above), `Vodafone`$_{[26202]}$ actually respects ECS queries, making it possible to easily demonstrate the filtering[8]. While most of the queries that were able to discover `Vodafone`$_{[26202]}$'s ePDG were issued within Germany, the DNS server occasionally answered requests from external countries (e.g., several close countries like Austria, and Ireland, but also more distant countries like Kazakhstan and Japan). We tried to investigate what caused these false positives and checked the IP information of several results according to the MaxMind database. We found, that many misclassified IPs had Germany set as the `registered_country` (an additional meta-information in the database), although delivering an external country as the primary hosting country.

IPv6. Again, the vast majority (over 90 %) of all domains that return `AAAA` records can be found within the first group (G1). Additionally, we found members of (G2) and (G3), namely Israeli `Cellcom`$_{[42502]}$, replying with a single IP chosen without any visible location bias ((G2)) during a transition period switching their ePDG server, and `Canadian Bell`$_{[302610]}$, that serve their customers with dedicated IPs that are (vaguely) grouped by geographic region. In contrast to IPv4, we did not see any operator that used DNS for geoblocking purposes.

4.2 Probing VoWiFi Servers

After identifying the ePDG target IP addresses, we need to investigate whether the ePDG accepts connections from different geographic regions. To distribute our measurements across the globe, we again use our containerized architecture that leverages various VPN- and cloud services.

Data Sources and Covered Countries. Both MaxMind [39] and Android's MCC table [1] link entities (i.e., IP addresses, operators) to

[7] Jio also uses 21 other MNCs that were shortened for the sake of visibility.

[8] Example queries are shown in the Appendix A.1

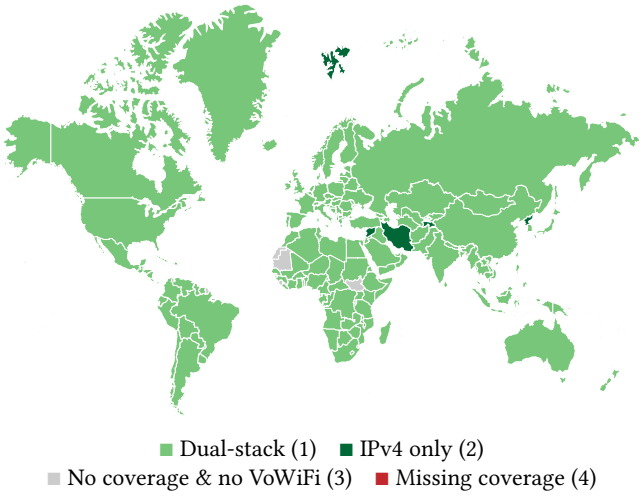

Figure 5: Leveraging VPN and cloud services, we reach de facto worldwide measurement coverage.

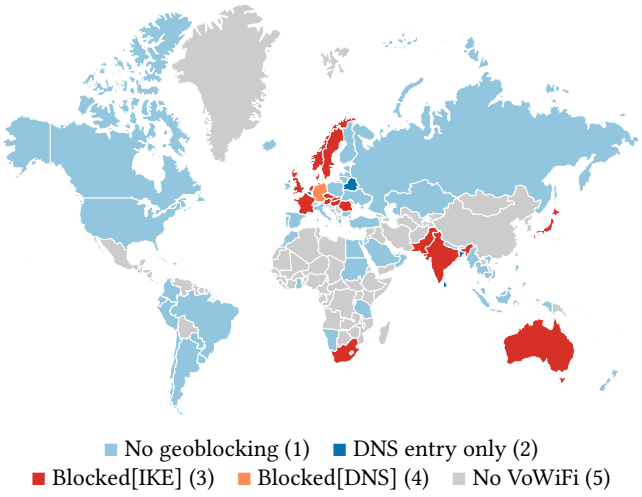

Figure 6: Summarized results or our DNS discovery and IKE probing measurements.

a geographical region (i.e., an ISO 3166-1 [24] country). ISO 3166-1 currently comprises 249 countries, and each can be linked to its corresponding continent.

In total, we issued more than 55,700 IKE scan rounds, that were executed from 219 different countries for IPv4 and 208 for IPv6 respectively. Table 3 gives an overview on how the measurements are distributed among countries and services.

The number of countries we used for scanning greatly exceeds the number of countries where operators actually support and use VoWiFi in practice. To maximize the scope of our study and gain a defacto worldwide view, we scanned from all 219 available countries. More specifically, this was done i) to maximize the discovered DNS entries in case of DNS-based blocking, and ii) to also detect blocking of countries that do not have VoWiFi yet, but are blocked by foreign operators (e.g., for political reasons).

4.2.1 Measurement Coverage and Domestic Results. Our measurements are limited by the countries that are available via our VPN- and cloud services. We cover 107/109 (IPv4) and 16/16 (IPv6) of our target countries (target territories defined by the DNS discovery). The two countries we are missing for IPv4 are both overseas departments of France, which are relatively small countries: French Polynesia (one operator) and La Réunion (two operators). Within French Polynesia, the single operator that was discovered via DNS ($\texttt{Ora}_{[54705]}$) responds to IKE requests from all over the globe and thereby is not geoblocked. The same holds true for one Reunionese carrier($\texttt{Zeop}_{[64704]}$), while the second one ($\texttt{Orange}_{[64700]}$) was not responsive from any country we scanned from and thereby is out of scope of our measurement coverage[9]. Figure 5 gives an overview of the global scope of our measurements: We've accomplished dual-stack connectivity in nearly all covered countries (1) and have some countries with IPv4 only coverage (2). Several countries that were not available via our scan infrastructure do not have VoWiFi yet (3), i.e., there are no DNS entries for any ePDG within that area. The two countries with missing coverage (i.e., French Polynesia and La Réunion) are very small and thereby not visible on the global map (4).

We scan every IP address that was discovered via DNS in the previous step (Table 2) from all available countries. However, not all endpoints are reachable and actually respond to requests. Presumably, some of the DNS entries are only set for testing purposes and are in fact not in active use. Table 4 reduces the original DNS set by removing all IPs that do not answer requests from any possible location (i.e., not even when connecting to the ePDG from a domestic IP address).

Dealing with Inaccuracies. Besides blocking according to a user's location, operators might also block the usage of popular VPN services or cloud infrastructure as a connection relay. More specifically, they might block some of our VPN services, or Autonomous Systems (ASes) that are commonly shared among popular VPN services. Furthermore, not all operators use MaxMind as their geolocation broker, introducing potential inconsistencies between our classification and the actual geolocation at the operator's sides. Additionally, we might occasionally experience connection hiccups within our scan infrastructure (e.g., when the used VPN unexpectedly closes the current connection). Lastly, some ePDGs seem to be very sensitive and do not accept repeated connections from the same IP address, simply ignore IKE handshakes that contain inappropriate cipher sets or go on/offline (i.e., experience downtimes) throughout our measurement study. To cope with these instabilities, we randomly switch VPN servers between subsequent measurements and aim for a big and diverse set of VPN services and realized measurements.

Also, we use the *responsiveness* (i.e., the percentage an ePDG was reported as responsive) of the domestic case as a *baseline*, to decide whether the server was blocked in a roaming case. As a matter of precaution, we consider some space for generous error bounds (e.g., when we or the operator misclassify the VPN IP and assume the wrong country) by only flagging an area as *geoblocked*, when it has

[9]For the remaining paper, we've treated it as a non-responsive ePDG, although technically it could be geoblocked and merely reachable via the home country (La Reunion).

Region (via MCC)	IPv4 Countries [b]		IPv4 Domains		IPs		IPv6 Countries [b]		IPv6 Domains		IPs	
2 Europe	37	90%	128	86%	271	87%	5	62%	5	56%	9	56%
3 North America & Caribbean	19	95%	61	88%	113	89%	1	50%	1	50%	5	71%
4 Asia, Middle East	19	90%	122	92%	141	86%	3	100%	16	94%	8	73%
5 Australia, Oceania	9	100%	28	88%	49	82%	0	0%	0	0%	0	0%
6 Africa	8	100%	12	86%	19	86%	0	0%	0	0%	0	0%
7 South- & Central America	9	100%	24	92%	35	88%	1	100%	1	100%	1	100%
9 Worldwide [c]	0	0%	0	0%	0	0%	0	-	0	-	0	-
Total	101	93%	375	89%	628	87%	10	62%	23	74%	23	57%

[b] according to the MCC. [c] Satellite, Air, Maritime, Antarctica.

Table 4: Overview of ePDGs responding to our IKE scan from at least one vantage point. The percentage columns compare the values to the results of the previous step (i.e., the values in Table 2).

less than 10% of the assumed *baseline responsiveness*. Thereby, the responsiveness remains comparable and we can correctly classify an ePDG, even when unexepcted events occur, e.g., when the ePDG server experiences a downtime during our measurement campaign. Also, this approach allows us to more accurately flag a country as *geoblocked*, even when we get responses in a minority of cases due to geolocation errors from the operator.

We do not differentiate between a successful `IKE_INIT` phase and a received error message. For example, when the ePDG responds with a `NO_PROPOSAL_CHOSEN` error to indicate that the offered ciphers are not accepted by the gateway we assume that there is no geoblocking for this client IP since a response packet was received (i.e., there is no IP-based blocking for this location).

4.2.2 Roaming Results. We found geoblocking at the IKE layer in various forms and granularities. For example, the target area of the blocking can be rather big (e.g., blocking all foreign connections) or small (e.g., only blocking a specific set of target countries). The confidence and robustness of our classification results (whether a server blocks by location or not) corresponds to the amount and diversity (e.g., IP- and AS diversity) of our measurements within that area. Therefore, we automatically classify global and continental geoblocking, but rely on manual inspection to identify country-level geoblocking, due to reduced diversity in small target countries. A domain is only flagged as geoblocked, when we observe geoblocking for all corresponding IP addresses.

Large-scale Geoblocking. According to our results, we experience global geoblocking for 12.5% (IPv4) and 65.2% (IPv6) of all tested domains. If we extend this to domains that are blocked from at least one continent (while being reachable from other areas) the percentage increases to 14.6% for IPv4 and remains unchanged for IPv6. Table 5 shows the detailed roaming results of our IKE probing. Overall, our measurements show that geoblocking is especially common within Europe and Asia but there are also continents without any large-scale blocking at all (e.g., North and South America).

Interestingly, we found numerous operators in European countries (Austria, Czech Republic, Denmark, France, Hungary, Luxembourg, the Netherlands, Norway, Romania, Sweden, and the United Kingdom) with large-scale blocking measures. Moreover, many operators within the EU also block connections from their neighboring EU countries. In contrast, intra-EU roaming via regular radio access is possible without additional costs in these countries, due to the Roam Like At Home (RLAH) doctrine [15]. As an exception, we've found a single Slovakian operator with worldwide geoblocking that specifically exempts EU/EAA countries from the blocking.

While most operators employing large-scale blocking within Asia are based in India (15/37), we've also discovered geoblocking at operators from Hong Kong, Israel, Japan, Pakistan, and Singapore. Lastly, the remaining operators were found in Australia and South Africa.

The overall results are visualized in Figure 6. For the majority of countries there was no large-scale geoblocking discovered (1). Some territories had DNS entries for an ePDG, but did not respond to any of our IKE scans (2). Moreover, we found geoblocking measures via IKE (3) and DNS (4) scans. Finally, some countries do not have DNS entries for ePDGs at all and therefore do not support VoWiFi yet (5).

Country-targeted Geoblocking. In some cases we see more fine-grained blocking or exemptions from large-scale blocks. For example, one Australian operator that generally blocks foreign IPs specifically allows connections from other Oceanian (e.g., New Zealand) and Asian (e.g., the Philippines, Malaysia , China) countries.

However, we also see country-targeted blocking within continents and countries that otherwise do not engage geoblocking. For example, an Israeli operator specifically blocks several African (e.g., Lybia, Algeria) and Asian (e.g., Iran, Iraq) countries, despite their geographical proximity. Moreover, several operators, e.g., in the United States or Ecuador, block connections coming from Russia or Ukraine, potentially for political or security reasons.

IPv6. For IPv6, we've detected geoblocking for 65.2% of all tested domains. However, these numbers are only caused by operators from two distinct countries: India and Japan. Compared to IPv4, the overall percentage is higher because India is among the leading nations when it comes to IPv6 adoption and simultaneously a country where geoblocking at VoWiFi is fairly popular.

Interestingly, we've found one Hungarian operator that supports both IPv4 and IPv6 and blocks external connections only on the IPv4

	IPv4				IPv6			
Region (via MCC)	Countries [b]		Domains		Countries [b]		Domains	
2 Europe	12	32%	19	15%	0	0%	0	0%
3 North America & Caribbean	0	0%	0	0%	0	0%	0	0%
4 Asia, Middle East	5	26%	32	26%	2	67%	15	94%
5 Australia, Oceania	2	22%	3	11%	0	-	0	-
6 Africa	1	12%	1	8%	0	-	0	-
7 South- & Central America	0	0%	0	0%	0	0%	0	0%
Total	20	20%	55	15%	2	20%	15	65%

[b] according to the MCC.

Table 5: Overview of ePDGs where we encountered large-scale (global or continental) geoblocking. The percentage columns relate the values to the parent population of responsive ePDGs in the corresponding area (cf. Table 4).

stack. Thereby, customers could circumvent the blocking by simply connecting via IPv6 (a similar phenomenon has been discovered by previous research [8]).

Overall, the available geolocation data seems to be more accurate for IPv6 because — compared to IPv4 — we see less blurring (i.e., for each distinct country the responsiveness is either 0 or 100%).

Revisited: `Reliance Jio`$_{[405874]}$ India. As stated in Section 4.1, we found that this operator clearly separates the IP addresses that are returned via DNS for local and external customers. Analyzing the two subsets (i.e., local, and external) at the ePDG layer, we see that this behavior also reoccurs when connecting to the gateway: The set of local IP addresses does not accept any connections from abroad. Interestingly, this behavior is also mutual, i.e., the external ePDG does not accept any local connections from India either. Since a customer can thereby establish a connection to an ePDG from any location we did not account this behaviour as geoblocking. However, the existing separation mechanism could possibly be used to differentiate or block at a later stage.

Revisited: `Vodafone`$_{[26202]}$ Germany. In Section 4.1 we showed that this operator uses DNS-based blocking to prevent customers from connecting to the ePDG from external locations. Taking a closer look at the probing results of the corresponding endpoints, we see that the blocking is solely done by the DNS server and does not occur at the IKE layer (i.e., it accepts connections from all tested countries). Thereby, sneaky customers may simply evade the blocking by manually adding the correct DNS entries to their system, or by using specific DNS servers that always return the corresponding IPs (e.g., a local resolver in Germany that does not forward the client's subnet).

5 RELATED WORK

This section presents an overview of existing research and studies that contribute to the understanding and context of the subject matter at hand.

Geoblocking and Internet Censorship. In 2018, the European Union (EU) banned unjustified geoblocking within the European single market [14]. Nevertheless, the regulation includes a number of exceptions (e.g., for copyrighted audiovisual content like Netflix) and significant portions of the world remain without regulatory measures.

McDonald et al. [40] proved the prevalence of geoblocking practices in the Internet by finding geoblocking at large CDNs for nearly all of the 177 examined countries.

Additionally, Kumar et al. [31] analyzed the mobile app ecosystem from vantage points in 26 countries. Aside from geoblocking being a common practice in the mobile app field they also found geodifferences occurring between differing countries (i.e., developers shipping different versions of an app to specific regions).

Lastly, geoblocking is often introduced as a governmental censorship measure. Ramesh et al. [47] showed, that — ever since Russia's invasion of Ukraine in February 2022 — there are geofences between Russia and the rest of the world. Thereby, Russian users are not able to consume Western news or social media and Russian government domains remain inaccessible from regions like the EU and US.

VoLTE and VoWiFi Security. Prior research discovered numerous security- and privacy-related vulnerabilities in VoLTE and VoWiFi. For example, Kim [29] showed that early VoLTE deployments were prone to data traffic free-riding attacks since the packet-switched voice channel provided an unmetered breakout to the public Internet. Furthermore, both VoLTE and VoWiFi were found to occasionally leak precise subscriber info (e.g., Cell IDs) via the underlying SIP traffic [30]. Additionally, VoWiFi is vulnerable to IMSI catching attacks [42, 43].

More recently, Lu et al. [33], Xie et al. [56], and Lee et al. [32] presented practical Denial of Service (DoS) attacks for VoLTE and/or VoWiFi. Moreover, Hu et al. showed that VoLTE's emergency services are also vulnerable to DoS and free-riding attacks [22].

In 2023, the Google Project Zero team discovered four severe Exynos vulnerabilities that allowed an attacker to execute arbitrary commands on the baseband processor of the most recent Pixel and many Samsung phones by injecting malicious SIP messages [41] into the VoLTE/VoWiFi VoIP traffic.

Lastly, Gegenhuber et al. [17, 18] uncovered insecure VoWiFi configurations and shortcomings at the corresponding key exchange.

Active Roaming Experiments. Large-scale studies that involve many operators and countries are usually limited by the complex

ecosystem and the required coordination effort. However, there are several approaches [37, 51] where specifically built measurement devices were placed into target locations to measure the implications (e.g., QoE) of roaming. Additionally, Sahin and Francillon [50] observed hijacking of traditional voice calls that were redirected to over-the-top (OTT) services (e.g., WhatsApp, Viber) to bypass/monetize termination fees.

Recently, Gegenhuber et al. [20, 19] introduced the MobileAtlas measurement platform that tries to overcome the mentioned scalability issues by tunneling the communication between SIM card and modem over the Internet. Their platform provides flexible roaming measurements and capabilities for a rich set of cellular features, including Internet and voice-based measurements.

Evaluating and Fingerprinting VPNs. The commercial VPN ecosystem is a multi-billion dollar industry [21] and thereby has been an interesting research target. For example, previous work [28, 46] analyzed and compared existing VPN services and found that many solutions leak user traffic or advertise wrong server locations.

In contrast, Maghsoudlou et al. [36] did not purchase any VPN subscriptions but executed Internet-wide scans to discover and fingerprint VPNs, finding over 7 million IPsec servers.

6 DISCUSSION

Our findings indicate that a notable proportion of operators are implementing IP-based restrictions to prevent customers from using VoWiFi in specific locations. While we also discovered DNS-based approaches, most operators implement it directly at the IKE layer. Furthermore, the found geoblocking measures exhibit a degree of regionality, meaning they are more prevalent in certain areas (e.g., Eurasia) compared to others (e.g., North- and South America).

To the best of our knowledge, this is the first study providing a comprehensive overview of the existing VoWiFi infrastructure on a global scale. Understanding the current deployment of any widely used telecommunication system is vital from a security standpoint. Our findings go beyond this by revealing that the observed blocking has significant repercussions for emergency calling.

Implications to Emergency Calling. Recent reports show, that there currently is no adequate support for VoLTE roaming in substantial parts of the world [48, 54]. Since many operators are actively shutting down their 2G/3G legacy networks, this scenario has the potential to result in significant repercussions for the functionality of emergency calling [49, 10, 11].

Although we believe that affected operators will address and fix these issues in the long term, VoWiFi could help to mitigate these shortcomings in the present day. Tourists or travellers frequently have access to WiFi, such as in their accommodations or through free WiFi hotspots in public spaces. According to the specification [13], VoWiFi should be used by the UE for emergency calling when traditional radio services (VoLTE roaming, CSFB) are unavailable. The phone ultimately tries to reach both the home and the visited ePDG. However, there are circumstances where the visited ePDG might not be available, e.g., when there is no VoWiFi support in the visited country or when the customer leaves the phone in flight mode to not cause any unintentional roaming fees and thereby the current location is not known to the phone).

While operators can override the default ePDG for emergency services by setting corresponding DNS records (`sos.epdg.epc.mnc{y}.mcc{x}.pub.3gppnetwork.org`) [12], only four operators had appropriate DNS entries. In all four cases, the emergency ePDG referenced the original ePDG's IP address, which is also the default behaviour when no `sos` entry is found. Controversially, two of the operators specifically using `sos`-domains nevertheless block IKE-inquiries coming from foreign IP addresses.

If an operator deploys DNS- or IKE-based geoblocking, these measures will also impact emergency services, actively denying persons in need from making an emergency call. Similarly, the emergency service via Wi-Fi is also unavailable in the home country, when customers use a VPN connection or an international SIM card (e.g., utilizing a travel router) that provides the Internet uplink via a foreign country.

Economic and Net Neutrality Perspective. In contrast to regular roaming over the radio interface – where the foreign roaming partner charges the home operator for the terminated calls and services – there is no additional economic overhead for VoWiFi calls that are initiated from overseas customers. In fact, calls terminated via VoWiFi are notably cost-effective for operators, as they eventually reduce expenses associated with the required radio transmission infrastructure (i.e., base stations) and spectrum licensing fees. Instead, the traffic is routed via external infrastructure (i.e., a WiFi AP) that was provided and paid for by the customer.

Moreover, adhering to the principle of net neutrality and the Open Internet, it is not allowed to discriminate (i.e., block) a customer's data packets by their source or destination IP address, particularly when motivated solely by economic interests (cf. differential pricing and zero-rating). Assuming the discovered blocking practices were employed mainly for economic reasons, they could potentially be seen as a net neutrality violation.

Ways to Evade Geoblocking. Common mobile operating systems (i.e., Android and iOS) support changing the used DNS server for WiFi interfaces out of the box, which should allow easy bypassing of DNS-based blocking.

Additionally, both Android and iOS have built-in support for applying a system-wide VPN connection. However, even with an active VPN, VoWiFi uses a direct route over the WiFi interface. While this hinders standalone solutions on non-rooted phones, a viable alternative could be to use so-called travel routers. These devices act as an intermediary between WiFi AP and smartphone and typically offer the ability to redirect all traffic through a VPN connection, and thus via a customer's home country.

Inaccurate Geolocation and Blocked VPN Services. Each VPN service uses one or more IP addresses for each country within its coverage. In the course of this study, we occasionally experienced outliers where certain IP addresses, address ranges, or Autonomous Systems (ASes) from specific VPNs experienced blocking even though belonging to the same country as the probed operator. We suppose that those connections were either blocked because their geolocation was wrongfully classified from the operator, or because the operator specifically blocked connections from IPs that are associated with certain VPN services.

6.1 Limitations

Although we are able to detect a considerable amount of blocking operators, several factors limit our approach. Due to the fact that these constraints limit the geoblocking variants that we're able to detect, our results can be seen as a lower bound. Thereby, the actual occurrence of geoblocking in practice is most likely even higher.

More Advanced Blocking. Our current approach is designed to detect simple IP-based blocking rules. However, some operators use more sophisticated (e.g., IMEI-based) ways to decide whether a customer should be able to use VoWiFi under current circumstances. For example, an operator could use the last known roaming status via the radio network to decide whether a customer is currently in their home country or abroad. Additionally, VoWiFi roaming can only be offered to a limited set of customers (i.e., *premium users*). For example, we found an Austrian operator that requires an additional subscription package to get VoWiFi enabled during international roaming [35]. In this case, the operator initially accepts IKE packets from all locations and decides whether to grant (or drop) access to VoWiFi at a later stage, when the subscriber's identity is known. We focus on straightforward IP-based blocking because measuring these more advanced blocking techniques on a global scale would necessitate the acquisition of SIM cards for an unfeasible number of operators. Moreover, it is crucial to highlight that relying solely on IP address-based blocking for VoWiFi access also results in the restriction of access to emergency calling services. Implementing blocking techniques that compromise the unconditional availability of emergency services that people depend on in life-threatening situations is highly ill-advised.

Implementation Incompatibility and Blocked VPN Services. Our IKE probing is based on a cellular-specific open-source implementation of the IKEv2 protocol[10]. Possibly, some ePDGs are not compatible with this implementation or do not answer requests that offer inappropriate cipher suites. Similarly, operators could block access from well-known VPN services or ASes and IP ranges that are used by them. As a countermeasure, we use multiple services to increase the diversity within our clients. Since we got responses from a high share of ePDGs that were discovered via DNS, these two factors do not considerably influence our results.

Non-Native and Non-3GPP-Compliant VoWiFi. Whereas our approach focuses on the native 3GPP version of VoWiFi there are also other ways to support voice calling functionalities over Wi-Fi networks. For example, an operator might require their customers to download and install a dedicated VoWiFi app that gives direct access to the IMS network in a non-compliant way [34]. Additionally, some operators might use non-default ways to communicate their ePDGs, e.g., only resolve the hostname via an internal DNS server that is shipped to their customers via DHCP. Lastly, we do not cover VoIP calling via OTT services (e.g., WhatsApp, Viber, Skype).

6.2 Ethical Considerations

Ethical considerations are vital to the field of measurements, especially with active measurements conducted in live systems. From an operator's perspective, we only interact with two endpoints i.e., retrieving IP addresses via the authoritative DNS server and performing the initial IKE handshake with the ePDG. In both cases, we tried to mimic normal user behavior by sending well-formed requests, i.e., we did not deviate from the protocol specification or do any fuzzing. From a bandwidth perspective, our measurements should not overstress any operator, since for each measurement target we were only sending several requests per hour. Finally, our measurements did not involve any actual user data (e.g., IMSIs or IMEIs), since we were only performing the initial handshake where the cryptographic parameters for the subsequent connection are exchanged.

6.3 Dissemination and Responsible Disclosure

Beyond disseminating our findings to the scientific community, we want to enable an informed debate by raising awareness within the industry and highlight potential issues regarding IP-based geoblocking among regulators and emergency associations. Therefore, we reported our results to the GSM Association (GSMA), the Body of European Regulators for Electronic Communications (BEREC), and the European Emergency Number Association (EENA). GSMA and EENA invited us to expand upon and discuss our findings within dedicated meetings and BEREC responded to our inquiry via Email.

More specifically, GSMA discussed the topic within their panel of experts and invited us to *"present this case to the GSMA's Fraud and Security Architecture Group, to make the issue know to their members"*. According to BEREC *"there are no legal obligations for Wi-Fi calls in roaming stemming from the Roaming Regulation, and they do not see this as a breach of the Open Internet Regulation"*. Lastly, *"EENA will study the topic and discuss with its community to understand the extent of any potential impact the practice of geoblocking could have on access to emergency services through emergency communications"*.

7 CONCLUSION

Many operators worldwide have implemented support for VoLTE and VoWiFi and rely on the IP Multimedia Subsystem (IMS) as a centerpiece for their communication services. Additionally, the IMS and VoWiFi seamlessly integrate with the upcoming 5G network generation and thereby will also play a relevant role in the future.

Just like any crucial system that impacts our daily lives, it's important to be aware of its current state and to comprehend its internal workings. We therefore give a comprehensive overview of the global deployment of VoWiFi and investigate existing geoblocking measures, discovering IP-based blocking mechanisms both at the DNS and IKE layer. We emphasize that, unlike geoblocking measures commonly employed in web or streaming applications, telecommunications is a more sensitive domain, where such measures could potentially have adverse effects on the functionality of emergency calls. Thus, we hope that the insights of our study will raise the awareness among customers and security researchers, while also contributing to the decision-making processes of policy makers and operators in the future.

To encourage other researchers to further profit from our work and engineering effort, we've publicly released the source code of our measurement infrastructure [11].

[10] https://github.com/fasferraz/SWu-IKEv2

[11] https://github.com/sbaresearch/scanywhere

ACKNOWLEDGMENTS

We want to thank Quentin McGaw and all other Gluetun contributors – their previous work made it considerably easier to build *scanywhere* and thus to globally distribute our measurements.

This project was funded through the NGI0 Entrust Fund, a fund established by NLnet with financial support from the European Commission's Next Generation Internet, under the aegis of DG Communications Networks, Content and Technology under grant agreement No 101069594.

SBA Research (SBA-K1) is a COMET Centre within the COMET – Competence Centers for Excellent Technologies Programme and funded by BMK, BMAW, and the federal state of Vienna. COMET is managed by FFG.

A APPENDIX

A.1 DNS-based Blocking at Vodafone

Resolving standardized ePDG domain to `CNAME` reference:

```
$ dig epdg.epc.mnc002.mcc262.pub.3gppnetwork.org
=> returns CNAME epdg.epc.drz1.vodafone-ip.de
```

Actual resolution (Google vs. Vodafone IP range):

```
# requesting via Google IP (United States)
$ dig +trace epdg.epc.drz1.vodafone-ip.de +subnet=104.154.0.0/24
# requesting via Vodafone IP (Germany)
$ dig +trace epdg.epc.drz1.vodafone-ip.de +subnet=109.192.0.0/24
```

A.2 Artifact Appendix

The research artifacts accompanying this paper are available via 10.5281/zenodo.11089362.

REFERENCES

[1] Google (AOSP). 2006. Android MCC Table. WebPage. Accessed: 2023-07-23. (2006). https://android.googlesource.com/platform/frameworks/opt/telephony/+/refs/heads/main/src/java/com/android/internal/telephony/MccTable.java.

[2] 2023. Airtel India: WiFi calling FAQs. WebPage. Accessed: 2023-08-21. (2023). https://www.airtel.in/wifi-calling/faqs.

[3] 2017. Android WiFi Calling VoWifi not working, wont resolve domain. WebPage. Accessed: 2023-07-27. (2017). https://groups.google.com/g/public-dns-discuss/c/AExOcbpl09w.

[4] Jari Arkko and Henry Haverinen. 2006. Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA). RFC 4187. (Jan. 2006). DOI: 10.17487/RFC4187.

[5] Thomas P. Brisco. 1995. DNS Support for Load Balancing. RFC 1794. (Apr. 1995). DOI: 10.17487/RFC1794.

[6] Cloudflare. 2021. Cloudflare FAQ: ECS Policy. WebPage. Accessed: 2023-07-04. (2021). https://developers.cloudflare.com/1.1.1.1/faq/#does-1.1.1.1-send-edns-client-subnet-header.

[7] Carlo Contavalli, Wilmer van der Gaast, David C Lawrence, and Warren "Ace" Kumari. 2016. Client Subnet in DNS Queries. RFC 7871. (May 2016). DOI: 10.17487/RFC7871.

[8] Jakub Czyz, Matthew Luckie, Mark Allman, Michael Bailey, et al. 2016. Don't forget to lock the back door! a characterization of ipv6 network security policy. In *Network and Distributed Systems Security (NDSS)*.

[9] Dr. Steve E. Deering and Bob Hinden. 2006. IP Version 6 Addressing Architecture. RFC 4291. (Feb. 2006). DOI: 10.17487/RFC4291.

[10] 2022. EENA 2022: Access to emergency services is being impacted by the lack of VoLTE interoperability. WebPage. Accessed: 2023-08-21. (2022). https://eena.org/knowledge-hub/press-releases/many-europeans-cannot-call-911-when-traveling-to-the-us/.

[11] 2022. Ensuring continuity of access to emergency services in the transition to IMS/VoLTE services. WebPage. Accessed: 2023-08-21. (2022). https://eena.org/blog/webinars/volte-standardisation-problem/.

[12] ETSI. 2023. Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Numbering, addressing and identification. ETSI, (2023). https://www.etsi.org/deliver/etsi_ts/123000_123099/123003/17.10.00_60/ts_123003v171000p.pdf.

[13] ETSI. 2022. Universal Mobile Telecommunications System (UMTS); LTE; Architecture enhancements for non-3GPP accesses. ETSI, (2022). https://www.etsi.org/deliver/etsi_ts/123400_123499/123402/17.00.00_60/ts_123402v170000p.pdf.

[14] European Parliament, Council of the European Union. 2018. Regulation (EU) 2018/302. (2018). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018R0302.

[15] European Parliament, Council of the European Union. 2022. Regulation (EU) 2022/612. (2022). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:4593182.

[16] Sheila Frankel and Suresh Krishnan. 2011. IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap. RFC 6071. (Feb. 2011). DOI: 10.17487/RFC6071.

[17] Gabriel K. Gegenhuber, Philipp É. Frenzel, and Edgar Weippl. 2024. POSTER: Never Gonna Give You Up: Exploring Deprecated NULL Ciphers in Commercial VoWiFi Deployments. In *17th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*.

[18] Gabriel K. Gegenhuber, Florian Holzbauer, Philipp É. Frenzel, Edgar Weippl, and Adrian Dabrowski. 2024. Diffie-Hellman Picture Show: Key Exchange Stories from Commercial VoWiFi Deployments.

[19] Gabriel K. Gegenhuber, Wilfried Mayer, and Edgar Weippl. 2022. Zero-Rating, One Big Mess: Analyzing Differential Pricing Practices of European MNOs. In *IEEE Global Communications Conference (GLOBECOM)*.

[20] Gabriel Karl Gegenhuber, Wilfried Mayer, Edgar Weippl, and Adrian Dabrowski. 2023. MobileAtlas: Geographically Decoupled Measurements in Cellular Networks for Security and Privacy Research. In *Usenix Security Symposium 2023*.

[21] 2020. Google Trends Reveals Surge in Demand for VPN. WebPage. Accessed: 2023-08-21. (2020). https://www.namecheap.com/blog/vpn-surge-in-demand/.

[22] Yiwen Hu et al. 2022. Uncovering Insecure Designs of Cellular Emergency Services (911). In *Proceedings of the 28th Annual International Conference on Mobile Computing And Networking*, 703–715.

[23] 2018. Ich hab Probleme wifi calling zu aktivieren. WebPage. Accessed: 2023-07-27. (2018). https://forum.vodafone.de/t5/Archiv-Apple/Ich-hab-Probleme-wifi-calling-zu-aktivieren/td-p/1718155.

[24] 2000. ISO 3166-1:1997: Codes for the representation of names of countries and their subdivisions — Part 1: Country codes. Standard. International Organization for Standardization, (Nov. 2000). https://www.iso.org/iso-3166-country-codes.html.

[25] ITU. 2017. T-SP-E.212A: List of Mobile Country or Geographical Area Codes. WebPage. Accessed: 2023-07-23. (2017). http://handle.itu.int/11.1002/pub/80f1788f-en.

[26] Charlie Kaufman. 2005. Internet Key Exchange (IKEv2) Protocol. RFC 4306. (Dec. 2005). DOI: 10.17487/RFC4306.

[27] Charlie Kaufman, Paul E. Hoffman, Yoav Nir, Pasi Eronen, and Tero Kivinen. 2014. Internet Key Exchange Protocol Version 2 (IKEv2). RFC 7296. (Oct. 2014). DOI: 10.17487/RFC7296.

[28] Mohammad Taha Khan, Joe DeBlasio, Geoffrey M Voelker, Alex C Snoeren, Chris Kanich, and Narseo Vallina-Rodriguez. 2018. An Empirical Analysis of the Commercial VPN Ecosystem. In *Proceedings of the Internet Measurement Conference 2018*, 443–456.

[29] Hongil Kim, Dongkwan Kim, Minhee Kwon, Hyungseok Han, Yeongjin Jang, Dongsu Han, Taesoo Kim, and Yongdae Kim. 2015. Breaking and Fixing VoLTE: Exploiting Hidden Data Channels and Mis-implementations. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 328–339.

[30] Sekwon Kim, Bonmin Koo, and Hwankuk Kim. 2015. Tracking Location Information of VoLTE Phones. In *2015 International Conference on Computational Science and Computational Intelligence (CSCI)*. IEEE, 703–708.

[31] Renuka Kumar, Apurva Virkud, Ram Sundara Raman, Atul Prakash, and Roya Ensafi. 2022. A Large-scale Investigation into Geodifferences in Mobile Apps. In *31st USENIX Security Symposium (USENIX Security 22)*, 1203–1220.

[32] Hyunwoo Lee, Imtiaz Karim, Ninghui Li, and Elisa Bertino. 2022. Vwanalyzer: a systematic security analysis framework for the voice over wifi protocol. In *Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security*, 182–195.

[33] Yu-Han Lu, Chi-Yu Li, Yao-Yu Li, Sandy Hsin-Yu Hsiao, Tian Xie, Guan-Hua Tu, and Wei-Xun Chen. 2020. Ghost calls from operational 4G call systems: IMS vulnerability, call DoS attack, and countermeasure. In *Proceedings of the 26th Annual International Conference on Mobile Computing and Networking*, 1–14.

[34] 2017. Magenta Austria: VoWiFi Roaming. WebPage. Accessed: 2023-08-21. (2017). https://www.gsma.com/futurenetworks/digest/vowifi-implementation-insight-china-unicom/.

[35] 2023. Magenta Austria: VoWiFi Roaming. WebPage. Accessed: 2023-08-21. (2023). https://www.magenta.at/handytarife/zusatzpakete/vowifi-roaming.

[36] Aniss Maghsoudlou, Lukas Vermeulen, Ingmar Poese, and Oliver Gasser. 2023. Characterizing the VPN Ecosystem in the Wild. In *International Conference on Passive and Active Network Measurement*. Springer, 18–45.

[37] Anna Maria Mandalari et al. 2018. Experience: Implications of Roaming in Europe. In *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking*, 179–189.

[38] Philip Matthews, Iljitsch van Beijnum, and Marcelo Bagnulo. 2011. Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers. RFC 6146. (Apr. 2011). DOI: 10.17487/RFC6146.

[39] MaxMind, Inc. 2023. GeoLite2 Free Geolocation Data. WebPage. Accessed: 2023-08-01. (2023). https://dev.maxmind.com/geoip/geolite2-free-geolocation-data.

[40] Allison McDonald, Matthew Bernhard, Luke Valenta, Benjamin VanderSloot, Will Scott, Nick Sullivan, J. Alex Halderman, and Roya Ensafi. 2018. 403 Forbidden: A Global View of CDN Geoblocking. In *Proceedings of the Internet Measurement Conference 2018*, 218–230.

[41] 2023. Multiple Internet to Baseband Remote Code Execution Vulnerabilities in Exynos Modems. WebPage. Accessed: 2023-08-21. (2023). https://googleprojectzero.blogspot.com/2023/03/multiple-internet-to-baseband-remote-rce.html.

[42] Piers O'Hanlon and Ravishankar Borgaonkar. 2016. WiFi-Based IMSI Catcher. Blackhat Europe 2016. (2016).

[43] Piers O'Hanlon, Ravishankar Borgaonkar, and Lucca Hirschi. 2017. Mobile Subscriber WiFi Privacy. In *2017 IEEE Security and Privacy Workshops (SPW)*. IEEE, 169–178.

[44] Kenechi Okeleke, Harry Fernando Aquije Ballon, and James Joiner. 2023. GSMA: The Mobile Economy 2023. https://www.gsma.com/mobileeconomy/wp-content/uploads/2023/03/270223-The-Mobile-Economy-2023.pdf.

[45] 2017. Probleme und Workarround für WiFi Calling mit Vodafone. WebPage. Accessed: 2023-07-27. (2017). https://ntankl3.de/probleme-und-workaround-fuer-wifi-calling-mit-vodafone/.

[46] Reethika Ramesh, Leonid Evdokimov, Diwen Xue, and Roya Ensafi. 2022. VPNalyzer: Systematic Investigation of the VPN Ecosystem. In *Network and Distributed System Security*, 24–28.

[47] Reethika Ramesh et al. 2023. Network Responses to Russia's Invasion of Ukraine in 2022: A Cautionary Tale for Internet Freedom. In *32nd USENIX Security Symposium (USENIX Security 23)*, 2581–2598.

[48] 2022. Roaming goes down the drain as AT&T disconnects European travellers. WebPage. Accessed: 2023-08-21. (2022). https://www.capacitymedia.com/article/2a5x2tyoz25np4z7yz1fk/news/roaming-goes-down-the-drain-as-at-t-disconnects-european-travellers.

[49] Hendrik Rood and Rudolf Berg. 2022. RE-VoLTE: Should we stop the shutdown of 2G/3G to save lives?? A lack of VoLTE standardisation breaks voice calling globally. (July 2022). DOI: 10.13140/RG.2.2.12321.28007.

[50] Merve Sahin and Aurélien Francillon. 2016. Over-The-Top Bypass: Study of a Recent Telephony Fraud. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 1106–1117.

[51] Matteo Varvello and Yasir Zaki. 2023. A Worldwide Look Into Mobile Access Networks Through the Eyes of AmiGos. In *2023 7th Network Traffic Measurement and Analysis Conference (TMA)*. IEEE, 1–10.

[52] 2018. Vodafone Germany VoWiFi in Roaming. WebPage. Accessed: 2023-07-27. (2018). https://volteromania.blogspot.com/p/blog-page_25.html.

[53] 2016. Vodafone WiFi Calling nur ohne Google DNS möglich. WebPage. Accessed: 2023-07-27. (2016). https://www.mielke.de/blog/Vodafone-WiFi-Calling-Google-DNS--471/.

[54] 2022. VoLTEgate: Tomia says 50m visitors to US this year will be cut off from voice roaming. WebPage. Accessed: 2023-08-21. (2022). https://www.capacitymedia.com/article/2a9s377bx0f611rx9lfr5/news/voltegate-tomia-says-50m-visitors-to-us-this-year-will-be-cut-off-from-voice-roaming.

[55] 2019. WiFi-Calling, Evolved Packet Data Gateway und Google DNS. WebPage. Accessed: 2023-07-27. (2019). https://blog.rolandmoriz.de/2019/01/13/wifi-calling-evolved-packet-data-gateway-und-google-dns/.

[56] Tian Xie, Guan-Hua Tu, Bangjie Yin, Chi-Yu Li, Chunyi Peng, Mi Zhang, Hui Liu, and Xiaoming Liu. 2020. The Untold Secrets of WiFi-Calling Services: Vulnerabilities, Attacks, and Countermeasures. *IEEE Transactions on Mobile Computing*, 20, 11, 3131–3147.