If you cite this paper, please use the IMC reference: Patrick Sattler, Juliane Aulbach, Johannes Zirngibl, and Georg Carle. 2022. Towards a Tectonic Traffic Shift? Investigating Apple's New Relay Network. *In ACM Internet Measurement Conference (IMC '22)*, October 25–27, 2022, Nice, France. ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3517745.3561426

Towards a Tectonic Traffic Shift? Investigating Apple's New Relay Network

Patrick Sattler
Technical University of Munich
Germany
sattler@net.in.tum.de

Juliane Aulbach
Technical University of Munich
Germany
aulbach@net.in.tum.de

Johannes Zirngibl
Technical University of Munich
Germany
zirngibl@net.in.tum.de

Georg Carle
Technical University of Munich
Germany
carle@net.in.tum.de

ABSTRACT

Apple recently published its first Beta of the iCloud Private Relay, a privacy protection service with promises resembling the ones of VPNs. The architecture consists of two layers (ingress and egress), operated by disjoint providers. The service is directly integrated into Apple's operating systems, providing a low entry-level barrier for a large user base. It seems to be set up for significant adoption with its relatively moderate entry-level price.

This paper analyzes the iCloud Private Relay from a network perspective, its effect on the Internet, and future measurement-based research. We perform EDNS0 Client Subnet DNS queries to collect ingress relay addresses and find 1586 IPv4 addresses. Supplementary RIPE Atlas DNS measurements reveal 1575 IPv6 addresses. Knowing these addresses helps to detect clients communicating through the relay network passively. According to our scans, ingress addresses grew by 20 % from January through April. Moreover, according to our RIPE Atlas DNS measurements, 5.3 % of all probes use a resolver that blocks access to iCloud Private Relay.

The analysis of our scans through the relay network verifies Apple's claim of rotating egress addresses. Nevertheless, it reveals that ingress and egress relays can be located in the same autonomous system, thus sharing similar routes, potentially allowing traffic correlation.

CCS CONCEPTS

• **Networks** → *Network measurement*.

KEYWORDS

Relay Networks, Overlay Networks, DNS ECS enumeration

ACM Reference Format:
Patrick Sattler, Juliane Aulbach, Johannes Zirngibl, and Georg Carle. 2022. Towards a Tectonic Traffic Shift? Investigating Apple's New Relay Network. In *Proceedings of the 22nd ACM Internet Measurement Conference (IMC '22), October 25–27, 2022, Nice, France.* ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3517745.3561426

IMC '22, October 25–27, 2022, Nice, France

ACM ISBN 978-1-4503-9259-4/22/10.
https://doi.org/10.1145/3517745.3561426

1 INTRODUCTION

Apple presented iCloud Private Relay [16] as a new privacy protection service at its developer conference (WWDC) in June 2021. The first beta release was included with iOS 15. This new system seeks to protect its user's privacy by proxying the traffic through an Apple-controlled ingress to an externally controlled egress node. The service's advertised purpose is to protect the visibility of the user's Internet activity. It hides the communication partners from passive network observers (*e.g.*, Internet service providers (ISPs)).

The barrier to entry for iCloud Private Relay is much lower compared to competing privacy protection techniques (*e.g.*, Virtual Private Networks (VPNs), Proxies, The Onion Router (Tor)). All paying iCloud+ customers can use it on their Apple devices. Currently, the cheapest iCloud+ plan is $0.99 per month, which is only a fraction of what, *e.g.*, VPN operators typically charge. iCloud Private Relay is integrated into Apple's iOS, iPadOS, and macOS operating systems. Apple's global smartphone market share is 25 % [33]. All iCloud+ customers can use the relay network by flipping a switch in their device settings. Apple also announced that it would turn on the service by default after it left the beta testing phase. We expect to see a significant usage increase when that happens. The ease-of-use aspect, the hidden metadata, and a potential broad adoption scenario are also alarming to the actors in the networking community (see [37]).

This paper analyzes the goals, architecture, and behavior of iCloud Private Relay to provide fellow researchers and network operators insight into the system and what they can expect when the service adoption gains traction. iCloud Private Relay influences the operation of passive network analysis, and due to its workings, it can also impact intrusion detection systems (IDSs). Its structure also allows the participating Content Delivery Networks (CDNs), which host the egress nodes, to use their involvement in this system to provide content hosted with them faster than 3rd-party content. The focus of this paper is the network point of view, and where applicable, we evaluate the effect of our findings on the system's privacy and security.

This paper provides the following contributions:

(i) We analyze the iCloud Private Relay ingress layer and collect 1586 IPv4 and 1575 IPv6 ingress relay IP addresses through active

Domain Name System (DNS) scans. The ingress addresses can be used to identify relay traffic as a passive network observer. Researcher can use our published results in their analysis.
(ii) We evaluate the egress addresses and show their geographical and topological bias towards the US. The egress addresses provide us with a better understanding of the service's deployment status.
(iii) We perform active scans through the relay network and find that the egress relay not only rotates its address but also does this for every new client connection. Services similar to iCloud Private Relay (*e.g.*, VPN, Tor) do not exhibit such a behavior. Therefore, IDSs need to consider this new type of connection pattern. The scans also reveal that ingress and egress addresses can be located behind the same last-hop router, enabling the network operator to perform correlation attacks similar to the ones known for Tor [11, 22, 27].
(iv) In Section 6 we discuss our results considering a broader usage in the future. We consider passive network analyses, the topological location of relay nodes, and the impact on network defense systems.

We publish data used throughout this work as a research data archive [31] and provide current and future measurement results at: *https://relay-networks.github.io*.

Outline: We introduce iCloud Private Relay in detail in Section 2 and describe our measurement setup and scans in Section 3. We analyze ingress relays, egress relays, and their interplay in Section 4. In Section 5 we list related work, and Section 6 concludes the paper with a discussion on our findings and the design of iCloud Private Relay.

2 ICLOUD PRIVATE RELAY

iCloud Private Relay is a new service provided by Apple [16] in order to protect the user's privacy. It aims to protect unencrypted HTTP traffic, DNS queries, and connections initiated by Apple's web browser Safari. Moreover, no network operating party can observe the client and server addresses directly. The architecture of iCloud Private Relay (see Figure 1) is built as a two-layer relay structure as lined out in its whitepaper [16]. Clients, *i.e.*, iOS or MacOS devices, connect to an ingress relay for authentication and location assignment. The clients use this information to initiate a proxy connection to the egress relay through the ingress. The latter then initiates the connection to the actual target host. Apple *operates* the ingress layer relays, while CDN providers Akamai, Cloudflare, and Fastly operate the egress relays (*cf.*, Section 4.2). Note that while Apple states it operates the ingress layer nodes, Section 4.1 shows that these are not necessarily located in a network Apple operates.

This architecture enables several advantages compared to traditional proxy or VPN services, *e.g.*, the egress layer can initiate the connection and use additional latency-reducing techniques (*e.g.*, using TCP fast open). Cloudflare, an egress relay operator, claims to use Argo [21], its *virtual backbone* which analyzes and optimizes routing decisions [20] and improves connection performance. We assume the other CDN egress operator have similar measures in place. These measures might be enough to equalize any latency drawbacks due to the two-hop relay system.

Proxying traffic through the ingress relay protects the client's IP address from the egress relay, the destination server, and the network operating entities on the path between the relay to the destination. Conversely, the ingress relay cannot decrypt traffic to the egress and is, therefore, unable to observe the destination address or any other information. Network operators between client and ingress are also unable to observe the actual destination address. This layered structure has similarities with anonymization networks such as Tor. Tor uses at least three layers, and volunteers independently operate its relays. In this paper, we will apply analysis approaches similar to the ones used for Tor localization and evaluation [17, 22, 23, 35].

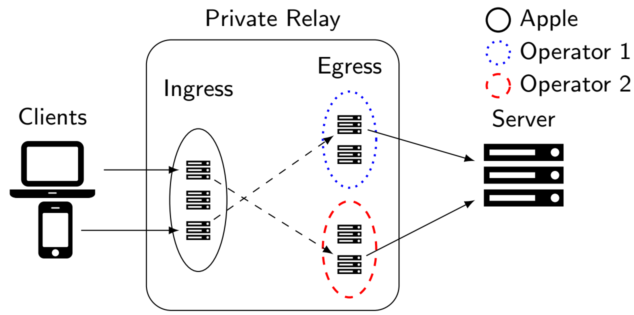


Figure 1: iCloud Private Relay Architecture. Ingress nodes are operated by Apple itself, while egress nodes are operated by different entities. Only the ingress can identify the client whereas only the egress knows the targeted service.

iCloud Private Relay uses QUIC for its connection to the ingress relay. The tunnel to the egress uses a secure proxying protocol using HTTP/3 [19, 29] proposed by the Multiplexed Application Substrate over QUIC Encryption (MASQUE) IETF working group [1]. HTTP/3 uses QUIC as the transport protocol providing a secure connection with the possibility to combine multiple connections within a single proxy connection. The service uses the fallback to HTTP/2 and TLS 1.3 over Transmission Control Protocol (TCP) when the QUIC connection fails. Clients resolve `mask.icloud.com` to obtain the ingress relay's addresses for the QUIC connection. During the TCP fallback, clients resolve `mask-h2.icloud.com`. The whitepaper explicitly states the possibility of blocking iCloud Private Relay by not resolving DNS requests for the service's domain names.

To authenticate servers, iCloud Private Relay relies on *raw public keys* (see RFC 7250 [38]) instead of the usual certificate authentication within its TLS handshake. Deployed key pinning prevents interception using TLS proxies, so an in-depth analysis of the protocol is infeasible. Additional measures for fraud prevention are in place, *e.g.*, a limited number of issued tokens to access the service per user and day.

iCloud Private Relay is unavailable in some countries where local laws do not permit Apple to operate it (*e.g.*, China, Belarus, and Saudi Arabia [24]). The current system claims to not use any network block circumvention mechanisms as Tor and VPN services often do. iCloud Private Relay can easily be blocked through its domain names. Differences compared to other tunneling services are that iCloud Private Relay does not apply to all traffic. Moreover, it uses the MASQUE proxying technique. Currently, proxying UDP traffic is not supported by MASQUE, but the MASQUE working group is working on a new draft [32].

3 MEASUREMENT AND ANALYSIS SETUP

We aim to shed light on the network-level implementation of the iCloud Private Relay and its inner workings. The ingress and egress relays are the visible points of the system from an external perspective. Collecting and understanding the properties of the relays is essential to understand the systems deployment and which prefixes and addresses are relevant for network analysis. Thus, we analyze ingress and egress relays regarding their topological distribution from a network perspective (*i.e.*, used addresses, prefixes, and operators). For all active measurements, we apply the ethical measures described in Section 7.

Relay IP Addresses: Apple does not publish used ingress IP addresses, unlike egress addresses. As ingress addresses are the relay network's entry point, it is crucial to obtain them. They can detect the presence and prevalence of relay network traffic. We rely on DNS queries for the domains used by iCloud Private Relay to obtain the ingress IP addresses. The iCloud Private Relay name servers are operated by AWS Route 53 and have the Extension Mechanisms for DNS (EDNS0) Client Subnet (ECS) extension enabled. ECS allows a resolver to attach the client's subnet to a DNS query [9]. The authoritative name server can use this query information to provide a subnet-based (*i.e.*, geolocation-based) response.

Streibelt et al. [34] and Calder et al. [6] first described ECS enumeration approaches. Our scan iterates over the IPv4 address space and sends A record queries with /24 subnets in its ECS extension to the authoritative name server. This ECS-based approach does not work for IPv6. The name server always returns an ECS scope indicating that the response is valid for the entire IPv6 address space.

To cover IPv6 (*AAAA* queries) and to verify the results obtained by the ECS-based scans, we use RIPE Atlas DNS measurements, offering globally distributed probes and thus a geographically distributed view. RIPE Atlas *A* queries are used to validate our ECS-based DNS scans. Additionally, we use the *A* and *AAAA* measurements to track the service's availability. We use the RIPE Atlas DNS resolutions to gain insight into the number of probes failing to resolve the service domain names. Even though RIPE Atlas probes are not distributed equally [5], they are located in 3326 different Autonomous Systems (ASes) and 168 countries and, therefore, can provide us with a distributed view. Tracking the availability is an important future task as the service can be easily blocked through DNS. Several ISPs voiced concerns [37] over the service, and some might start blocking it in their network.

In contrast to ingress relays, Apple publishes egress relay IP addresses for geolocation and allow-listing [15]. We assume this list to be complete and use it in the following.

Measurements using iCloud Private Relay: We perform several scans to improve our understanding of the system outside the published information. As explained in Section 2, we cannot examine the communication itself due to the pinned public key. In fact, testing standard QUIC handshakes using the QScanner published by Zirngibl et al. [39] or a current curl version does not even trigger a response by ingress nodes, neither a QUIC initial nor an error. The connection attempt times out. Interestingly, a version negotiation from ingress nodes can be triggered using the latest ZMap module from Zirngibl et al. [39] to identify QUIC support. The response indicates support for QUICv1 alongside drafts 29 to 27. These response properties verify that nodes support standardized QUIC, but due to its peculiarities, unintended handshakes are prevented.

Instead, we perform long-running measurements on a MacBook Pro laptop with iCloud Private Relay enabled to understand how often the egress operator and IP address change. The service emphasizes privacy as the primary goal and announces to rotate the egress IP address regularly, a feature unique among similar services (*e.g.*, VPN, Tor). The address rotation hinders IP address-based tracking significantly more than without it. For this, we set up a MacOS laptop running the latest OS version as a client for the iCloud Private Relay and deployed a simple web server to observe the egress relay's connection attempt. The scan performs two requests: *(i)* It instructs *Safari* to open the URL to our web server; and *(ii)* we use curl to fetch `http://ipecho.net/plain`, a service that mirrors the requester's IP address. We directly log the requester's IP address on our web server and extract the IP address from the response of `http://ipecho.net/plain`. Therefore, we can observe and correlate ingress *and* egress relay operator and evaluate how parallel connections behave.

We implement this scan in two versions. *(i)* An open scan, where required DNS queries are sent to a local recursive resolver to initiate the iCloud Private Relay connection. Thus, this scan uses IP addresses received live from authoritative name servers. *(ii)* We perform scans forcing the client to use specific DNS configurations. Therefore, we deploy and use a local unbound resolver to steer the service's DNS resolution. A custom configured local zone for the required domain names can direct the service to a selected ingress relay. Such a forced ingress selection allows us to test the relay's behavior when using different IP addresses from our ECS scan results as ingress nodes.

4 ANALYSIS OF SCANNING RESULTS

In the following section, we analyze the topological distribution and inner workings of the iCloud Private Relay.

4.1 Uncovering Ingress Relays

We use the ECS scans to uncover globally distributed ingress addresses from a single vantage point and verify its results in the second part of this section by using RIPE Atlas measurements.

ECS DNS scans: Table 1 gives an overview of the number of seen ingress IP addresses per AS from four scans between January and April 2022. Ingress addresses are located at Apple (AS714) or Akamai (AS36183) and within 123 routed BGP prefixes. AS36183 appears to be only recently active in BGP and is related to iCloud Private Relay. We use Akamai$_{PR}$ to denote AS36183. The increase of ingress addresses is solely attributable to Akamai$_{PR}$. Especially, the fallback TCP relays were initially served by Apple, and only after the deployment of relays at Akamai$_{PR}$ the fallback relays could catch up with the QUIC relays.

In April, our scan uncovered 1586 ingress IP addresses in responses with up to eight different records. Akamai$_{PR}$ locates more than 75 % of all relays. Therefore, the question arises: How reliant is iCloud Private Relay from Akamai$_{PR}$, *i.e.*, who serves its clients? The ECS scan collects this information as the sent extension data represents the client's subnet. The name server always uses the

Table 1: The ASes of ingress relays and their proportional distribution. Only Apple and the recently occurring Akamai$_{PR}$ AS (AS36183) is visible. In January the fallback scan is absent.

	Default				Fallback			
	Apple		Akamai		Apple		Akamai	
Jan	365	30.6%	823	69.4%	-	-	-	-
Feb	355	29.5%	845	70.5%	356	100.0%	-	-
Mar	347	26.9%	945	73.1%	334	93.0%	25	7.0%
Apr	349	22.0%	1237	78.0%	336	24.0%	1062	76.0%

Table 2: Number of client ASes served by each ingress relay AS for the scan in April. The AS population is sourced from the APNIC AS pop data [3].

AS	AS Pop	ASes	/24 Subnets
Akamai$_{PR}$	994M	34 627	1.1M
Apple	105M	20 807	0.2M
Both[1]	2373M	17 301	10.6M

[1] Apple's subnet share is 76 %

subnet provided in the query, and all response records are in the same AS. As we send /24 client subnets, we obtain a /24 prefix granularity. Table 2 summarizes the collected data on AS and subnet levels.

Although Apple only provides 25 % of all ingress IP addresses, it serves 69 % of all subnets. We use the APNIC AS population dataset [3] to understand how many potential users are served by the two operators. As the population dataset has only an AS granularity, ASes served by both cannot be attributed. These ASes contain the largest share of subnets and users. The relays at Akamai$_{PR}$ exclusively cover 34.6 k ASes with 994 M users. In comparison, relays at Apple only cover 105 M users in 20.8 k ASes. This breakdown shows that the deployment in the Apple AS differs from the one in Akamai$_{PR}$. If network traffic is evaluated on a service level, it is crucial to consider this split-world for iCloud Private Relay. Our ingress address dataset helps to attribute IP addresses and aggregate service level data.

iCloud Private Relay evolved during our four-month observation period: The number of QUIC-enabled relays increased by 34 %, and the number of relays for the TCP fallback increased from only 356 addresses to 1398 (+293 %) in April. Such a development is expected for a service in its beta phase. It shows the importance of continuous measurements to understand its impact. We will perform regular scans in the future and publish the collected ingress addresses.

ECS Scan Validation: The ECS-based ingress scan uses the DNS extension's properties to get a distributed view of the service. We perform these scans from a single vantage point. Therefore, they are susceptible to anycast-based behavior differences. To validate our results, we use the RIPE Atlas measurement platform, which allows us to perform DNS measurements on more than 10 k available probes. The RIPE Atlas probe location bias towards North America and Europe is similar to the egress subnet locations (*cf.*, Section 4.2). Therefore, we acknowledge the uneven distribution of RIPE Atlas but argue that it also roughly represents the current service deployment of iCloud Private Relay.

In total, our RIPE Atlas measurements in April report 1382 distinct ingress IPv4 addresses, *i.e.*, 200 fewer than the ECS scan at a similar time. All but one address from the RIPE Atlas measurement are also visible in our ECS scan. The single missing address can be attributed to the time difference between the two scans. While the RIPE Atlas scan only takes minutes, our ECS scan takes up to 40 hours due to the strict rate limiting. We can find this single missing address during the following verification ECS scans. We conclude that our ECS scan can uncover not only all addresses seen by the RIPE Atlas measurement but also 200 additional ones.

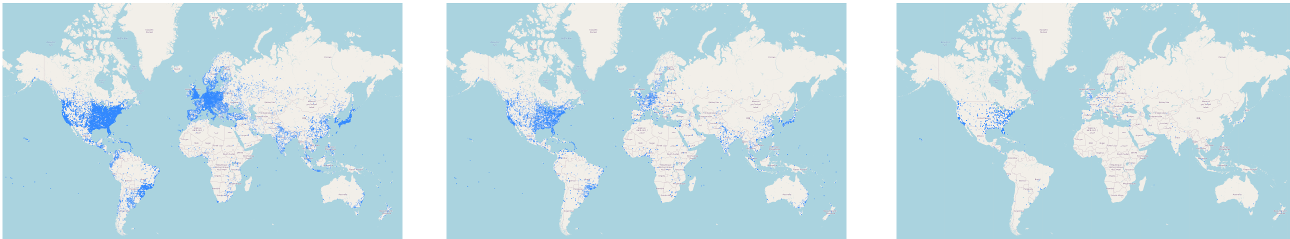
IPv6 Ingress Addresses: We also perform four *AAAA* DNS scans with RIPE Atlas as our ECS scan only supports IPv4 with A type records. We use *AAAA* measurements targeting the local resolver and an authoritative name server. According to our measurement towards `whoami.akamai.net`, which returns the resolver's requester IP address, more than half of all probes use one of the following resolvers: Google's public resolver [14], Cloudflare's public resolver [8], Quad9 [2], or OpenDNS [7]. Although, the geographical bias of RIPE Atlas probes and the concentrated public resolver usage limits the visibility of this scan, resolvers are visible in 1.8 k different ASes.

In total, we find 1575 IPv6 addresses in the same two ASes. The size of the discovered IPv6 address set through RIPE Atlas is larger than the IPv4 one, possibly due to the larger address space. The AS share of addresses is similar to what we find in our ECS scans: 346 relays are within Apple's AS and 1229 relays are provided by the Akamai$_{PR}$ AS. The DNS requests directed to an authoritative name server do not expose significantly more or other addresses as the resolver scan does. This measurement provides us basic view into the IPv6 side of the service.

State of Service Blocking: We analyze the RIPE Atlas DNS errors to check where the DNS resolution fails and where the service might be blocked. 10 % of all requested probes fail with a request timeout. An additional measurement towards another domain showed similar timeout shares. Therefore, we do not account these as service blocking attempts. Nevertheless, 7 % of the probes fail to resolve the domain name but receive a DNS response by their resolver. 72 % of these probe's response codes are *NXDOMAIN*, 13 % *NOERROR*, and 5 % *REFUSED*. The remaining ones report either *SERVFAIL* or *FORMERR*. Responses with *NXDOMAIN* or *NOERROR* with no data are responses where the resolver claims to have completed the resolution to the authoritative name server and to have returned its result. We know that the authoritative name server does not respond with any of the results above. Therefore, we attribute these response codes as intentional blocking of the iCloud Private Relay domain names. In one occurrence we observe a DNS hijack hinting at the use of nextdns.io, a DNS resolver claiming to protect from different Internet threats. The instances returning *REFUSED* might also be caused by erroneous DNS setups but in our case we verified the functioning of the resolver using a second unrelated domain. Therefore, we find a total of 645 (5.5 %) probes without access to the service due to DNS blocking.

4.2 Egress Nodes

The egress node is the second hop of the iCloud Private Relay infrastructure. Depending on the selected option, the node either



(a) **Akamai$_{PR}$ and Akamai$_{Est}$** (b) **Cloudflare** (c) **Fastly**

Figure 2: Geolocation of egress subnets per providing AS[1].

Table 3: Comparison of egress subnets for the operating ASes. Number of possible IPv6 addresses is left out, since every subnet mask has length 64.

	IPv4			IPv6		
	Subnets	BGP Pfxs	IP Addr.	Subnets	BGP Pfxs	CCs
Akamai$_{PR}$[1]	9890	301	57 589	142 826	1172	236
Akamai$_{Est}$[2]	1602	1	5100	23 495	1	24
Cloudflare[3]	18 218	112	18 218	26 988	2	248
Fastly[4]	8530	81	17 060	8530	81	236

[1] AS36183; [2] AS20940; [3] AS13335; [4] AS54113

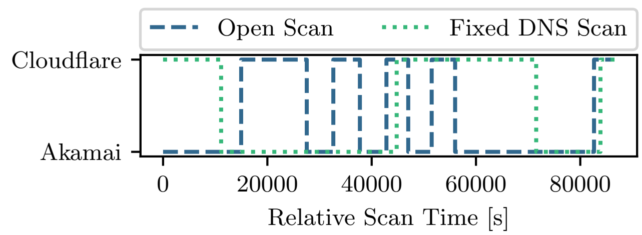


Figure 3: Egress operator changes over the course of a scan day.

maintains the user's region by leveraging geohash information or only preserves the country and time zone. Apple provides a list of the egress nodes [15] that currently (2022-05-11) contains 238 k subnets, each mapped to a represented country code (CC), region, and city. For 1.6 % of the subnets, the city is missing. We assume those subnets are used if a user does not want to maintain the region, leaving it blank for our analysis. Compared to Jan. 2022, the number of subnets grew by 15 % with little churn.

AS Distribution: As depicted in Table 3 the subnets are all in the ASes of Akamai, Cloudflare, and Fastly, with Akamai being represented by two different ASes, namely Akamai$_{PR}$ (AS36183) and AS20940. We refer to the latter as Akamai$_{Est}$. Interestingly, Akamai$_{PR}$ also hosts ingress nodes, as shown in Section 4.1, thus combining both layers of the iCloud Private Relay within the same AS. While Cloudflare offers the most IPv4 subnets, Akamai provides more possible IP addresses. Regarding IPv6, Akamai is offering the most subnets. All listed IPv6 subnets by Apple have a 64 bit subnet mask. Hence no number of addresses is explicitly given. For the 9890 subnets of Akamai$_{PR}$, we see 301 different routed BGP prefixes, whereas Akamai$_{Est}$ routes all 1602 subnets over the same BGP prefix. This single IPv4 BGP prefix contains subnets covering 18 countries distributed over North and South America and Europe. Even though the egress relays could theoretically all be placed at the Apple-provided location, it does not seem likely as to get low latency relays have to be located in a topologically convenient place. Akamai publishes a list of countries with points of presence. We compared this list to the countries in the egress list and found several small countries (*e.g.*, Saint Kitts and Nevis) with a representing IP address from Akamai but without any point of presence. This analysis shows that the published location information does not necessarily represent the egress node's actual location but is used to represent the client's assumed location.

We also used the MaxMind GeoLite2 geolocation database to obtain the location for the egress IP addresses and found that they adapted the Apple egress mapping for most subnets. Among others, MaxMind advertises its GeoIP databases to be used for content customization and advertising. Therefore, their goal is to represent the user's location, not the relay node's actual location, and thus these databases cannot be used to determine the relay node's location.

Geo Distribution: Figure 2 shows the distribution of egress subnets over the globe. Cloudflare provides egress relays in 248 and Akamai and Fastly in 236 CCs. There are only 11 CCs that one AS uniquely covers; in all cases, this AS is Cloudflare. Akamai$_{PR}$ covers all CCs that Akamai$_{Est}$ covers plus 212 more. The analysis of cities covered by subnets (see Appendix A) shows an even distribution across operators (800 to 1000) for IPv4. However, while Fastly does not, Akamai and Cloudflare provide a manifold (14 k and 5 k respectively) of cities with IPv6 subnets. Note that more than 58 % of all subnets cover the US, and the second largest CC is DE, with only 3.6 %. Therefore, iCloud Private Relay has a massive bias towards the US in its current deployment, while a set of 123 countries are assigned less than 50 subnets each.

4.3 Scans Through the Relay

This section looks at the scans through the iCloud Private Relay. We perform the two requests (using curl and Safari) every five minutes over over a day on multiple days in May 2022. We look at: *(i)* the chosen egress operator and *(ii)* the egress address rotation behavior.

[1]Data by ©OpenStreetMap (http://openstreetmap.org/copyright), under ODbL (http://www.openstreetmap.org/copyright)

Cloudflare and Akamai$_{PR}$ are the only ASes visible as egress operators. Fastly's absence is explained by its sparse presence at our measurement location. Figure 3 shows changes between egress operators relative to the scan start. The open DNS resolution scan has a handful of seemingly regular operator changes in the middle of its scan, but no pattern over the full scan time is visible. Similarly, the *fixed* scan does not indicate regular operator changes.

Compared to operators, egress addresses change more regularly, on average, after every second request. We adapt our scan to reduce the time between each request round to 30 seconds to get a more fine-grained resolution. During the observation period of 48 hours we find six different egress addresses from four egress subnets. In more than 66 % of the request attempts, the address changes compared to the previous one. Due to the relatively low number of six different addresses, it seems plausible that the egress relay selects the address per connection attempt. We can also support this claim based on the occurrence of different egress addresses for the parallel curl and Safari requests. To summarize these findings, we can verify the whitepaper's [16] claim about address rotation, and it seems suitable to protect the user's IP address from multiple operators in parallel.

Finally, we did not observe egress behavior or address differences when forcing a specific ingress relay address.

5 RELATED WORK

iCloud Private Relay has similar goals and architecture as other anonymization tools (*e.g.*, Tor) and it encounters the same problems. Different research groups [11, 22, 27] showed how Tor services could be located and passively observed to perform traffic analysis. Others [10, 18, 23, 26] analyzed to which degree ASes can de-anonymize Tor traffic based on the correlation of traffic entering and leaving the Tor layers. Given the small number of involved operators of the relay network and Akamai$_{PR}$ containing ingress and egress relays, similar correlations are drastically more straightforward. We discuss this in more detail in Section 6.

MASQUE is used by iCloud Private Relay to proxy the users traffic. Kühlewind et al. [19] evaluated the performance metrics of MASQUE proxies and found, among other things, an increased RTT when congestion occurs on the target host.

6 DISCUSSION AND CONCLUSION

Shortly after the announcement of iCloud Private Relay, the system gained significant attention, especially from network operators debating its architecture and potential impact. This section discusses our results and how research and network operators can use them to prepare for more significant system adoption. Moreover, we present findings as part of our system analysis, giving a new viewpoint on the promised privacy claims. In the following, we assume a wide adoption of iCloud Private Relay in the future.

Passive Measurements and iCloud Private Relay: Network engineers and researchers use passive network measurements to, *e.g.*, analyze service usage, traffic categories, and user behavior [12, 13, 36]. Clients moving seemingly randomly from one egress address to a different one were not yet part of the requirements. Furthermore, the service potentially multiplexes various traffic and service types in the future. Especially the egress address rotation and the fact that a client can have multiple parallel connections with differing egress addresses pose a challenge for passive analyses. These properties differ significantly from the behavior of similar technologies. Therefore, iCloud Private Relay potentially introduces a new client request pattern that might be classified as anomalous by IDSs (*e.g.*, see issue report on Imperva DDoS and iCloud Private Relay [25]). We suggest consulting the published egress list to identify matching addresses to mitigate the issues.

Research evaluating user behavior using network monitoring in access networks and ISPs needs to tae the client-side properties of the service into account. The analysis of ISP network data, as done by Trevisan et al. [36] and Feldmann et al. [12], would not be able to differentiate the service types for relay traffic. Ingress relays will appear as a highly active destination, but the attribution of traffic to the user's visiting service is impossible. Moreover, ISPs need to evaluate their paths towards the ingress addresses as an increased load on these should be expected. These newly appearing traffic patterns can be attributed to our ingress address dataset.

Akamai's Presence and its Implications: Apple claims that tracking users is impossible due to the two layers and separation between operators into distinct entities. The corresponding stated goal is: "No one entity can see both who a user is (IP address) and what they are accessing (origin server)"[30]. According to Apple's claims, distributing the service's duties prevents such a correlation. We use our previous findings to evaluate this claim on a network level.

If an operator can see both the connection by the client to the ingress and the traffic from the egress relay to the target, it can infer the actual communication partners. The MASQUE draft [29] explicitly lists traffic analysis as an issue the protocol cannot overcome. If an observing entity is the egress relay operator, it can use the timing of the requests to extract metadata information and use the relay's provided geohash. The service derives the geohash from the IP address geolocation, and when the entity observes the client's IP address on the ingress, it can derive its approximate geohashes.

Akamai$_{PR}$ locates the largest number of ingress as well as egress relays. Therefore, it was no surprise that we find occurrences of the AS in the ingress and the egress in our relay scan (see Section 4.3). We validated these findings through traceroute measurements and found the same last hop address for ingress and egress addresses. In contrast to the MASQUE draft, iCloud Private Relay does not only define the protocol but has also designed its architecture and deployment strategy. Apple could ensure that ingress and egress addresses are not part of the same AS and entity to prevent such an issue in the future. Nevertheless, currently, the AS contributing the largest share of ingress and egress relays is also the source of this traffic analysis issue.

Akamai$_{PR}$ as the culprit of this problem has only one publicly visible peering link to Akamai$_{Est}$, providing egress relay nodes. In total, the 478 IPv4 and 1335 IPv6 BGP prefixes are visible. We find at least one ingress relay in 201 and one egress relay in 1472 prefixes (IPv4+IPv6). Given that ingress and egress relays at least do not share the same BGP prefix, 92.2 % (1673) of announced prefixes are used for iCloud Private Relay.

We examined the BGP visibility of the AS monthly from 2016 to 2022. Its first occurrence was detected in June 2021, coinciding with the launch of iCloud Private Relay. This information strongly hints that Akamai$_{PR}$ is specifically used for iCloud Private Relay. For this purpose, we have sent an inquiry to Akamai, which could not be answered due to proprietary information. Nevertheless, it seems to be an odd decision to design the system with the claimed privacy goals, but these mentioned issues as Apple is directly involved in writing the MASQUE draft.

Conclusion: In this work, we provide an overview of iCloud Private Relay and highlight its effect on future research and network operators. We collect an ingress address data set that can be used to identify client connections to the iCloud Private Relay. Our scans uncover the Akamai private relay AS that locates ingress and egress relays and potentially allows traffic correlation.

During this study, we found some research topics we consider important in the future: *(i)* Where and how is traffic routed to and from the relay nodes? Does the system have bottlenecks that can lead to congestion for its users? *(ii)* How does the system evolve, and where is it available? Some countries disallow its usage due to the censorship evasion possibility. *(iii)* How does the service impact the user's QoE? Apple claims the impact is low, and caching would also lead to faster page load times.

7 ETHICS

Before conducting active measurements we follow an internal multiparty approval process, which incorporates proposals by Bailey et al. and Partridge and Allman. We asses if our measurements induce harm on scanned infrastructure or other actors and minimize the risk of doing so. In this paper we performed active Internet scans towards a limited target set. We apply a strict query rate limit for all of our scans. Our scanning IP range has an according WHOIS entry, reverse DNS entries and the scanning hosts operate an informational webpage. We comply with opt-out requests and operate a blocklist for all our scans. All our active scans target either services or our own infrastructure. This works measurements did not trigger any abuse notification.

We apply additional measures to reduce the number of ECS queries. To lower the load on the authoritative name servers, we sparsely scan the address space not seen as routable by our local BGP router. This address space is not valuable as it does not contain possible users for the service. We also respect the ECS information sent by the name server, *i.e.*, the validity of the answer for a prefix of any size. If the prefix is large than /24, we do not perform any other ECS query within that prefix. These measures help to reduce the number of redundant queries needed and therefore are beneficial for the scanned infrastructure.

ACKNOWLEDGMENTS

The authors would like to thank the anonymous reviewers and our shepherd Alan Mislove for their valuable feedback. This work was partially funded by the German Federal Ministry of Education and Research under the project PRIMEnet, grant 16KIS1370.

REFERENCES

[1] 2020. *Multiplexed Application Substrate over QUIC Encryption.* Retrieved May 11, 2022 from https://datatracker.ietf.org/doc/charter-ietf-masque/
[2] 2022. *Quad9.* Retrieved 2022-05-14 from https://www.quad9.net/
[3] APNIC. 2022. *Visible ASNs: Customer Populations.* Retrieved 2022-05-14 from https://stats.labs.apnic.net/aspop
[4] Michael Bailey, David Dittrich, Erin Kenneally, and Doug Maughan. 2012. The Menlo Report. *IEEE Security Privacy* (2012).
[5] Vaibhav Bajpai, Steffie Jacob Eravuchira, and Jürgen Schönwälder. 2015. Lessons Learned From Using the RIPE Atlas Platform for Measurement Research. *SIGCOMM Comput. Commun. Rev.* (jul 2015).
[6] Matt Calder, Xun Fan, Zi Hu, Ethan Katz-Bassett, John Heidemann, and Ramesh Govindan. 2013. Mapping the Expansion of Google's Serving Infrastructure. In *Proceedings of the 2013 Conference on Internet Measurement Conference* (Barcelona, Spain) *(IMC '13)*. Association for Computing Machinery, New York, NY, USA.
[7] Cisco. 2022. *OpenDNS.* Retrieved 2022-05-14 from https://www.opendns.com/
[8] Cloudflare. 2022. *1.1.1.1.* Retrieved 2022-05-14 from https://developers.cloudflare.com/1.1.1.1/
[9] Carlo Contavalli, Wilmer van der Gaast, David C Lawrence, and Warren "Ace" Kumari. 2016. Client Subnet in DNS Queries. RFC 7871. https://www.rfc-editor.org/info/rfc7871
[10] Matthew Edman and Paul Syverson. 2009. As-Awareness in Tor Path Selection. In *Proc. ACM SIGSAC Conference on Computer and Communications Security (CCS)* (Chicago, Illinois, USA).
[11] Nick Feamster and Roger Dingledine. 2004. Location Diversity in Anonymity Networks. In *Proceedings of the 2004 ACM Workshop on Privacy in the Electronic Society* (Washington DC, USA).
[12] Anja Feldmann, Oliver Gasser, Franziska Lichtblau, Enric Pujol, Ingmar Poese, Christoph Dietzel, Daniel Wagner, Matthias Wichtlhuber, Juan Tapiador, Narseo Vallina-Rodriguez, Oliver Hohlfeld, and Georgios Smaragdakis. 2020. The Lockdown Effect: Implications of the COVID-19 Pandemic on Internet Traffic. In *Proc. ACM Int. Measurement Conference (IMC)* (Virtual Event, USA).
[13] Romain Fontugne, Patrice Abry, Kensuke Fukuda, Darryl Veitch, Kenjiro Cho, Pierre Borgnat, and Herwig Wendt. 2017. Scaling in Internet Traffic: A 14 Year and 3 Day Longitudinal Study, With Multiscale Analyses and Random Projections. *IEEE/ACM Transactions on Networking* (2017).
[14] Google. 2022. *Public DNS.* Retrieved 2022-05-14 from https://developers.google.com/speed/public-dns/
[15] Apple Inc. 2021. *Access IP geolocation feeds.* Retrieved 2022-05-16 from https://mask-api.icloud.com/egress-ip-ranges.csv
[16] Apple Inc. 2021. iCloud Private Relay Overview. (2021). https://www.apple.com/privacy/docs/iCloud_Private_Relay_Overview_Dec2021.PDF
[17] Aaron Johnson, Chris Wacek, Rob Jansen, Micah Sherr, and Paul Syverson. 2013. Users Get Routed: Traffic Correlation on Tor by Realistic Adversaries. In *Proc. ACM SIGSAC Conference on Computer and Communications Security (CCS)* (Berlin, Germany).
[18] Aaron Johnson, Chris Wacek, Rob Jansen, Micah Sherr, and Paul Syverson. 2013. Users Get Routed: Traffic Correlation on Tor by Realistic Adversaries. In *Proc. ACM SIGSAC Conference on Computer and Communications Security (CCS)* (Berlin, Germany).
[19] Mirja Kühlewind, Matias Carlander-Reuterfelt, Marcus Ihlar, and Magnus Westerlund. 2021. Evaluation of QUIC-Based MASQUE Proxying. In *Proceedings of the 2021 Workshop on Evolution, Performance and Interoperability of QUIC* (Virtual Event, Germany).
[20] Rustam Lalkaka. 2017. *Introducing Argo — A faster, more reliable, more secure Internet for everyone.* Retrieved 2022-09-13 from https://blog.cloudflare.com/argo/
[21] Rustam Lalkaka. 2022. *iCloud Private Relay: information for Cloudflare customers.* Retrieved 2022-09-13 from https://blog.cloudflare.com/icloud-private-relay/
[22] Steven J. Murdoch and George Danezis. 2005. Low-Cost Traffic Analysis of Tor. In *Proc. IEEE Symposium on Security and Privacy (S&P).*
[23] Milad Nasr, Alireza Bahramali, and Amir Houmansadr. 2018. DeepCorr: Strong Flow Correlation Attacks on Tor Using Deep Learning. In *Proc. ACM SIGSAC Conference on Computer and Communications Security (CCS)* (Toronto, Canada).
[24] Stephen Nellis and Paresh Dave. 2022. *Apple's new 'private relay' feature will not be available in China.* Retrieved 2022-09-03 from https://www.reuters.com/world/china/apples-new-private-relay-feature-will-not-be-available-china-2021-06-07/
[25] Lyndon Nerenberg. 2022. *Imperva / Apple Private Relay issues.* Retrieved 2022-09-15 from https://mailman.nanog.org/pipermail/nanog/2022-September/220491.html
[26] Rishab Nithyanand, Oleksii Starov, Adva Zair, Phillipa Gill, and Michael Schapira. 2016. Measuring and Mitigating AS-level Adversaries Against Tor. In *Proc. Network and Distributed System Security Symposium (NDSS).* San Diego, CA.
[27] Lasse Overlier and Paul Syverson. 2006. Locating Hidden Servers. In *Proc. IEEE Symposium on Security and Privacy (S&P).*
[28] Craig Partridge and Mark Allman. 2016. Ethical Considerations in Network Measurement Papers. *Commun. ACM* (2016).
[29] Tommy Pauly and David Schinazi. 2022. *QUIC-Aware Proxying Using HTTP.* Internet-Draft draft-pauly-masque-quic-proxy-03. Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/draft-pauly-masque-quic-proxy-03 Work in Progress.
[30] Pauly, Tommy. 2008. *iCloud Private Relay.* Retrieved May 11, 2022 from https://datatracker.ietf.org/meeting/111/materials/slides-111-pearg-private-relay-00

[31] Patrick Sattler, Juliane Aulbach, Johannes Zirngibl, and Georg Carle. 2022. *Data and Analysis at TUM University Library.* https://mediatum.ub.tum.de/1687050 doi:10.14459/2022mp1687050.
[32] David Schinazi. 2022. Proxying UDP in HTTP. RFC 9298. https://www.rfc-editor.org/info/rfc9298
[33] Statista. 2022. *Mobile operating systems' market share worldwide from January 2012 to January 2022.* Retrieved 2022-05-14 from https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009/
[34] Florian Streibelt, Jan Böttger, Nikolaos Chatzis, Georgios Smaragdakis, and Anja Feldmann. 2013. Exploring EDNS-Client-Subnet Adopters in Your Free Time. In *Proc. ACM Int. Measurement Conference (IMC)* (Barcelona, Spain).
[35] Yixin Sun, Anne Edmundson, Laurent Vanbever, Oscar Li, Jennifer Rexford, Mung Chiang, and Prateek Mittal. 2015. RAPTOR: Routing Attacks on Privacy in Tor. In *24th USENIX Security Symposium (USENIX Security 15)*. USENIX Association, Washington, D.C.
[36] Martino Trevisan, Danilo Giordano, Idilio Drago, Maurizio Matteo Munafò, and Marco Mellia. 2020. Five Years at the Edge: Watching Internet From the ISP Network. *IEEE/ACM Transactions on Networking* (2020).
[37] Woods, Ben and Titcomb, James. 2022. *Apple under fire over iPhone encryption tech.* Retrieved May 11, 2022 from https://www.telegraph.co.uk/business/2022/01/09/apple-fire-iphone-encryption-tech/
[38] Paul Wouters, Hannes Tschofenig, John IETF Gilmore, Samuel Weiler, and Tero Kivinen. 2014. Using Raw Public Keys in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS). RFC 7250. https://doi.org/10.17487/RFC7250
[39] Johannes Zirngibl, Philippe Buschmann, Patrick Sattler, Benedikt Jaeger, Juliane Aulbach, and Georg Carle. 2021. It's over 9000: Analyzing early QUIC Deployments with the Standardization on the Horizon. In *Proc. ACM Int. Measurement Conference (IMC)* (Virtual Event, USA).

A LOCATIONS COVERED BY EGRESS OPERATORS

The important findings regarding egress node locations are collected in Section 4.2. The following presents numbers (Table 4) and visualizes these results in more detail, cities (Figures 4a and 4b), covering CCs (Figures 4c and 4d), and a visualization of egress node locations separated into IP versions (Figure 5). The US are the top CC which subnets got assigned to and a focus towards North America and Europe is currently visible.

Table 4: Number of CCs by IPv4 subnets, IPv6 subnets and both combined.

	Covered Cities	Covered Cities IPv4	Covered Cities IPv6
Akamai_{PR} [1]	14 088	853	14 085
Akamai_{Est} [2]	7507	455	7507
Cloudflare[3]	5228	1134	5228
Fastly[4]	848	848	848

[1] AS36183; [2] AS20940; [3] AS13335; [4] AS54113

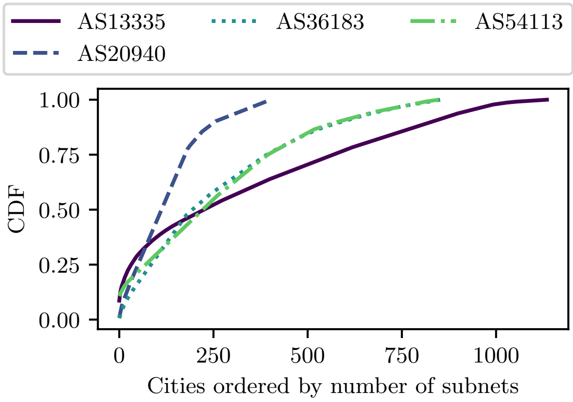
B ADDITIONAL OBSERVATIONS

Apple introduced Oblivious DNS over HTTPS (ODoH) to describe DNS in iCloud Private Relay. DNS queries are sent encrypted through the first relay, similar to the HTTP requests but are then routed directly to the DNS over HTTPS (DoH) server. The client can learn its egress IP address and include it in the DNS queries ECS information to receive an optimized response for the egress layer.

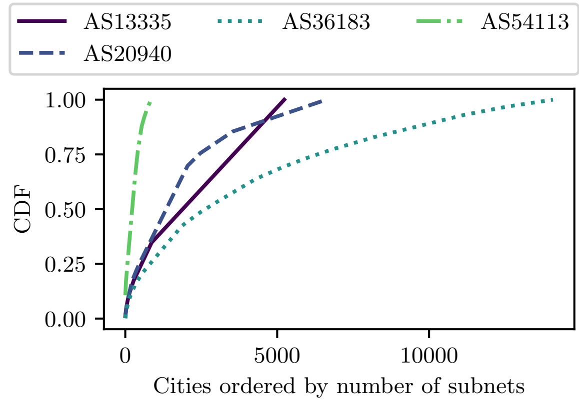
Given an active relay connection, the system ignores the local DNS resolver and uses its oblivious DoH server, *i.e.*, a DoH server connection through the relay system. Currently, we identify Cloudlfare's public resolver [8] as the one being used.

During our manual iCloud Private Relay testing we observed that the service accepts the provided DNS records and connects to the corresponding ingress relay. Nevertheless, after a short period of time we see that an additional QUIC connections is initiated. In our observation, its target address is in the prefix (or AS in the dual stack case) of the configured ingress. We assume these being backup or management connections to control the service on the client outside the actual service connection.

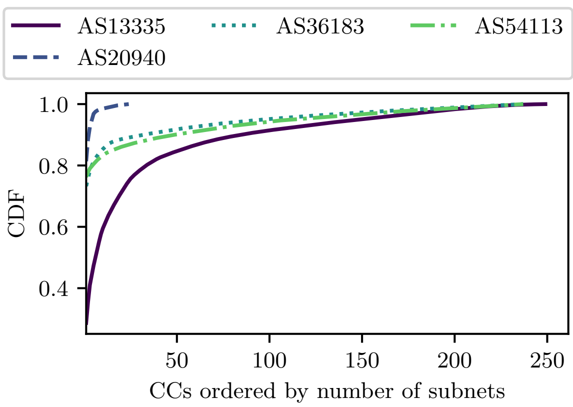
[2]Data by ©OpenStreetMap (http://openstreetmap.org/copyright), under ODbL (http://www.openstreetmap.org/copyright)



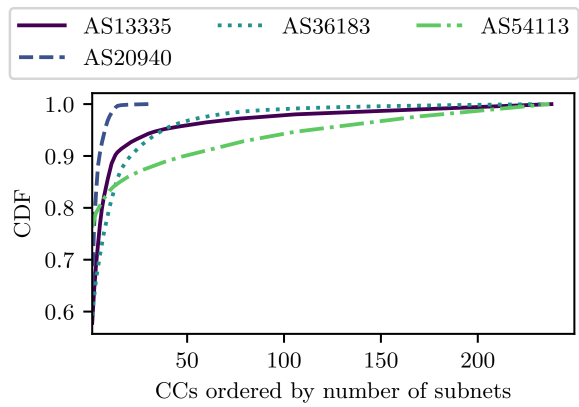
(a) IPv4 - Cities



(b) IPv6 - Cities

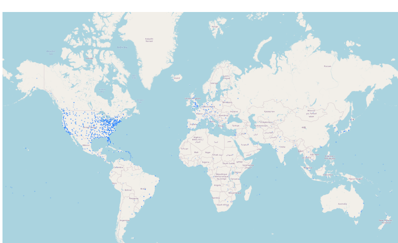


(c) IPv4 - Countries

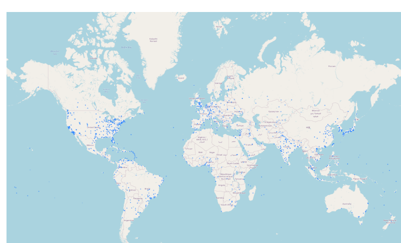


(d) IPv6 - Countries

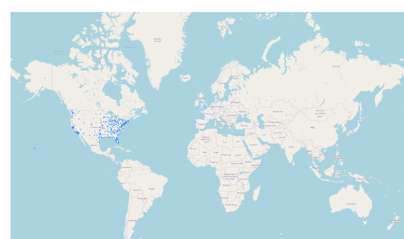
Figure 4: Distribution of subnet locations across countries and cities per egress operator AS.



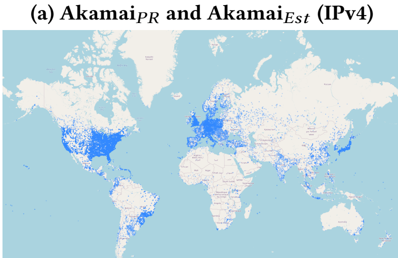
(a) Akamai$_{PR}$ and Akamai$_{Est}$ (IPv4)



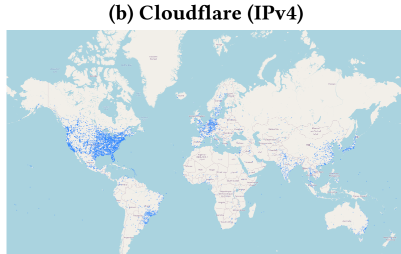
(b) Cloudflare (IPv4)



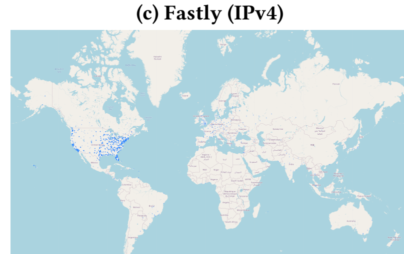
(c) Fastly (IPv4)



(d) Akamai$_{PR}$ and Akamai$_{Est}$ (IPv6)



(e) Cloudflare (IPv6)



(f) Fastly (IPv6)

Figure 5: Geolocation of egress subnets per providing AS as published by Apple [15][2].