

Internet Localization of Multi-Party Relay Users: Inherent Friction Between Internet Services and User Privacy

Sean Flynn

University of Hawai‘i at Mānoa

Francesco Bronzino

École Normale Supérieure de Lyon

Paul Schmitt

University of Hawai‘i at Mānoa

ABSTRACT

Internet privacy is increasingly important on the modern Internet. Users are looking to control the trail of data that they leave behind on the systems that they interact with. Multi-Party Relay (MPR) architectures lower the traditional barriers to adoption of privacy enhancing technologies on the Internet. MPRs are unique from legacy architectures in that they are able to offer privacy guarantees without paying significant performance penalties. Apple’s iCloud Private Relay is a recently deployed MPR service, creating the potential for widespread consumer adoption of the architecture. However, many current Internet-scale systems are designed based on assumptions that may no longer hold for users of privacy enhancing systems like Private Relay. There are inherent tensions between systems that rely on data about users—estimated location of a user based on their IP address, for example—and the trend towards a more private Internet.

This work studies a core function that is widely used to control network and application behavior, IP geolocation, in the context of iCloud Private Relay usage. We study the location accuracy of popular IP geolocation services compared against the published location dataset that Apple publicly releases to explicitly aid in geolocating PR users. We characterize geolocation service performance across a number of dimensions, including different countries, IP version, infrastructure provider, and time. Our findings lead us to conclude that existing approaches to IP geolocation (e.g., frequently updated databases) perform inadequately for users of the MPR architecture. For example, we find median location errors >1,000 miles in some countries for IPv4 addresses using IP2Location. Our findings lead us to conclude that new, privacy-focused, techniques for inferring user location may be required as privacy becomes a default user expectation on the Internet.

1 INTRODUCTION

Nearly everything we do on the Internet leaves a trace, and in recent decades the value of user data has proven to be highly-profitable and become a fundamental business strategy of the Internet [46, 59]. The only recourse users have for this situation is through increased privacy, and it has long been understood that privacy is not solely a benefit for individuals, but also aids society as a whole [16, 33, 35, 44, 45, 47]. It stands

to reason, then, that improving Internet privacy is a critical need, yet it is uniquely difficult on the Internet because we must rely on others to carry and serve our traffic.

The networking and security communities have long recognized the importance of privacy, and have been designing solutions across the network stack for decades. Beyond confidentiality (*i.e.*, TLS encryption), which has thankfully been largely solved, privacy research has focused on unlinkability between user identifiers and their traffic. For example, even with encrypted payloads, the IP endpoints of TCP sessions can be used to infer “who is talking to whom.” Chaum’s foundational mixnet work introduced the first architecture for anonymous communication over the Internet [8]. Syverson *et al.* furthered the mixnet concept and attempted to balance privacy and performance with Onion Routing [54] and eventually Tor [53]. While these systems have been widely available for decades, their adoption has largely been limited to a small fraction of total Internet users [55]. One potential reason for limited adoption has been relatively poor and/or unpredictable performance [12, 52].

Modern systems have sought to enhance user privacy without sacrificing performance by leveraging the Multi-Party Relay architecture [44]. Apple’s iCloud Private Relay (PR) is a prime example of an MPR service. PR, currently in public beta [2], was introduced by Apple in 2021 and the service is available to iCloud subscribers. In PR, users pass through a first hop relay that is operated by Apple and a second hop relay that is operated by one of Apple’s infrastructure partners (Akamai, Cloudflare, and Fastly) before egressing onto the open Internet. Using the MPR architecture, Private Relay masks user IP addresses from Internet hosts (as well as the second hop relay), while minimizing latency penalties due to the addition of multiple middleboxes. In some ways, PR is similar to a VPN but it offers improved privacy guarantees as VPN users must trust the VPN provider, who is able to see both the user’s identity and their traffic. In contrast, the PR architecture ensures that neither Apple nor their partners have access to both the user’s identity and their traffic. The integration of PR into Apple’s platforms lowers the barriers to widespread adoption of privacy-enhancing architectures, and has the opportunity to influence future privacy-focused Internet systems.

The trend towards privacy brings inherent tensions with the practice of leveraging information about the user to tailor network behavior—a common example of this being IP geolocation. IP geolocation is a long-studied networking problem as mapping IP addresses to location has many uses, including routing client traffic to “nearby” CDN infrastructure, language localization, and restricting content based on geography (e.g., live sports or other licensed streaming content). Additionally, governments use geolocation data for emergency planning, taxation, and regulation. IP geolocation is a fundamental component of the modern Internet, yet it may be imperiled by the (justifiable) trend towards enhanced user privacy. As users are decreasingly identifiable on the open Internet, how will existing services perform? In this work, we study the performance of popular IP geolocation services in the context of Apple’s iCloud Private Relay – a popular consumer MPR service.

We conduct a measurement campaign to investigate the accuracy of popular IP geolocation services with regard to Private Relay. PR is a unique service in that it seeks to provide a specific dimension of privacy (*i.e.*, masking user IP addresses) while maintaining the expected user experience while using the Internet. To accomplish this, Apple publishes fine-grained location information for all of the IP prefixes that PR users are assigned to while using the system. We compare geolocation service performance against the publicly available location information for PR IP prefixes over the course of a 5 month period. We analyze geolocation errors across a number of factors, including country, infrastructure partner, IP geolocation service, IP version, and time. We find that IP geolocation accuracy varies dramatically depending on these underlying factors, and that geolocation errors for Private Relay users can be up to thousands of miles.

Ultimately, our main goal in this work is not to solely focus on the accuracy performance of IP geolocation services for iCloud Private Relay users. Instead, we seek to shed an initial light on inherent tensions between the status quo of a core component (in this case localization) of the modern Internet and the trend of increased user privacy. Certainly, localization of Internet users is only one example of leveraging user metadata to personalize services, yet it provides a tractable dimension for measurement and reasoning about system performance as privacy is increased. Our findings lead us to conclude that existing solutions are not currently viable for MPR users in cases where highly accurate location information is required, and that fundamentally new designs will be needed to provide equivalent localization functionality for users of privacy-enhancing systems moving forward.

The rest of the paper is structured as follows: We first introduce PR and discuss the context of our research in Section 2. Section 3 describes our proposed method. In Section 4 we present the results of our study. We discuss the implication

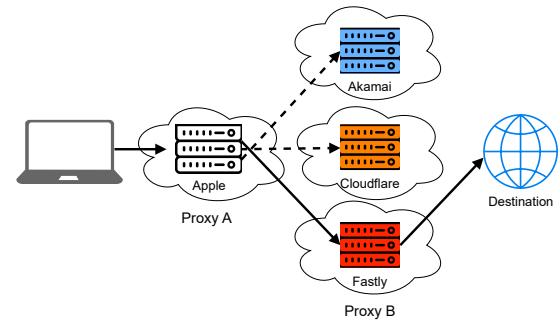


Figure 1: Private Relay Architecture

of our results in Section 5. Finally, we discuss related work and conclude our study in Sections 6 and 7 respectively.

2 BACKGROUND

In this section we provide a brief overview of the iCloud Private Relay architecture. Further, we discuss the role of IP geolocation in the modern Internet and the inherent challenges of providing geolocation over privacy focused architectures.

2.1 Apple iCloud Private Relay

Private Relay (PR) aims to provide network-layer identifier (IP address) privacy of its users by routing their Internet traffic through a Multi-Party Relay architecture. Figure 1 shows a basic overview of the PR design. With PR, the user’s IP address is known to the first proxy (Proxy A in Figure 1), operated by Apple, but their traffic is not known as it is encapsulated within an encrypted stream. The second proxy (Proxy B in Figure 1), operated by one of Apple’s infrastructure partners (Cloudflare, Fastly, and Akamai), is unable to “see” the user’s IP address, rather it only sees the IP address of the first proxy. However, the second proxy may learn information about the user’s request, such as the FQDN of the origin server. Lastly, the origin server only learns the user’s request and sees traffic originating from the second proxy IP address. PR is available to all Apple device users who have a subscription to iCloud+. Apple has incorporated PR into its operating systems such as iOS, iPadOS, and macOS [24].

The PR architecture is similar in spirit to classic systems such as Chaum’s mixnets [8] or Tor [11], but differs in two ways. First, it utilizes well-known rather than specialized protocols. The default protocol for communication between the client and Proxy A is QUIC, but if there are issues with QUIC setup, HTTP/2 and TLS is used as a fallback. When communicating with Proxy B, HTTP/3 and Multiplexed Application Substrate over QUIC Encryption (MASQUE) [41, 42] are used. If HTTP/3 is not available, the traditional HTTP CONNECT protocol over TLS is used for communication

with the second proxy [56]. Second, PR is operated on commercial infrastructure rather than volunteer-run nodes and includes functionality designed to maximize performance. For example, Cloudflare utilizes Argo [31], a virtual network infrastructure designed to optimize routing to minimize disruptions caused by congestion [32]. These strategies of the CDN egress providers help to mitigate performance issues caused by introducing the additional network hops necessary for an MPR architecture [40].

2.2 IP Geolocation

IP geolocation involves solving the problem of mapping the geographic location of a given IP address. Many applications can benefit from using IP geolocation to determine the geographic location of hosts on the Internet. For example, online advertisers and search engines tailor their content based on the client’s location. Content providers can use IP geolocation to enforce digital rights management policies and prevent users from accessing content that is not licensed for their geographic location. In recent years, IP geolocation has become increasingly relevant as Internet services aim to deploy low latency applications such as cloud based online gaming and augmented reality.

Depending on the different use cases listed above, IP geolocation services can be delivered with different degrees of granularity, varying from country level localization down to city level. There exist two main approaches to geolocation based on different techniques they employ: either relying on active network measurements to determine the location of the host associated to the target IP address or by querying an IP to geolocation mapping database. In this paper we focus on the latter which is the common solution provided by commercial IP geolocation services.

Typically, a geolocation database entry is composed of a pair of values, corresponding to the integer representation of the minimum and maximum address of an IP address block. Each block is then associated with several pieces of information helpful for localization: country code, city, latitude and longitude, and Zip code. There exist two classes of commercial databases: freely accessible databases (e.g., MaxMind GeoLite2 City [34], IP2Location LITE [25]) and subscription based services (e.g., ipstack [26]). Free services are often advertised as slightly less accurate than their paid counterparts.

2.3 Challenges of IP Geolocation over Private Relay

Any platform that aims to provide IP address privacy impacts the ability to map a user’s IP address to a geographic location. PR is unique in that it attempts to find a balance between

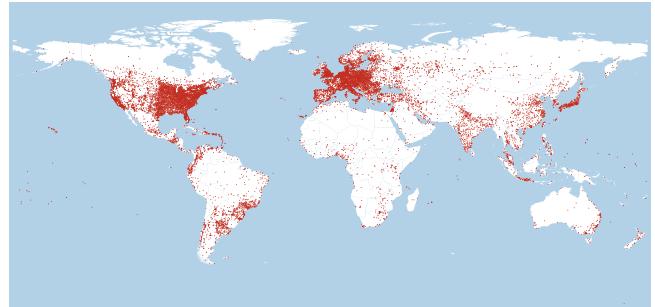


Figure 2: Advertised Apple iCloud Private Relay egress locations (red).

user privacy and user experience. Unlike VPNs, which, in addition to masking user IP addresses are often used to provide a means to access geographically filtered content¹ [29], PR is solely focused on masking users’ IP addresses and it explicitly does not attempt to provide these other functionalities. PR includes functionality in which Proxy A establishes the client’s location using traditional IP geolocation and then provides a geohash to the client, which is subsequently offered to Proxy B in order to map to a Proxy B IP address that is geographically near the client.

Apple and its infrastructure partners regularly publish Proxy B IP addresses and their locations [3] in order to inform external services—*i.e.*, IP geolocation services—of “accurate” PR user locations while maintaining their IP address privacy. Proxy B egress IP prefixes are advertised to be in locations across a wide geographic footprint, as shown in Figure 2, allowing for web services to localize PR users with relatively fine-grained accuracy. Interestingly, the end result of the PR design is that advertised egress IP address locations are, in many cases, obviously false. For example, the egress IP dataset includes prefixes that are advertised to be hosted in North Korea, even though we find no evidence of any of the three infrastructure partners operating in North Korea. In a less extreme example, thousands of IP prefixes are advertised in rural areas across the world.

The focus of this work is to understand the interaction between these published IPs and their locations versus the performance of popular IP geolocation services to anticipate potential localization issues in reality.

3 METHODOLOGY

In this section, we outline our data collection methodology. We then describe the analysis we conduct and inherent limitations.

¹VPNs are also commonly used to circumvent Internet censorship. We could find no documentation that PR looks to provide censorship benefits [1].

| CDN | IPv4 | | | | IPv6 | | | | Total |
|------------|--------|-----|-----|-----|---------|-------|-------|-----|---------|
| | US | FR | AU | ZA | US | FR | AU | ZA | |
| Akamai | 28,816 | 480 | 594 | 130 | 267,846 | 6,720 | 1,398 | 812 | 306,796 |
| Cloudflare | 6,030 | 401 | 290 | 103 | 46,684 | 1,796 | 1,240 | 172 | 56,716 |
| Fastly | 11,526 | 110 | 72 | 8 | 11,526 | 110 | 72 | 8 | 23,432 |
| Total | 46,372 | 991 | 956 | 241 | 326,056 | 8,626 | 2,710 | 992 | |

Table 1: Measured Private Relay Egress IPs by CDN and country on May 31, 2023.

3.1 PR egress IPs and locations

We establish ground truth using the egress (*i.e.*, Proxy B in Figure 1) IP address information provided by Apple for the iCloud Private Relay service [3]. The published file is a CSV that includes fields for IP block, city, state (or region), and country. This dataset is publicly released and periodically updated in order to allow for IP geolocation services and or web services to associate Private Relay IP addresses to the locations intended by Apple and their infrastructure partners. To assess the evolution of PR egress IPs over time we download the file daily from January 1, 2023 through May 31, 2023.

Geographic ground truth. As mentioned in Section 2.1, geographic “ground truth” is a somewhat misleading term in Private Relay. In this work we assign ground truth to the location that Apple and its infrastructure partners attest to, we do not attempt to verify each location. We use Nominatim [36], an open source geocoding tool based on OpenStreetMap, to establish baseline geographic coordinates for each advertised egress location (*i.e.*, geographic coordinates for the center of a city listed in the published egress file). Note that while each line in the file has fields for city, region, and country, not all records are complete. Additionally, many locations in the file are listed under multiple strings (*e.g.*, Ciudad Juarez and Juarez, Mexico), resulting in an artificially inflated number of unique locations. Overall, we observe a total of 18,110 unique location names in the dataset. Figure 2 shows a map with the egress locations around the world. For brevity, we focus our analysis on four countries: the United States, France, Australia, and South Africa. We choose these countries as they represent a range of deployment and coverage density, as shown in Table 1.

IP address ground truth. We extract individual IP addresses out of their IP blocks differently depending on the IP type. For IPv4 addresses, we include every individual address in our measurements. Conversely, the IPv6 address prefixes in the dataset are typically listed as /45 or /64 blocks, which include an infeasible number of individual IPs to measure. Therefore, for each IPv6 prefix, we simply extract the first two IP addresses for measurement purposes. We ran small

experiments to test whether random selection or larger numbers of IPv6 addresses would affect results, but we observed no difference in performance. We also assign IPs to the respective infrastructure partner by performing autonomous system whois lookups for each prefix.

Table 1 shows PR egress IP addresses categorized by autonomous system and IP version for each of Apple’s three infrastructure partners on a single day. As shown, Akamai offers the largest number of both IPv4 and IPv6 address blocks, followed by Cloudflare and Fastly, respectively.

3.2 Analyses

IP Geolocation services. We use three popular IP geolocation services to compare computed locations based on IP address versus the published ground truth dataset. The services we use are MaxMind GeoLite2 City [34], IP2Location LITE [25], and ipstack [26]. The MaxMind and IP2Location services are commonly used free services, while ipstack is a commercial API. Each of the services outputs the geographic coordinates associated with an IP address at the city level. Web services commonly use geolocation services to tailor (or often restrict) content based on a user’s location. We choose the city-level services as many streaming services (*e.g.*, live sports) require localizing users at a level finer than country-level.

To understand temporal performance of the service, we explore MaxMind’s performance over time (Section 4.3.3) by downloading every release of the MaxMind database during the measurement campaign. MaxMind publicly releases the database twice per week, and we download versions from December 30, 2022 through May 30, 2023.

Geographic error. For each IP address, we calculate the distance between the ground truth coordinates and the geolocated coordinates from each service, allowing us to reason about how web services would localize users connecting from PR egress IP addresses, and whether those locations match locations from which Apple intends them to appear.

Limitations. Our study is necessarily limited to the IP geolocation services that we have selected. Certainly, other geolocation services may perform better or worse compared

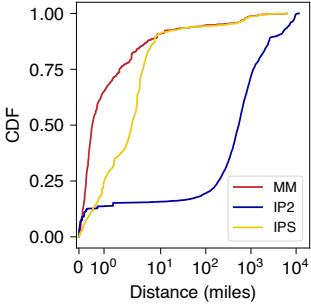


Figure 3: US IPv4

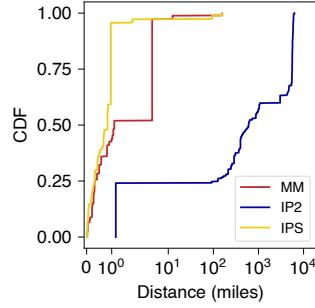


Figure 4: FR IPv4

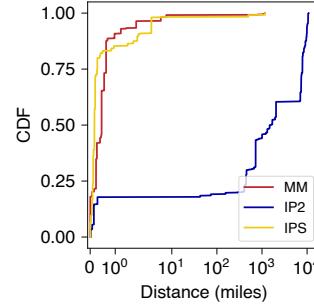


Figure 5: AU IPv4

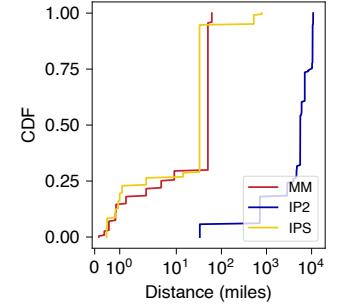


Figure 6: ZA IPv4

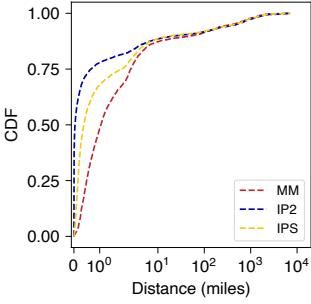


Figure 7: US IPv6

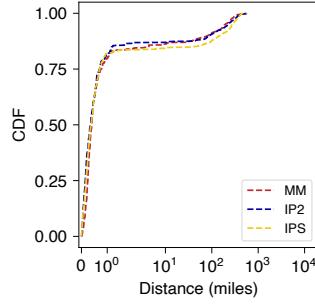


Figure 8: FR IPv6

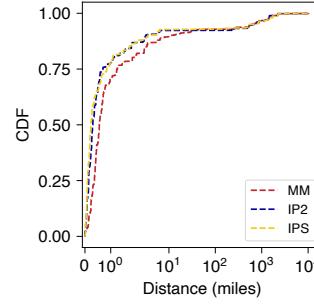


Figure 9: AU IPv6

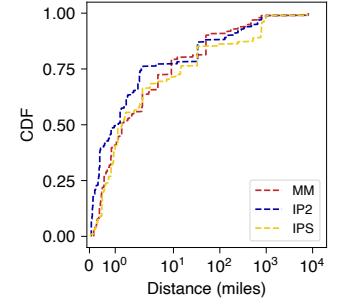


Figure 10: ZA IPv6

with those studied. As this study is meant to shine a light on potential web localization issues that could arise from privacy-preserving system architectures, we leave in-depth, service-by-service exploration for future work. We also do not study the relationship between the actual location of PR users and the egress locations they are assigned to as this is proprietary information. For simplicity, we assume the general use case of PR is that users are assigned egress IPs and locations that are geographically closest to their actual locations.

4 RESULTS

In this section we analyze IP geolocation services with respect to PR across a number of dimensions, including country, IP version, IP geolocation service, PR infrastructure partner, and time.

4.1 Country-wide IP geolocation service performance

We begin by studying IP geolocation service accuracy for each country in our dataset. For this experiment, we choose a single day (March 15, 2023) to calculate geographic distance between the advertised PR egress IP locations and the geolocated coordinates. Figures 3 to 10 display the results for IPv4 and IPv6 for each country and for each service (MaxMind

is labeled ‘MM’, IP2Location is labeled ‘IP2’, and ipstack is labeled ‘IPS’).

For IPv4 addresses, we observe that IP2Location (IP2) tends to perform worst among the geolocation services across all of the countries studied, oftentimes showing distance errors 5,000 - 10,000 miles larger than the other two services. For every country, IP2 performs relatively well for a small percentage of the IPv4 addresses; for example, roughly 20% of Australian IPv4 errors are less than 1 mile. However, the median distance error for IP2 in Australia is 1,479 miles. The other two services (MM and IPS) result in significantly lower distance errors on the whole, with neither service performing particularly better than the other. When looking from a country-wide perspective, we observe the highest accuracy in Australia for MM and IPS, with both services showing >90% of distance errors less than 10 miles. We posit that Australia may benefit from the nature of its population concentration in relatively few areas along the coasts, whereas the populations of the other countries studied are more evenly spread geographically. Australia’s dense urban areas offer more obvious locations for CDNs to install infrastructure, in comparison. The United States and France both also show results that would appear acceptable for MM and IPS, with median errors of less than 2 miles for the services in both countries. As one might anticipate, South Africa, the country with the least dense PR deployment (Table 1), has

the highest median errors for all three services (50, 5,592, and 33 miles for MM, IP2, and IPS, respectively).

Interestingly, IPv6 results (Figures 7 to 10) differ significantly compared to IPv4 addresses. We see that all geolocation services tend to perform similarly for each country. IP2Location, the worst performing service for IPv4 addresses, shows the highest accuracy for the United States and South Africa, and comparative accuracy for France and Australia. Additionally, IPv6 distance error distributions tend to be dominated by highly accurate measurements (*i.e.*, less than 10 miles) with a long tail reaching thousands of miles. Overall, our results indicate that PR users that are given IPv6 addresses are more likely to be accurately geolocated compared to users assigned to IPv4 PR addresses.

4.1.1 IPv6 distribution similarity. As shown in Figures 3 to 6, the error distributions for the IP geolocation services can differ widely for IPv4 egress addresses. However, we notice that the error distributions for IPv6 addresses qualitatively appear similar for many of the countries (Figures 7 to 10). To explore this quantitatively, we perform one-way ANOVA analysis to discover whether the error distributions are statistically similar. The output of one-way ANOVA is a p-value, which can be understood to indicate whether the differences in the means of multiple distributions are statistically significant. If the p-value is less than or equal to 0.05 we reject the null hypothesis that states that the means are equal. Higher p-values suggest that we do not have sufficient evidence to reject the null hypothesis, and that the distribution means could be equal. Table 2 shows the results. We see that the p-value for all countries is far below 0.05 for IPv4, meaning we reject the null hypothesis. Conversely, we observe significantly higher p-values for IPv6 and both Australia and South Africa, meaning the three error distributions could be considered similar.

| One-way ANOVA p-value | | |
|-----------------------|-----------|----------|
| Country | IPv4 | IPv6 |
| US | 0.0 | 1.28e-58 |
| FR | 3.06e-251 | 6.41e-27 |
| AU | 4.47e-290 | 0.967 |
| ZA | 2.41e-159 | 0.155 |

Table 2: One-way ANOVA results. IPv6 error distributions in some countries could be argued to be similar (p-value >0.05) across geolocation services, while IPv4 error distributions are not similar (p-value <0.05).

The precise reason for these results is unclear. We posit that the IP geolocation services may have added new IPv6 entries as a direct result of Apple publicly releasing the ground

truth egress location dataset - meaning all of the services would be working from the same, relatively recent starting point. Conversely, all or nearly all IPv4 addresses have been present in IP geolocation databases for several years and could have changed ownership or location—particularly IP addresses associated with public cloud infrastructure can be “moved” readily. Unfortunately, the IP geolocation services that we leverage in this work do not publish historical information about IPs in their databases. Further investigation into the discrepancy in performance between IPv4 and IPv6 addresses is left to future work.

4.1.2 Characterizing large errors. We look to further understand extremely large distance errors that we encounter when processing the dataset. For each record in the countries we study with a distance error >1,000 miles, we compare the ground truth country information versus the geolocated country along with the infrastructure partner that owns the IP prefix.

We find that behavior varies between different combinations of geolocation service, infrastructure, and country. MaxMind returns the correct country for all large errors in both Australia and South Africa, but returns a number of different (incorrect) countries for IP prefixes in France and the United States. For French IP prefixes that are operated by Fastly, MaxMind geolocates to Belgium, and, more interestingly, some in Uruguay. Conversely, French prefixes operated by Akamai are geolocated to France. MaxMind is most interesting in the United States—while the vast majority of large geolocation errors are geolocated within the United States, a small fraction return locations in 32 different countries, including India and Guatemala for Fastly-owned prefixes, and Afghanistan for Akamai-owned prefixes. Notably, we find that >1,000 mile errors for MaxMind do not occur for Cloudflare prefixes in any country outside of Australia.

IP2Location, generally the least accurate geolocation service, expectedly results in quite different behavior for large errors. In Australia, the majority (89.9%) of >1,000 mile errors are associated with Cloudflare IP prefixes. Akamai prefixes never result in large errors, while Fastly accounts for ~10%. Australian prefixes are most commonly geolocated to the United States for Cloudflare, and to Sweden for Fastly IPs when using IP2Location. South Africa and France demonstrate roughly similar behavior, with erroneous Cloudflare prefixes most commonly associated to the United States and Fastly prefixes to Sweden. This behavior appears to be explained by whois information associated with the prefixes owned by the infrastructure partners. A large number of prefixes owned by Fastly are registered as being located in Sweden, while Cloudflare’s prefixes are associated with their headquarters in the United States. We believe that IP2Location may fall back to basic whois information for

an IP address if the database does not include more specific location information for the associated IP prefix.

Large errors with IP2Location in the United States provide perhaps the most interesting results. For example, a large number of errors for prefixes owned by Akamai are geolocated to Australia. Fastly prefixes are again most often erroneously mapped to Sweden, but they are additionally geolocated to Cyprus and Macau. Cloudflare prefixes are geolocated to Japan and Great Britain. Overall, we observe no discernable pattern when investigating large geolocation errors for IP prefixes that are meant to be located in the United States. We believe additional study into the nature of geolocation errors for core Internet infrastructure IP addresses (*i.e.*, rather than residential or edge addresses) is warranted and we leave this for future work.

4.1.3 False ground truth locations. As mentioned in Section 2.1, the ground truth dataset advertises many locations where there is almost certainly no partner cloud infrastructure deployed. One example of this is North Korea. The May 31, 2023 egress dataset advertises 39 IP prefixes located in North Korea: 24 IPv4 prefixes and 15 IPv6 prefixes. The prefixes are hosted by Akamai and Cloudflare, and we find no evidence of Akamai or Cloudflare deployments in North Korea.

We attempt to geolocate North Korean IP addresses in each of the prefixes using all three services. Table 3 shows the country codes returned by each of the services for IPv4 addresses. As shown, both MaxMind and ipstack, the more accurate services in our prior analysis, report North Korea for all of the IP addresses. IP2Location, on the other hand, never reports North Korea as the country and instead often reports Japan as the location. We attempt to verify the actual location of the IP addresses using looking glass servers located around the world. We find evidence that many of the IP addresses are in fact hosted on infrastructure in Japan (*i.e.*, ping RTTs of ~1-2ms from looking glass servers located in Japan).

| | Country | | | |
|-------------|---------|----|----|----|
| | KP | JP | TW | US |
| MaxMind | 24 | 0 | 0 | 0 |
| IP2Location | 0 | 18 | 1 | 5 |
| IP Stack | 24 | 0 | 0 | 0 |

Table 3: IPv4 country locations for IP prefixes advertised as within North Korea (KP).

Conversely, all three of the geolocation services report North Korea as the country for every IPv6 address in the dataset. This result furthers the notion that IP version has a dramatic impact on geolocation accuracy when using PR. As

seen in Figures 7 to 10, IPv6 errors tend to be similar across all geolocation services.

These results beg the question: what is geolocation “accuracy” for a system that purposefully falsifies location information of its users? One could argue that closely matching Apple’s advertised location is the ideal outcome for web services (*e.g.*, the behavior of MaxMind and ipstack, in this case). Of course, this assumes that PR users are mapped to the geographically closest egress IP addresses when using the system. Alternatively, one could argue that IP2Location is the more accurate service for these IP addresses, as it is more accurately characterizing the locations in which user traffic actually ingresses and egresses from the Internet. While this discussion is beyond the scope of a measurement campaign, we briefly discuss the overall goals of IP geolocation in Section 5.

4.2 Infrastructure partner IP geolocation service performance

Next, we investigate IPv4 geolocation service performance with respect to the different infrastructure partners that operate PR egress infrastructure (Akamai, Cloudflare, and Fastly). For brevity, and given that we found MaxMind and ipstack to perform similarly in Section 4.1, we only focus on results using MaxMind (MM) and IP2Location (IP2). We again calculate the geographic error distance between the Apple published egress ground truth locations and the geolocated coordinates, only we now categorize based on the partner AS that owns the IPs in question. Figures 11 to 14 show the results for MaxMind and Figures 15 to 18 show the results for IP2Location.

We find that it appears as though different combinations of infrastructure partner and IP geolocation service matters greatly in terms of accuracy. For instance, Akamai IP addresses tend to be geolocated with the highest accuracy when using IP2, but the same cannot be said for MM, with Akamai IP addresses often resulting in the worst or nearly the worst accuracy. Curiously, both Akamai and Fastly South African IP addresses result in consistent values when using MaxMind. We investigate and find that they each repeatedly geolocate to static locations and their corresponding ground truth locations are similar. For instance, MaxMind ground truth IPv4 addresses are located in Pretoria, while the geolocated coordinates are south of Johannesburg, 50.2 miles away.

We are unsure as to why there are significant localization performance gaps depending on the infrastructure partner and IP geolocation service, given that the ground truth location information is kept up to date and published by Apple in a single file for all partners combined. We posit that the differences we witness could be historical artifacts based

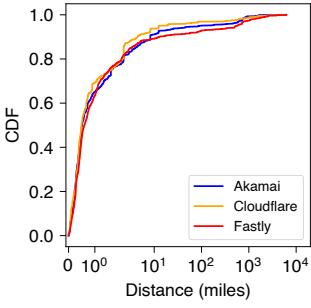


Figure 11: MM US

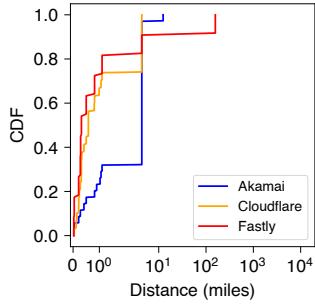


Figure 12: MM FR

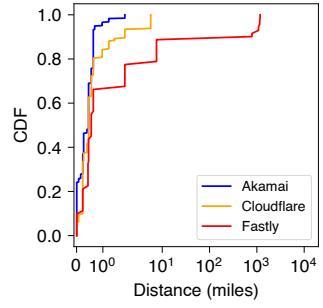


Figure 13: MM AU

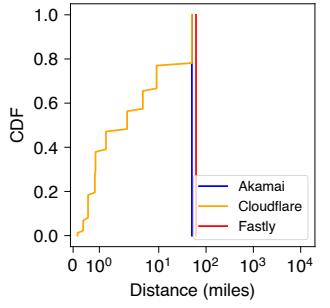


Figure 14: MM ZA

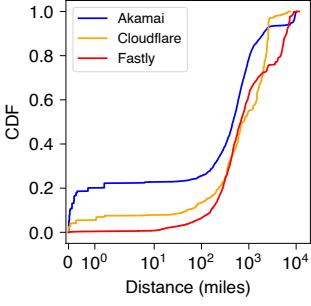


Figure 15: IP2 US

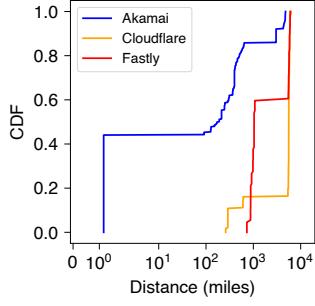


Figure 16: IP2 FR

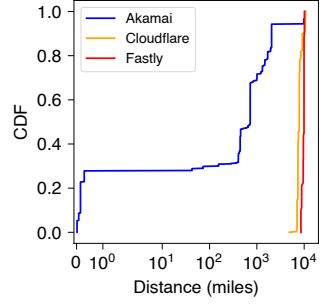


Figure 17: IP2 AU

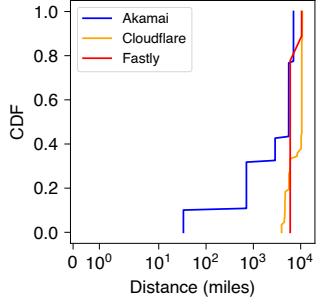


Figure 18: IP2 ZA

on IP re-use practices of the partners themselves or on the ground truth IP location ingestion practices of the geolocation services (*e.g.*, how each service manages partially complete records in the ground truth dataset).

This analysis shows us that the combination of PR infrastructure partner and the IP geolocation service used to locate a given user can have a significant impact on the ability to accurately localize a user. Unfortunately, the method used to map users to egress IPs (and thus to infrastructure partners) is not public information. Likewise, the vast majority of services on the Internet that use IP geolocation service do not advertise which service(s) that they subscribe to. Ultimately, this means that users have little predictive control over localization of themselves when using PR to connect to Internet services. This result, along with the scale of the error for some of the services (*e.g.*, medians of 1,479 miles and 5,592 miles for IP2 in Australia and South Africa, respectively), lead us to conclude that geolocation outcomes for users of systems like Private Relay are non-deterministic as of today.

4.3 Temporal evolution of Private Relay egress IPs and geolocation services

Next, we investigate the published egress IP and location dataset to understand its evolution over time. Our intuition is that a high churn rate of IP prefixes or locations could

negatively impact the accuracy of IP geolocation services. For brevity, we limit geolocation accuracy results to MaxMind, the best-performing geolocation service provider, for the remainder of this paper. We then study the accuracy performance of MaxMind over time as the database is updated to reflect changes in the PR egress dataset.

4.3.1 Stability of egress IP addresses over time. We first analyze the published egress dataset to highlight changes that occur over the course of the observation period. As Private Relay is a relatively new service, it stands to reason that the egress dataset is evolving over time. Further, we anticipate that major changes to the dataset could negatively effect the accuracy of IP geolocation services when locating PR egress IP addresses, as lag time in database updates would manifest in location errors.

IP address space. Figure 19 shows the measured IP addresses in the four countries we study during the observation period categorized by infrastructure partner and IP version. We see that in the beginning of the measurement campaign, a large number of IPv6 addresses owned by Cloudflare were advertised and subsequently removed before another short-lived increase roughly one week later. The other infrastructure partners tend to advertise a more stable number of IP addresses throughout the study. Akamai offers significantly

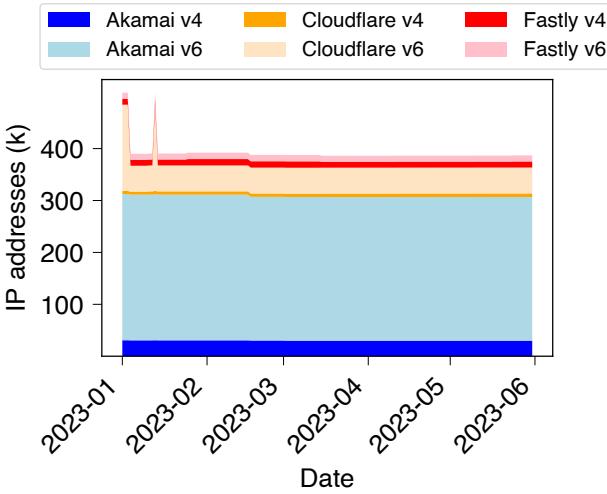


Figure 19: Measurable egress IP addresses advertised over time.

more addresses than Cloudflare or Fastly throughout. Overall, the total count of IP addresses does not drastically change over the course of the observation period. It would logically follow that short-lived IP addresses such as those offered by Cloudflare in the beginning of the study could potentially experience poor geolocation accuracy due to lag between the IP addresses being newly advertised as part of the PR egress service and geolocation services updating their databases. We explore this further in Section 4.3.3.

Added, split, and merged IP prefixes. While the total count of measurable IP addresses remains relatively stable in the observed countries, further exploration reveals that the egress IP prefixes evolve more subtly. We find that a significant number of IP prefixes are added during the measurement campaign. Over the duration of our observation, we find a total of 10,131 new IP prefixes were added representing 19,663 measurable IP addresses - roughly equivalent to 5% of the total IP address space. This result is unintuitive given the stability shown in Figure 19, but can be explained by observing aggregation and disaggregation of IP prefixes into different sized CIDR blocks. We observe many instances of IP prefixes being split (*i.e.*, disaggregated into smaller CIDR blocks) and merged (*i.e.*, aggregated into larger CIDR blocks) over time.

Over the duration of our observation, 132,377 prefixes were split, and 23,713 prefixes were merged. We measure the accuracy performance of MaxMind for added, merged, and split IP prefix and plot the results in Figure 20. As shown, newly added IP addresses tend to result in lower geolocation accuracy compared with addresses belonging to split

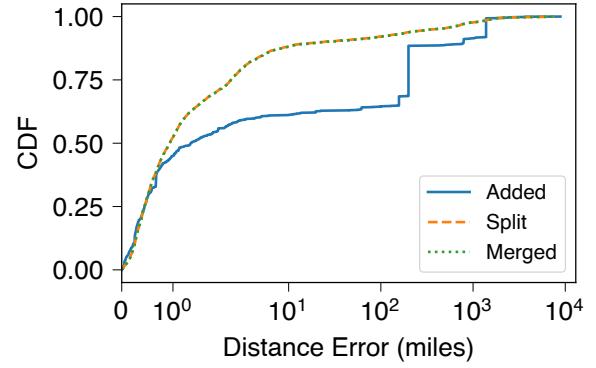


Figure 20: Added IP prefixes

or merged IP prefixes. We also see that split and merged IP prefixes result in nearly identical error distributions. We find that split and merged prefixes were all owned by Cloudflare, and we believe this accuracy performance could be attributable to split or merged prefixes not changing location at the time of a change, resulting in no change in geolocation accuracy.

4.3.2 Stability of egress geographic locations over time. In addition to newly added, split, and merged IP prefixes in the dataset, we also observe a small number of prefixes whose location is changed in the ground truth egress dataset. In this analysis we include all moved IP prefixes, not limited to the four countries presented previously. We include worldwide moves to illustrate the large changes that are present in the dataset.

For qualitative purposes, we plot the movement of IP prefixes in the egress dataset in Figure 21. The color of the arcs in the figure indicate the CDN that owns the prefix: Akamai moves are blue, Fastly are red, Cloudflare did not move any prefixes during the study. The arcs also indicate direction of the move as they can be followed clockwise, for instance, a large number of Fastly prefixes moved from the west coast of the United States to Florida. We see that prefixes associated with Fastly are most commonly moved, with Akamai limited to relatively few. We also see that moves are not constrained to small geographic distances, rather they are commonly moved thousands of miles. The median change is 2,553.9 miles, 25th percentile is 605.8, and 75th percentile is 5,599.4 miles. Further, prefix moves are not limited to within a single country. This map illustrates the dramatic geographic changes to the ground truth dataset, changes that IP geolocation services must quickly respond to by updating their databases.



Figure 21: IP prefixes that moved during the observation period. Arcs indicate direction of the move (clockwise). Color indicates infrastructure partner: Akamai in blue, Fastly in red, Cloudflare did not have any moved IP prefixes.

While IP prefixes can and do change location or ownership between autonomous systems in all networks including residential or mobile ISPs along with cloud providers, we believe the nature and goals of Private Relay presents a uniquely difficult challenge for IP geolocation. Cloud infrastructure is characterized by its flexibility and dynamism—cloud IPs and services are ephemeral by their nature and can be brought online or offline in minutes. This paradigm, which is a fundamental reason for the dominance of cloud infrastructure, can be detrimental for services that perform best for relatively static information such as IP geolocation services. Overall, the results show that IP geolocation services are facing a new and difficult challenge for Private Relay users: accurately locating end users using the lens of cloud infrastructure IPs, which can undergo unpredictable changes.

4.3.3 IP geolocation service evolution. Instability in the advertised egress IP information has a direct effect on IP geolocation service accuracy, as any lag in the database update process could result in inaccurate results for some time. We can leverage our dataset to discover geolocation service updates over time with respect to newly added IPs to the system. We parse the duration of the egress IP dataset to identify IP prefixes that were added during the measurement campaign.

To explore the evolution of geolocation service accuracy over time, we only select newly added IP prefixes that remained in the dataset for at least 30 days and were advertised to be in a single location throughout, resulting in a total of 7,405 prefixes. We plot geolocation error CDFs for MaxMind in Figure 22. We plot error distributions for added IP prefixes at day 0, 7 and 30. As shown, the poorest accuracy tends to occur for prefixes on day zero when they first appear in the egress dataset. This result can be expected, as the MaxMind database is updated twice per week and newly added IPs may not have been previously present in the database or could be associated with erroneous past geographic information

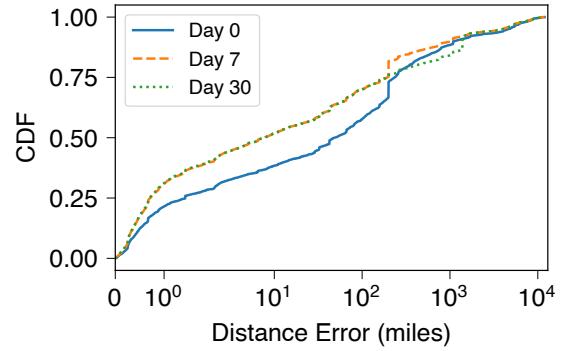


Figure 22: MaxMind geolocation accuracy for newly advertised IP addresses over time.

until MaxMind has the chance to update its database. As expected, we see on day 7 the accuracy is improved over the day zero case, with a median value of 7.8 miles versus an initial median of 48.3. Interestingly, day 30 results largely match day 7, leading to the conclusion that MaxMind does not appear to refine its database beyond any early updates as new IPs are added to the PR service. Unexpectedly, we observe a small number of cases where day 30 is less accurate than day 7. We are unable to explain this result. Overall, it appears that users of Private Relay can expect slightly poorer IP geolocation as geolocation services update their databases based on new information. We also observe that the overall distribution for newly added prefixes is rather broad, with a significant portion (e.g., 25%) resulting in distance errors greater than 190 miles.

5 DISCUSSION

Multi-party relay architectures like Apple’s PR are designed to achieve a compromise between performance and privacy. However, while doing so, PR renders IP geolocation services ineffective in determining the physical location of clients. The previous section sheds light on how IP geolocation services are affected by the use of MPR architectures like Apple’s iCloud Private Relay. In this section we discuss the implications of our findings and outline potential paths forward.

What is the role of IP geolocation in the modern Internet? IP geolocation is a key element of how the Internet functions today and its role is poised to increase in importance. As more applications aim to reduce latency to deploy real-time services, the ability to localize users at fine-grained levels could greatly impact the ability of such services to succeed. This raises questions on the fundamental role of IP geolocation moving forward. In the modern Internet, IP geolocation services serve, through a single tool, two main purposes:

mapping both clients and infrastructure to a physical location. This approach has inherent problems as the two use cases have different requirements. For example, the location of infrastructure is (most often) not a privacy concern, while the location of clients may be.

Overall, the concept of IP geolocation is inherently problematic when applied to user localization. A simple example of the problem is roaming in cellular networks, where users remain connected to a home gateway located in the country of origin while being physically in a different location. VPNs have abused this concept for years, allowing users to appear as if they were in a different country and inciting battles between content providers and VPNs [28]. Our results demonstrate that the adoption of multi-party relay architectures, such as PR, will only exacerbate the issue.

To combat this problem, we argue that we should fundamentally rethink how modern IP geolocation operates. We believe that to achieve both aforementioned applications—*i.e.*, infrastructure and users localization, we need to decouple the two to allow for different requirements and intents.

How to localize infrastructure? Identifying the location of infrastructure is a problem that has been studied for years (*e.g.*, [13, 18, 57]). The most common approach requires the use of active tools such as traceroute and ping to identify the location of a network interface. However, this approach is not always accurate as the last hop responding in a traceroute experiment may not be the closest to the target machine. In addition, traceroute is not always available, especially in the case of IPv6, meaning there is space for improvement.

To avoid relying on these techniques with PR, Apple opts to provide a hand-crafted map of the IP addresses belonging to the PR infrastructure to their nominal location. The results in the previous sections presented the issues of such approach: the hand-crafted map is not always complete and accurate and can easily generate inconsistencies with the results provided by commonly used IP geolocation services. The viability for this approach would be to exclusively rely on Apple (or any one central authority in an MPR architecture) for correctness and completeness, which raises questions in terms of trust.

We believe that the best course of action would be to improve on existing techniques and avoid relying on single organization to provide ground truth. While providing a solution to this problem is out of the scope of this paper, new promising techniques have emerged in recent years that could be leveraged to solve this problem. For example, concepts from Riemannian geometry have been recently proposed to compensate for probe inaccuracies in traceroute-based measurement techniques [39].

How to localize users without compromising their privacy? This study demonstrates that relying on IPs to identifies

users' location is becoming increasingly impractical, if not impossible. This raises the question of how to obtain information on a user location without compromising their privacy. While the solution to this problem could take many forms, for near-term deployability reasons we envision the development of a trusted third party architecture that could enable users to prove their location to services without revealing their identity. Such an architecture could be built around short-lived location tokens that could be used to prove a user's location through a consensus based approach across multiple parties. Of course, a number of practical challenges remain open in order to develop such an architecture. For example, how to verify client location? How to prevent abuse of the system? How to prevent a black market for location tokens? How to prevent a single party from being able to track a user's location?

6 RELATED WORK

Privacy-preserving Internet communications. Systems designed to provide anonymous communication have been studied for decades, with the first well known architecture being Chaum's mixnets [8], which introduced the concept of multi-hop relaying to provide anonymity. Mixnets provide multiple forms of privacy, including sender and receiver anonymity. The fundamental design of mixnets were later modified by Syverson *et al.* for use in real-time Internet communications in their work on Onion Routing [54], and subsequently improved in the Tor system [11]. All of these systems provide privacy through the technique of decoupling [44]. Many systems leverage decoupling to achieve anonymity for use cases beyond real-time communications. Chaum's blind signatures provide a means for anonymous access and authentication [6, 7], and were later adapted by Privacy Pass [9, 10]. Prior work has also directly studied Apple's iCloud Private Relay, focusing on infrastructure usage and separation of trust [40], Internet traffic performance [56], and resistance to traffic analysis attacks [58].

Privacy-preserving Internet naming. There has been prior work implementing privacy preservation in the global DNS system. Two prominent examples are DNS-over-TLS (DoT) and DNS-over-HTTPS (DoH) [21, 22]. In both cases, a client sends DNS queries to the resolver over an encrypted transport (TLS), which relies on the Transmission Control Protocol (TCP). ODNS [43] extends these designs by obfuscating users queries making it impossible for DNS resolver to match requests to a given user. EncDNS is functionally similar to ODNS [20]; however, EncDNS doesn't address key distribution. Most prior proposed DNS privacy mechanisms are protecting against an adversary, but not a DNS operator. Castillo-Perez and Garcia-Alfaro evaluate privacy-preserving DNS mechanisms, but show that they need additional measures to

enhance their security [5]. Similarly, Query Name Minimization is a proposal that limits what name servers see in DNS queries, but a recursive resolver’s operator still learns the domain requested and the corresponding client who requested the domain [4]. Researchers have also pointed out how aspects of current (operational) DNS, such as prefetching, have privacy implications [30, 50]. Federrath *et al.* introduced a DNS anonymity service that employs broadcasting popular hostnames and low-latency mixes for requesting less popular domains.

IP geolocation. Commercial IP geolocation services often are delivered via database, and many prior works have focused on studying the performance of these databases [14, 17, 38]. Siwpersad *et al.* [51] conducted a study to investigate the level of geographic accuracy of two geolocation services also studied in this work, MaxMind GeoLite [34] and Hexasoft (IP2Location) [25], measuring the distance between the locations provided by each service. Their findings showed that for 50% of the addresses, the difference in distance was less than 100km. Similarly, Huffaker checked the accuracy of geolocation services by comparing the database results to active measurements collected by PlanetLab nodes, discovering that 90% of the IP addresses provided by these services were different from the actual locations measured by the nodes [23]. Techniques beyond database have also been explored, often using network latency [19, 27].

In 2010, Shavitt *et al.* [48] performed research to evaluate the accuracy of several geolocation services using the DICES Project’s Points of Presence (PoP) level map. The authors used an algorithm, which is based on interface graphs, to assign IP addresses to PoPs on a map. They made the assumption that if IP addresses are in the same PoP, they should correspond to the same physical location on the map. The evaluation showed that MaxMind GeoIP, GeoBytes, and Digital Envoy had the highest accuracy in placing IP addresses within 1 km of a given PoP, with percentages ranging from 74% to 82%. HostIP had a somewhat lower accuracy of 57%. In a later study, Shavitt and Zilberman found distributions ranging from hundreds to thousands of kilometers [49]. Lastly, Poese *et al.* found median accuracies to fall between tens to hundreds of kilometers for MaxMind and IP2Location [38].

Most pertinent to this work, researchers have studied IP geolocation accuracy in the context of physical network infrastructure [37]. Lastly, others have studied assumptions based on co-location of IP prefixes [15, 17]. This work seeks to explore IP geolocation services in the specific use case where a provider is explicitly and publicly advertising “ground truth” location rather than making location of IPs hosted on large infrastructure providers somewhat ambiguous or up for interpretation.

7 CONCLUSION

IP geolocation is fundamental to how the Internet functions today. Many applications benefit from using IP geolocation to determine the geographic location of hosts on the Internet and optimize their service, from search engines to content providers. Multi-party relay architectures like Apple’s iCloud Private Relay (PR) are designed to achieve a good compromise between performance and privacy. However, PR adversely affects the capability of IP geolocation services to accurately determine the physical location of clients. In this study we explore the accuracy of IP geolocation services with regard to PR by comparing their location data with Apple’s data. We observe that median errors can differ by up to 1,000 miles for IPv4 addresses.

Our investigation has the goal to highlight the need for the networking community to rethink IP geolocalization from the ground up. Looking ahead, we believe that a new systems approaches will be required to enable applications to continue to rely on geographical information while simultaneously respecting the increased expectation of user privacy on the Internet. We believe that the networking community is best positioned to take the lead in this effort, and we hope that our work will serve as a starting point for new research directions that seek to balance user privacy and system performance.

REFERENCES

- [1] Anonymous, David Fifield, and Amir Houmansadr. 2021. *Evaluating the censorship resistance of Apple’s iCloud Private Relay*. https://gfw-report.blog/private_relay_censorship/en/
- [2] Apple. 2021. About iCloud Private Relay. <https://support.apple.com/en-us/HT212614>.
- [3] Apple. 2023. *Private Relay Egress IPs*. <https://mask-api.icloud.com/egress-ip-ranges.csv>
- [4] S. Bortzmeyer. 2016. *DNS Query Name Minimisation to Improve Privacy*. RFC 7816.
- [5] Sergio Castillo-Perez and Joaquin Garcia-Alfaro. 2009. Evaluation of two privacy-preserving protocols for the DNS. In *Information Technology: New Generations, 2009. ITNG’09. Sixth International Conference on*.
- [6] David Chaum. 1983. Blind signatures for untraceable payments. In *Advances in Cryptology: Proceedings of Crypto 82*. Springer, 199–203.
- [7] David Chaum. 1984. Blind signature system. In *Advances in Cryptology: Proceedings of Crypto 83*. Springer, 153–153.
- [8] David L Chaum. 1981. Untraceable electronic mail, return addresses, and digital pseudonyms. *Commun. ACM* 24, 2 (1981), 84–90.
- [9] Alex Davidson, Ian Goldberg, Nick Sullivan, George Tankersley, and Filippo Valsorda. 2018. Privacy Pass: Bypassing Internet Challenges Anonymously. *Proceedings on Privacy Enhancing Technologies* 2018 (06 2018), 164–180.
- [10] A. Davidson, J. Iyengar, and C. A. Wood. 2022. *Privacy Pass Architectural Framework*. Internet-Draft. Internet Engineering Task Force. <https://www.ietf.org/archive/id/draft-ietf-privacypass-architecture-03.html> Work in Progress.
- [11] R Dingledine, N Mathewson, and P Syverson. 2004. Tor: the second-generation onion router’, USENIX Security Symposium.

- [12] Roger Dingledine and Steven J Murdoch. 2009. Performance Improvements on Tor or, Why Tor is slow and what we're going to do about it. *Online: http://www.torproject.org/press/presskit/2009-03-11-performance.pdf* (2009), 68.
- [13] Brian Eriksson, Paul Barford, Joel Sommers, and Robert Nowak. 2010. A learning-based approach for IP geolocation. In *Passive and Active Measurement: 11th International Conference, PAM 2010, Zurich, Switzerland, April 7-9, 2010. Proceedings 11*. Springer, 171–180.
- [14] Manaf Gharaibeh, Anant Shah, Bradley Huffaker, Han Zhang, Roya Ensafi, and Christos Papadopoulos. 2017. A Look at Router Geolocation in Public and Commercial Databases. In *Internet Measurement Conference* (London, United Kingdom) (IMC '17). Association for Computing Machinery, New York, NY, USA, 463–469. <https://doi.org/10.1145/3131365.3131380>
- [15] Manaf Gharaibeh, Han Zhang, Christos Papadopoulos, and John Heidemann. 2016. Assessing co-locality of IP blocks. In *IEEE Conference on Computer Communications Workshops*. IEEE, San Francisco, CA, USA, 503–508. <https://doi.org/10.1109/INFCOMW.2016.7562129>
- [16] John Gilliom. 2001. *Overseers of the poor: Surveillance, resistance, and the limits of privacy*. University of Chicago Press.
- [17] Bamba Gueye, Steve Uhlig, and Serge Fdida. 2007. Investigating the Imprecision of IP Block-Based Geolocation. In *Passive and Active Network Measurement*, Steve Uhlig, Konstantina Papagiannaki, and Olivier Bonaventure (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 237–240.
- [18] Bamba Gueye, Artur Ziviani, Mark Crovella, and Serge Fdida. 2004. Constraint-based geolocation of internet hosts. In *Proceedings of the 4th ACM SIGCOMM conference on Internet measurement*. 288–293.
- [19] Bamba Gueye, Artur Ziviani, Mark Crovella, and Serge Fdida. 2006. Constraint-Based Geolocation of Internet Hosts. *IEEE/ACM Trans. Netw.* 14, 6 (Dec. 2006), 1219–1232. <https://doi.org/10.1109/TNET.2006.886332>
- [20] Dominik Herrmann, Karl-Peter Fuchs, Jens Lindemann, and Hannes Federrath. 2014. EncDNS: A lightweight privacy-preserving name resolution service. In *European Symposium on Research in Computer Security*. Wroclaw, Poland.
- [21] Paul Hoffman and Patrick McManus. 2018. DNS queries over HTTPS (DoH). RFC 8484 <http://www.ietf.org/rfc/rfc8484.txt>.
- [22] Zi Hu, Liang Zhu, John Heidemann, Allison Mankin, Duane Wessels, and Paul Hoffman. 2016. Specification for DNS over transport layer security (TLS). RFC 7858 <https://www.ietf.org/rfc/rfc7858.txt>.
- [23] Bradley Huffaker, Marina Fomenkov, et al. 2011. *Geocompare: a comparison of public and commercial geolocation databases-Technical Report*. Technical Report. Cooperative Association for Internet Data Analysis (CAIDA).
- [24] Apple Inc. 2021. iCloud Private Relay Overview. https://www.apple.com/icloud/docs/iCloud_Private_Relay_Overview_Dec2021.pdf.
- [25] IP2Location. 2023. *Geolocate Your Visitor's Geographical Location*. https://lite.ip2location.com/?lang=en_US
- [26] ipstack. 2023. *Locate and identify website visitors by IP address*. <https://ipstack.com>
- [27] Ethan Katz-Bassett, John P. John, Arvind Krishnamurthy, David Wetherall, Thomas Anderson, and Yatin Chawathe. 2006. Towards IP Geolocation Using Delay and Topology Measurements. In *6th ACM SIGCOMM Conference on Internet Measurement* (Rio de Janeiro, Brazil) (IMC '06). Association for Computing Machinery, New York, NY, USA, 71–84. <https://doi.org/10.1145/1177080.1177090>
- [28] Etienne Khan, Anna Sperotto, Jeroen van der Ham, and Roland van Rijswijk-Deij. 2023. Stranger VPNs: Investigating the Geo-Unblocking Capabilities of Commercial VPN Providers. In *International Conference on Passive and Active Network Measurement*. Springer, 46–68.
- [29] 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* (Boston, MA, USA) (IMC '18).
- [30] Srinivas Krishnan and Fabian Monrose. 2010. DNS prefetching and its privacy implications: when good things go bad. In *Proceedings of the 3rd USENIX conference on Large-scale exploits and emergent threats: botnets, spyware, worms, and more*. USENIX Association, 10–10.
- [31] Rustam Lalkaka. 2017. Introducing Argo—A faster, more reliable, more secure Internet for everyone. <https://blog.cloudflare.com/argo/>
- [32] Rustam Lalkaka. 2022. *iCloud Private Relay*. <https://blog.cloudflare.com/icloud-private-relay/>
- [33] Rebecca MacKinnon. 2012. Consent of the networked: The worldwide struggle for Internet freedom. *Politique étrangère* 50, 2 (2012), 432–463.
- [34] MaxMind. 2023. *GeoIP2 Databases*. <https://www.maxmind.com/en/geoip2-databases>
- [35] Robert W McChesney. 2013. *Digital disconnect: How capitalism is turning the Internet against democracy*. New Press, The.
- [36] Nominatim. 2023. *Open-source geocoding with OpenStreetMap data*. <https://nominatim.org>
- [37] Venkata N. Padmanabhan and Lakshminarayanan Subramanian. 2001. An Investigation of Geographic Mapping Techniques for Internet Hosts. In *Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications* (San Diego, California, USA) (SIGCOMM '01). Association for Computing Machinery, New York, NY, USA, 173–185. <https://doi.org/10.1145/383059.383073>
- [38] Ingmar Poese, Steve Uhlig, Mohamed Ali Kaafar, Benoit Donnet, and Bamba Gueye. 2011. IP Geolocation Databases: Unreliable? *SIGCOMM Comput. Commun. Rev.* 41, 2 (April 2011), 53–56. <https://doi.org/10.1145/1971162.1971171>
- [39] Loqman Salamatian, Scott Anderson, Joshua Matthews, Paul Barford, Walter Willinger, and Mark Crovella. 2022. Curvature-based analysis of network connectivity in private backbone infrastructures. *Proceedings of the ACM on Measurement and Analysis of Computing Systems* 6, 1 (2022), 1–32.
- [40] 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*. 449–457.
- [41] D Schinazi. 2022. RFC 9298 Proxying UDP in HTTP. (2022).
- [42] David Schinazi and Lucas Pardue. 2022. *HTTP datagrams and the capsule protocol*. Technical Report. Internet-Draft draft-ietf-masque-h3-datagram-08. Internet Engineering Task
- [43] Paul Schmitt, Anne Edmundson, Allison Mankin, and Nick Feamster. 2019. Oblivious DNS: Practical Privacy for DNS Queries. *Proceedings on Privacy Enhancing Technologies* 2019 (04 2019), 228–244.
- [44] Paul Schmitt, Jana Iyengar, Christopher Wood, and Barath Raghavan. 2022. The Decoupling Principle: A Practical Privacy Framework. In *ACM SIGCOMM Workshop on Hot Topics in Networking (HotNets)*.
- [45] Bruce Schneier. 2012. *Liar's and outliers: enabling the trust that society needs to thrive*. John Wiley & Sons.
- [46] Bruce Schneier. 2015. *Data and Goliath: The hidden battles to collect your data and control your world*. WW Norton & Company.
- [47] Bruce Schneier. 2018. Surveillance kills freedom by killing experimentation. <https://www.wired.com/story/mcsweeney-excerpt-the-right-to-experiment/>
- [48] Yuval Shavitt and Noa Zilberman. 2010. A study of geolocation databases. *arXiv preprint arXiv:1005.5674* (2010).
- [49] Yuval Shavitt and Noa Zilberman. 2011. A Geolocation Databases Study. *IEEE Journal on Selected Areas in Communications* 29, 10 (2011), 2044–2056. <https://doi.org/10.1109/JSAC.2011.111214>

- [50] Haya Shulman. 2014. Pretty bad privacy: Pitfalls of DNS encryption. In *Proceedings of the 13th Workshop on Privacy in the Electronic Society*. ACM, 191–200.
- [51] SS Siwpersad, Bamba Gueye, and Steve Uhlig. 2008. Assessing the geographic resolution of exhaustive tabulation for geolocating Internet hosts. In *Passive and Active Network Measurement: 9th International Conference, PAM 2008, Cleveland, OH, USA, April 29–30, 2008. Proceedings* 9. Springer, 11–20.
- [52] Robin Snader and Nikita Borisov. 2008. A Tune-up for Tor: Improving Security and Performance in the Tor Network.. In *ndss*, Vol. 8. 127.
- [53] Paul Syverson, Roger Dингledine, and Nick Mathewson. 2004. Tor: The second generation onion router. In *Usenix Security*. 303–320.
- [54] Paul F Syverson, David M Goldschlag, and Michael G Reed. 1997. Anonymous connections and onion routing. In *Proceedings. 1997 IEEE symposium on security and privacy (cat. no. 97CB36097)*. IEEE, 44–54.
- [55] Tor. 2023. *Tor Metrics*. <https://metrics.torproject.org/userstats-relay-country.html>
- [56] Martino Trevisan, Idilio Drago, Paul Schmitt, and Francesco Bronzino. 2023. Measuring the Performance of iCloud Private Relay. In *Passive and Active Measurement*. Springer Nature Switzerland.
- [57] Inja Youn, Brian L Mark, and Dana Richards. 2009. Statistical geolocation of Internet hosts. In *2009 Proceedings of 18th International Conference on Computer Communications and Networks*. IEEE, 1–6.
- [58] Ali Zohaib, Jade Sheffey, and Amir Houmansadr. 2023. Investigating Traffic Analysis Attacks on Apple iCloud Private Relay. In *Proceedings of the 2023 ACM on Asia Conference on Computer and Communications Security* (Melbourne, VIC, Australia) (ASIA CCS ’23).
- [59] Shoshana Zuboff. 2015. Big other: surveillance capitalism and the prospects of an information civilization. *Journal of information technology* 30, 1 (2015), 75–89.