The Need for an Alternative to IP-Based Geolocation

Author: Zoltan Szamonek

Abstract

IP address geolocation (ip-geo) is currently the default for determining a device's real-world location, used for everything from content optimization to legal compliance. However, IP addresses were not designed for this purpose, leading to inherent inaccuracies and significant privacy concerns. This paper argues that long term continued reliance on ip-geo is unsustainable, especially with the rise of privacy-preserving network architectures. We advocate for standardizing a non-IP-based, user-controlled location signal that provides both the utility of coarse-grained location and the necessary trust for compliance, without compromising user privacy.

The Dual Role and Inherent Limitations of IP Geolocation

IP address geolocation provides valuable utility across the internet ecosystem, broadly falling into the categories:

1. Improve User Experience, providing defaults (like language, timezone, currency) or other location relevant content customization (like displaying local weather)
2. Network/performance optimization (like connecting to the closest server)
3. Legal and Regulatory Compliance: Determining jurisdiction for content filtering (e.g., pharmaceutical ads), taxation, or enforcing geographical licensing agreements

For the first 2 categories, the cost of a mistake is relatively low, a best effort location is usually good enough. However, the last category potentially carries notable risk even on the service provider side.

While ip-geo is useful, it suffers from fundamental limitations:

- Inaccuracy: IP addresses were designed for network routing, not real-world location. While there is a correlation, IP address sharing (potentially across thousands of users) or frequent reassignment of IPs mean the IP is, at best, an *approximate* predictor. Accuracy rapidly diminishes beyond the country level. Research indicates significant discrepancies (over 5%) even among country-level geolocation providers [1].
  Inaccuracy, especially below country level, may have significant impact on various local regulations (e.g., blocking a mobile app in Montana becomes hard if most devices in Montana on carrier IPs are identified as located in Colorado or Washington).
- The VPN/Proxy Challenge: Privacy-enhancing technologies (PETs) like VPNs and privacy relays (e.g., Apple Private Relay) intentionally obscure the user's true IP. The current solution, as demonstrated by Apple's allocation of over 60,000 IPv4 addresses to represent specific egress locations [2], is costly and impractical for smaller service providers, forcing reliance on ip-geo's flawed signal or resulting in the blocking of legitimate PET users.
- Ambiguity of the Location: When a user employs a German VPN server from Russia, is their legal location Russia (origin) or Germany (egress)? The answer is unclear and has profound implications for the applicability of regulations like GDPR, yet service providers are "on the hook" for correct application.

- Limited user consent availability: an IP based location also doesn't carry any user consent. It is available to pretty much anyone, unless the user goes out of their way to block it, e.g. by using PETs. This is true, whether the IP is a carrier IP used by thousands of users at the same time, spanning several US States, or it is the user's home IP address (potentially possible to pin to the user's postal code or even street level address). It is on the service providers to use the IP-based locations responsibly.

Need for a Trusted, Tamper-Proof Location Signal

The compliance use case creates a demand for a trusted location signal that is hard to spoof.

For user experience (e.g., providing local weather), inaccurate locations are not ideal, but often also not a huge problem, even accepting a spoofed location is OK, as it respects a user's preference for an experience (e.g., wanting a New York experience while traveling abroad). However, for compliance use cases, this is often unacceptable.

Current trusted solutions rely typically on IP based location or on high user friction methods (think credit card details, verified addresses, etc.). The reliance on ip-geo for compliance pushes service providers to accept compliance risk or implement anti-spoofing measures, for example, the need to block traffic from VPNs and proxies. Blocking VPNs forces users to potentially give up valuable privacy and security guarantees simply to access a service.

IP based location is relatively accurate on country level, but various compliance use cases may need regional or even finer location information. Think about US state specific regulations, like CCPA for California or regulations aiming to block various Apps in certain US States. Already at the US State Level, we've observed significant accuracy issues with IP based geolocation. As an example, mobile service providers often group mobile devices from nearby states together in a single IP allocation pool, making it impossible to use the IP address to identify if the device is in a specific state.

These issues, combined with the above mentioned significant costs for PET operators, makes IP based location less than ideal for compliance.

Beyond IP-geo

To move beyond ip-geo, we already have alternative location sources.

- GPS-based location
- Location inferred from cell towers or Wi-Fi access points
- Location inferred from timing information
- Verified real world addresses (like addresses for billing, delivery, credit cards, government ids and alike)
- and more.

There are various difficulties with each of these sources around coverage, accuracy, cost, potential spoofing (e.g., Smart TVs typically lack GPS, verifying a delivery address is slow and expensive). The mechanism must also respect user consent at least for fetching relatively precise location information (e.g., for GPS access, many systems already ask for user permission). And there's also no standard way of communicating such location information.

However, such alternative sources are already widely used, especially for use cases where the cost of not having a location or getting a spoofed location is low. For compliance use cases, due to its high

coverage and relatively hard to spoof status, IP based location is still the de-facto location provider, despite the various issues already mentioned above.

As an illustration of the feasibility of transitioning away from ip-geo, examine the following proposal.

The verification of locations or even providing trusted locations could involve other trusted parties. Such a trusted entity would attest that the location is accurate. The location, together with the attestation could then be sent to the web service, e.g. as a geo_hint in a Privacy Pass token [3], which offers a potential cryptographic mechanism for communicating location in a verifiable yet privacy-preserving manner, suggesting a promising direction for creating the required trust without forcing IP disclosure.

A location verifier could gain access to sensitive user or device data, such as verified addresses, device integrity, or proximity to the verifier, in order to confirm a user's location. This entity, however, would not know how the location information is being utilized by the service (e.g., for website access, payment processing, or streaming eligibility).

For instance, Internet Service Providers (ISPs) might run these location verifiers for their subscribers. When a device on their network sends a request to the ISP's service, which already has knowledge of the subscriber and their location, the ISP could either share the location with the device for attestation purposes, or simply confirm the accuracy of the location provided by the device (e.g., if a request states "I need to prove I'm in US, NY", the verifier service would provide the necessary confirmation).

Conclusion

IP-based geolocation is an obsolete technology being forced into a role it cannot reliably fill, creating conflicts between utility, legal necessity, and user privacy. While heavily used, its inaccuracy at finer granularities and its inability to provide a trusted, tamper-proof signal for compliance use cases are critical failures. Furthermore, its continued use directly conflicts with the adoption of privacy-enhancing technologies by driving operators to block VPNs and relays.

The community needs to develop an accepted, standardized, non-IP-based mechanism that can communicate a trusted (verifiable for compliance), privacy-preserving (user-consented, granular), and widely-available location signal. Moving away from ip-geo will not only benefit user privacy and location accuracy but also foster a healthier market for new, honest network players (VPNs, proxies) by eliminating the high cost of managing large, geographically dispersed egress IP pools.

References

[1] https://www.irtf.org/anrw/2020/anrw2020-final7.pdf
[2] https://mask-api.icloud.com/egress-ip-ranges.csv
[3] https://www.ietf.org/archive/id/draft-hendrickson-privacypass-geo-extension-00.html