Incorporating user agency in internet geolocation

Divyank Katira
internet Research Lab
divyank@irl.works

Gurshabad Grover
internet Research Lab
gurshabad@irl.works

Introduction

The primary function of the IP address is to identify and route to entities that are reachable through the internet. As RFC 791, an early specification, states: “The internet protocol provides for transmitting [...] datagrams from sources to destinations, where sources and destinations are hosts identified by fixed length addresses.”[1]

Since this early conception, IP addresses have come to be used in a number of other ways – primarily to glean information about end-users. This includes profiling internet users for behavioral advertising, abuse prevention and law enforcement; building IP reputation systems for spam and DDoS prevention; and geolocating users for localization, optimised service delivery and to comply with local laws.[2]

While not being designed for this purpose, the use of the IP address as a stand-in user identifier and for deriving information about a user has served as a quick-and-easy way for many business, security and legal use cases. These uses have found implicit and explicit support in various standards-setting processes.

We argue here that IP geolocation is an instance of sensitive and private data being generally abused to many ends, including for privacy violations and censorship. IP geolocation happens without user consent, and should be phased out in favour of privacy-respecting alternatives.

IP address is private data

There is an emerging recognition of the privacy risks of IP addresses’ use in profiling and identifying internet users, with some jurisdictions designating them as personally identifiable information for data protection purposes.[3]

---

[1] "RFC 791: Internet Protocol" (1981). https://datatracker.ietf.org/doc/html/rfc791
[2] Katira, D.. "How Internet Applications Geolocate Users and Why It Needs a Rethink." Public Interest Technology Group (2025). https://pitg.network/news/techdive/2025/07/20/geolocation.html.
[3] Office of the Privacy Commissioner of Canada, “Interpretation Bulletin: Personal Information”, Office of the Privacy Commissioner of Canada (2013). https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_02/; “Recital 30: Online identifiers for profiling and identification”, General Data Protection Regulation, https://gdpr.eu/recital-30-online-identifiers-for-profiling-and-identification/.

Users have also signaled a desire to keep their IP address private by adopting technical solutions, such as VPNs, proxies, mixnets and Tor, to obfuscate their IP address from the web services they interact with in order to use the internet more privately.

At the IETF, participants have acknowledged the need to keep IP addresses private and are developing and deploying protocols to help internet users protect their IP address from the web servers they interact with.[4] This work is primarily being done through the OHAI and MASQUE working groups, where participants are working on developing "privacy relays" and “oblivious routing” patterns.[5]

With the adoption of legal and technical safeguards to keep IP addresses private, the fundamental incompatibility between deriving information about users from an IP address with the user requirement for private internet use, is becoming apparent.

IP Geolocation is a violation of privacy

IP-based geolocation has served as a quick-and-easy way for applications to show their users locally relevant content and to demarcate virtual borders that are used to comply with local regulations.

Even though IP-based geolocation has become the norm, there is an important need to recognise that it amounts to abuse of network-layer metadata to derive private information about internet users without their knowledge or consent. Given that consent and agency is understood as a core component of privacy and data protection in most jurisdictions, IP geolocation fails to meet rudimentary standards of privacy. Further, the IAB itself, in RFC 6973 (Privacy Considerations for Internet Protocols) has acknowledged that “data collection and use that happen ‘in secret’, without the individual's knowledge, are apt to violate the individual's expectation of privacy and may create incentives for misuse of data.”[6] This is precisely what has transpired with IP geolocation.

The broad acceptance of non-consensual IP geolocation has spawned commercial services that profile internet users to gain more accurate geolocation estimates. With increased accuracy being a selling point for these services, they deploy data mining techniques against unsuspecting internet users, such as IP triangulation and purchasing third-party data, to improve their location estimates – and they can often succeed in pinpointing approximate geographical coordinates and postal code of a user.[7,8]

---

[4] Finkel, M., et al., "IP Address Privacy Considerations," Internet-Draft draft-irtf-pearg-ip-address-privacy-considerations-01, Internet Research Task Force (2022), https://datatracker.ietf.org/doc/draft-irtf-pearg-ip-address-privacy-considerations/.
[5] "Multiplexed Application Substrate over QUIC Encryption (MASQUE)," IETF Working Group, https://datatracker.ietf.org/wg/masque/about/.
"Oblivious HTTP Application Intermediation (OHAI)," IETF Working Group, https://datatracker.ietf.org/wg/ohai/about/.
[6] Cooper, A. et al., "Privacy Considerations for Internet Protocols," RFC 6973, Internet Architecture Board (2013), https://datatracker.ietf.org/doc/html/rfc6973#section-6.2.
[7] For example, MaxMind, "GeoIP Databases," https://www.maxmind.com/en/geoip-databases.
[8] Zilberman, A., et al. "A Survey on Geolocation on the Internet." *IEEE Communications Surveys & Tutorials* (2024). https://ieeexplore.ieee.org/document/10802881.

IP geolocation is also increasingly[9] being used to enact geo-blocking – a form of internet censorship where content is withheld from internet users based on their geographical location.[10] When governments find it infeasible to block access to an entire online platform, they instead issue takedown orders to the platforms to block individual pieces of content. These platforms utilize IP-based geo-blocking to restrict access to content in the country.

A survey found that enhanced security, privacy and the ability to bypass censorship were the top three motivating factors for the general public to use VPNs.[11]

Despite (1) the evidenced use of IP geolocation to facilitate censorship and privacy violations, and (2) the fact that the general public is using VPNs and other technologies primarily to avoid such abuses and censorship, there are concerted efforts to preserve the status quo. For instance, in response to users' adoption of VPNs and relays, operators of privacy relay solutions – such as Apple's iCloud Private relay and Google Chrome's proposed IP Protection – are looking to convey geolocation information to web servers through alternate means. This is demonstrated by proposals relating to geohashing, geolocation client-hints and maintaining IP geolocation[12,13]. The use of such workarounds directly contradicts users' desires to keep their IP address and related metadata private by opting to use privacy solutions.

Alternatives to IP geolocation

There are other ways of geolocation that respect user agency. Popular mobile operating systems, such as iOS[14] and Android[15], require explicit user consent for location to be shared with a mobile application.

In the space of web browsers, the W3C geolocation specification explicitly includes a section on user consent.[16] While it is non-normative, it states that "an end-user will generally give express permission through a user interface." Popular browsers like Firefox[17] and Google Chrome[18] already mandate user consent before a website can access the user's coordinates.

---

[9] In India, for example, IP-based geo-blocking has become a popular way for the government to conduct internet censorship. Reports indicate that out of the 6,775 pieces of content (includes web pages, websites, apps, social media posts and accounts) blocked by the IT Ministry in 2022, about 50% were X posts and accounts and 25% were on Facebook.

[10] McDonald, A., et al., "403 Forbidden: A Global View of CDN Geoblocking," in *Proceedings of the Internet Measurement Conference 2018* (2018), 218-230, https://dl.acm.org/doi/abs/10.1145/3278532.3278552.

[11] Dutkowska-Zuk, A., et al., "How and Why People Use Virtual Private Networks," in *31st USENIX Security Symposium (USENIX Security 22)* (2022), https://www.usenix.org/system/files/sec22-dutkowska-zuk.pdf.

[12] Apple, "iCloud Private Relay Overview" (2021), https://www.apple.com/icloud/docs/iCloud_Private_Relay_Overview_Dec2021.pdf.

[13] Pauly, T., et al., "The IP Geolocation HTTP Client Hint," Internet-Draft draft-pauly-httpbis-geoip-hint-02, IETF (2025), https://datatracker.ietf.org/doc/draft-pauly-httpbis-geoip-hint/.

[14] "Turn Location Services and GPS on or off on your iPhone, iPad or iPod touch," Apple Support, https://support.apple.com/en-in/102647.

[15] "Request location permissions," Android Developers (2025), https://developer.android.com/develop/sensors-and-location/location/permissions.

[16] W3C, "Geolocation," W3C Recommendation (2022), https://www.w3.org/TR/geolocation/#user-consent.

[17] "Geolocation API," MDN Web Docs, https://developer.mozilla.org/en-US/docs/Web/API/Geolocation_API.

[18] "Manage your location settings in Chrome," Google Chrome Help, https://support.google.com/chrome/answer/142065.

An important distinction between IP geolocation and these two consensual ways of geolocation (in mobile OSs and web browsers) is that the latter rely on GPS. While GPS coordinates are more accurate and revealing, a user's location – at any granularity – is private information that they may choose to reveal, and not something a network protocol should decide on their behalf.

These mechanisms do suffer from a limitation. There are use-cases where user consent is difficult, such as in interface-less IoT devices and agents, where coarse geolocation might still be useful for localization. However, these devices can still rely on direct input from users during setup.

At the very least, it is important to recognise that explicit user consent is normalised in these mechanisms – the same cannot be said of IP geolocation and newer proposals like geolocation hint.[19]

Also note that there are efforts already to provide useful metadata, previously derived from IP addresses, to web servers in other ways. For example, anonymous credential schemes, like those used in the Privacy Pass standard, are being used to distinguish human traffic from bots without using signals like IP addresses or CAPTCHAs.Moving away from IP for geolocation would accompany this trend of not using network layer metadata without the user's consent.

Conclusion

As surveillance and censorship researchers, the history of protocols at the IETF demonstrates to us a pattern: (1) network-layer metadata reveals private information about internet users, (2) web servers and middleboxes design solutions based on free availability of this metadata, (3) the metadata is exploited to conduct privacy violations and censorship. Companies are only forced to reconcile with and reevaluate their dependence on these signals when the gap is plugged. We have seen this repeat with unencrypted HTTP requests and DNS queries, then the SNI field in TLS, and now with IP geolocation.

Given the pervasive reliance on IP geolocation by much of the web, it is easy to see why companies have taken a cautious approach in retaining support for it. But simultaneously, as we move away from IP metadata signals and design appropriate alternatives for them, it is important to recognise that IP geolocation was not intended as a function of the network routing protocol. It simply emerged from its design, and can and is being mitigated against.

Internet applications have incorrectly come to rely on network layer metadata to derive private information about internet users without their knowledge or consent. This metadata is also being misused to conduct privacy violations and censorship on a large scale. While it is not an easy task for companies to re-evaluate their assumptions on the availability of geolocation data, it is in the best interest of end-users to start planning a migration to consensual forms of location sharing on the internet, such as the W3C Geolocation API. The arrival of IP privacy solutions at the IETF is an opportune moment to do so.

---

[19] Pauly, T., et al., (n 13)