Network Working Group
Internet-Draft
Intended status: Informational
Expires: 10 October 2026

J. Iyengar

J. Livingood

T. Pauly

8 April 2026

Report from the IAB Workshop on IP Address Geolocation
draft-iab-ip-geo-workshop-report-01

Abstract

The IAB Workshop on IP Address Geolocation (IP-GEO) was held from December 3-5, 2025, as a three-day virtual meeting. It covered the use cases and background on using IP addresses as indicators of geolocation, explored various problems and challenges that exist in that ecosystem, and discussed future directions and opportunities to improve or replace the current practices.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://intarchboard.github.io/draft-iab-ip-geo-workshop-report/draft-iab-ip-geo-workshop-report.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-iab-ip-geo-workshop-report/.

Source for this draft and an issue tracker can be found at https://github.com/intarchboard/draft-iab-ip-geo-workshop-report.

Status of This Memo

This Internet-Draft will expire on 10 October 2026.

Table of Contents

1. Introduction 3
1.1. About this workshop report content 3
2. Conventions and Definitions 4
3. Current uses of IP geolocation 4
3.1. Why is IP geolocation used? 4
3.1.1. Localized and Relevant Content 5
3.1.2. Targeted Advertising 5
3.1.3. Network Optimization and Server Selection 5
3.1.4. Content Rights Management and Licensing 5
3.1.5. Fraud Detection and Security 6
3.1.6. Regulatory and Legal Compliance 6
3.2. What are the current IP geolocation mechanisms? 6
3.3. What does IP geolocation mean? 7
4. IP geolocation gaps & issues 7
4.1. Architectural issues 7
4.2. Geofeed gaps and inaccuracies 8
4.3. Ecosystem issues 9
4.4. Location-based issues 10
4.5. Privacy issues 10
5. Considering the future of geolocation 11
5.1. Why should IP geolocation change? 11
5.2. In what ways could IP geolocation change? 12
5.3. Considerations for future work 12
5.4. Further work and consideration is needed 13
6. Security Considerations 14
7. IANA Considerations 14
8. Informative References 14
Appendix A. Position Papers 18
Appendix B. Workshop Participatns 20
Appendix C. Workshop Program Committee 20
Acknowledgments 20
Authors' Addresses 20

1. Introduction

The Internet Architecture Board (IAB) holds occasional workshops designed to consider long-term issues and strategies for the Internet, and to suggest future directions for the Internet architecture. This long-term planning function of the IAB is complementary to the ongoing engineering efforts performed by working groups of the Internet Engineering Task Force (IETF).

Many services on the Internet map client IP addresses to a particular geolocation. For exmaple, they might infer that traffic originating from a particular IP address means the traffic originates from a particular city. This practice is widespread even though IP addresses are not designed or guaranteed to have a singular or fixed location associated with them.

Use of IP geolocation has significant impact on the architecture and realities of deploying systems on the Internet, but is frequently not documented or incompletely documented in standards.

The IAB convened a virtual workshop on IP Address Geolocation from December 3-5, 2025. The workshop aimed to:

* Understand the current use cases for publishing, discovering, and consuming IP address geolocation data (Section 3)

* Explore areas for improvement, both in ways to update or replace IP geolocation mechanisms (Section 4)

* Consider mechanisms that satisfy the use cases without relying on geolocating IP addresses (Section 5)

1.1. About this workshop report content

This document is a report on the proceedings of the workshop. The views and positions documented in this report are expressed during the workshop by participants and do not necessarily reflect IAB’s views and positions.

Furthermore, the content of the report comes from presentations given by workshop participants and notes taken during the discussions, without interpretation or validation. Thus, the content of this report follows the flow and dialogue of the workshop but does not attempt to capture a consensus.

2. Conventions and Definitions

Throughout this document, the following terms are used:

* "IP geolocation" is used to refer to the notion of mapping an IP address to one or more physical locations.

* A "geofeed" refers to a file that provides IP geolocation information. In this document, this is usually specifically referring to the format defined in [GEOFEED].

3. Current uses of IP geolocation

The initial discussion of the workshop focused on identifying the current use cases for IP geolocation, and how they interact with today’s mechanisms and ecosystem around IP geolocation.

3.1. Why is IP geolocation used?

Some of the identified use cases were focused on optimizations to user experience or network behavior, such as:

* Automatically choosing appropriate language or regional settings for content

* Providing relevant nearby content (for searches or serving advertisements)

* Optimizing network routes and server selection, generally used to optimize Content Delivery Network (CDNs)

For these use cases, errors in IP geolocation cause annoyance or performance issues, but are generally recoverable (the user can change their location preference or update their search).

Other use cases treat the accuracy of the IP geolocation as a more critical piece of information:

* Enforcing legal or compliance-related requirements

* Enforcing contractual requirements between corporations

* Providing information for disaster relief or law enforcement when other location signals are unavailable

IP geolocation is often not the only signal used to satisfy these use cases, but it is often used as an important piece of them.

All of these use cases are relying on IP geolocation being a passive and implicit signal, without explicit intent being communicated on network connections.

Details of some of these use cases are included below.

3.1.1. Localized and Relevant Content

As discussed in [KLINE], one of the major motivations for the development of the current geofeed format [GEOFEED] was to improve how search results were displayed based on client IP addresses. When users are performing searches or accessing sites that localize content, and the IP geolocation is incorrect, the user may be presented with content that is not relevant (seeing results for a far away city when searching for "pizza near me") or isn’t localized appropriately (seeing content in an unexpected language, or prices in an unexpected currency).

In the case of the development of [GEOFEED], these issues were seen when deploying IPv6, highlighting that the ecosystem had mainly only mapped out IPv4 addresses previously.

3.1.2. Targeted Advertising

The ad-tech ecosystem relies on geolocation to serve localized advertisements. This use represents the highest volume of geolocation queries globally.

3.1.3. Network Optimization and Server Selection

In general, Content Delivery Networks (CDNs) and cloud providers route traffic from clients based on optimizing network topological distance, but IP geolocation is sometimes used as an input to DNS-based routing systems to assist in server selection (see [NYGREN] and [BROWN]). Misalignment here results in suboptimal routing and increased latency for users.

3.1.4. Content Rights Management and Licensing

A primary driver for IP geolocation remains the enforcement of territorial licensing agreements for streaming video, which is the largest volume of data at peak hour on the internet today. Streaming services and media broadcasters rely heavily on IP-to-location mapping to restrict content availability based on country or region (Geo-blocking). Participants noted that this creates a high-stakes environment where accuracy is directly tied to contractual compliance.

3.1.5. Fraud Detection and Security

Financial institutions and identity providers use geolocation as a signal for risk assessment. "Impossible travel" (a user logging in from two distant countries within a short timeframe) or traffic originating from sanctioned regions are standard triggers for security alerts.

3.1.6. Regulatory and Legal Compliance

Operators increasingly use IP geolocation to comply with local laws, including:

* Gambling and Betting regulations: Restricting access to users within specific jurisdictions.

* Taxation: Determining the applicable VAT or sales tax based on the consumer’s location.

* Law Enforcement: Investigating cybercrime by mapping IP addresses to physical jurisdictions for warrant service.

3.2. What are the current IP geolocation mechanisms?

Geofeeds are defined by [GEOFEED] as CSV-formatted mappings from IP address subnets to locations, by country/region and city. [RFC9632] additionally defines how to discover this data and to authenticate it using the Resource Public Key Infrastructure (RPKI).

Often, servers that are checking IP geolocation information are not directly consuming geofeed information, but instead use the services of one or more IP geolocation providers. These services provide not only a mapping from IP address to location, but add in other information, such as notions of IP address "reputation" (indicating if they think this IP address represents traffic from a human user, an automated bot, or a malicious attacker) or a categorization (indicating if an address is associated with proxied or VPN traffic).

IP geolocation providers use various signals to improve the accuracy of their mapping from IP address to location, and have notions of confidence in the validity of the mapping. The workshop noted that various providers won’t necessarily agree on mappings; and, even when they do agree, that does not guarantee that the mapping is accurate. Additionally, the certainty around a location mapping is not something expressed in a standard format for geofeeds, so ambiguity is hidden.

The workshop discussion noted that current mechanisms generally assume that there is a single (generally stable) location associated with an IP address. This is flawed for various reasons: an associated location may change (as in cellular networks or satellite networks), and often there may be many users at different locations behind a single address.

3.3. What does IP geolocation mean?

One of the key points that was raised in discussion was that different use cases and different parties involved in using IP geolocation can have vastly different assumptions about what a particular IP-address-to-location mapping means. For any use case or deployment, a question needs to be asked: what is the claim being made about the IP geolocation mapping?

There are various possible interpretations of a mapping. The location could mean:

* The physical location of a user
* The location of a network egress
* The location of network infrastructure
* The regulatory jurisdiction associated with a network

Geofeeds provide mappings of IP addresses to locations, but they do not define any ontology to describe what these mappings are claiming.

4. IP geolocation gaps & issues

The workshop also focused discussion around identifying challenges with the status quo mechanisms, specifically looking at gaps in current solutions and issues that they raise.

These issues fall into different categories, detailed here.

4.1. Architectural issues

At an achitectural level, IP addresses are not designed to be indications of physical location. This point was brought up in many contexts. This underlying issue causes various problems:

* Geolocation effectiveness is reduced; accuracy issues often stem from the IP address being a poor indicator of location due to not having stable location or a one-to-one relationship with users.

* Privacy and lack of consent; the passive nature of looking at IP addresses and mapping them to locations means that users can have their location targeted without their knowledge, consent, or ability to opt out. Non-consensual geolocation also has the second-order effect of IP geolocation providers profiling internet users through undisclosed mechanisms to increase geolocation accuracy.

* Lack of support in standardization; IP geolocation is a very impactful part of deployment realities and heavily influences the experience users have, but changes to network protocols don’t necessarily account for the impact on IP geolocation. This is seen in cases where deployments as varied as IPv6 address support on servers and privacy proxy systems all needed significant work and engagement with IP geolocation providers to ensure that user experiences still functioned.

* Assumptions about the usefulness of geolocation; physical location does not necessarily correspond to network topologies, so systems assuming that closer physical locations will be faster can be detrimental to network performance.

* Inconsistent effectiveness for security; IP geolocation is often used as an element of security or compliance checks, but often has errors and is hard to validate. It cannot be relied on for security properties, but ends up being used as such in some scenarios.

4.2. Geofeed gaps and inaccuracies

Many of the issues raised were concerned with specifics of geofeeds. These take various forms, such as details that cannot currently be expressed in geofeeds, or inaccurate content in feeds.

The issues raised include:

* Entries cannot express an address being mapped to multiple locations, or express varying levels of confidence in a location mapping

* Names of regions and cities may not be consistent across geofeeds (due to typos, different languages, etc.)

* Identities of regions and cities may vary or have problematic geopolitical nuances

* False specificity occurs when feeds map an address to a city, but the location associated with the address is much bigger than the city

* Geofeed entries may be blatantly incorrect due to staleness or intentional inaccuracies

* Geofeeds may be out of date or stale, without a time-to-live or refresh mechanism

Some participants also expressed the diminishing utility of IP geolocation for compliance due to issues with accuracy and ease of circumvention. [CLARK]

Some of the biggest challenges for providing an accurate geofeed are in dealing with satellite networks or mobile networks using Carrier-Grade NATs (CGNAT). A client device may have a particular true location, but its traffic may exit to the internet via a gateway in a different region. Geo-locating the IP identifies the gateway, not the user, rendering the data coarse or misleading for hyper-local applications.

While country-level accuracy in geofeedds is generally high (estimated >95%), city-level or coordinate-level accuracy degrades significantly. Participants noted instances where IP geolocation defaults to the geographical center of a country or state when specific data is missing, creating "digital sinkholes" (e.g., a farm in Kansas mapped to millions of IP addresses).

4.3. Ecosystem issues

Some issues relate to the deployment and commercial realities of the IP geolocation ecosystem.

IP geolocation providers currently use differing proprietary formats and techniques. Methodologies for determining location are proprietary, and there is no standardized feedback loop for Internet Service Providers (ISPs) to correct erroneous data in third-party databases.

Additionally, updating the version of a IP geolocation database used by a server is asynchronous, and can be a manual process. When there is a major change, such as when an IP address block is transferred from an ISP in Asia to one in Europe, the addresses may remain "located" in Asia in some databases for weeks or months.

With IPv4 exhaustion, the secondary market for address space is active and exacerbates these problems. IP address blocks are frequently sold and moved globally. The "legacy" location data often sticks to these blocks in WHOIS registries or static datasets, leading to persistent misidentification of the new owners' locations.

4.4. Location-based issues

Assigning geolocation to addresses is fraught with issues around location borders. The discussion covered anecdotes of incorrect behavior that came from mobile devices being used near jurisdictional borders between two countries, where the device's IP geolocation could frequently "jump" between countries. Similarly, on borders between timezones, the correct behavior is often ambiguous if derived from IP addresses alone.

4.5. Privacy issues

As discussed in [RFC6973], IP addresses can be used as identifiers to correlate user activity and reveal user identity. IP addresses are often considered Personally Identifiable Information (PII), and the correlation to geolocation makes this very sensitive information that can be correlated to other metadata that identifies users.

Commercial services enrich their datasets to improve their location estimates, and can often succeed in pinpointing approximate geographical coordinates and postal code of a user.

The source IP addresses of a connection established by a client device working on behalf of a user does not come along with any specific consent for how the IP address will be used, and does not imply intent for geolocation or otherwise. In essence: Since IP addresses were not designed for geolocating end-users, IP geolocation amounts to abuse of network-layer metadata to derive private information about internet users without their knowledge or consent.

Virtual Private Networks (VPNs) or proxies (such as privacy proxies discussed in [RFC9614]) allow users to anonymize their specific IP addresses to avoid correlation, and are often used partly for this purpose. [DUTKOWSKA-ZUK]

Sometimes VPNs or proxies intentionally obfuscate or change how the user is represented to IP geolocation providers; but other deployments of privacy services do use geofeeds to preserve the general user location to avoid user experience or compliance issues.

5. Considering the future of geolocation

The final day of the workshop focused on next steps around IP geolocation, both in how to improve mechanisms and in how to build mechanisms that address the use cases in new ways.

One key recognition from the workshop was that IP geolocation, and the ecosystem around it, isn't going to go away or disappear. While it was not necessarily an intentional part of the Internet architecture, large parts of how the Internet functions have been established based on assumptions.

However, it was also recognized that the role and functionality of IP geolocation can change, and in many ways ought to change. This section discusses some of the considerations raised, and suggests next steps.

5.1. Why should IP geolocation change?

Various motivations for changing the status quo of the IP geolocation ecosystem were raised:

* Existing geofeeds have technical gaps that need addressing in order to scale well and continue to be used effectively

* New network deployments, such as satellite networks and privacy proxies, are stretching and challenging the status quo mechanisms

* Pressure from new policies or regulations add requirements for accurate assessment of client location, which IP addresses cannot always provide

* The bar for security and privacy is increasing, challenging the use of passive identifiers like IP addresses being used to tag location

* There are already ways to perform consensual geolocation at the application layer, such as with APIs that meet the W3C Geolocation specifications.

These various motivations and pressures are often in conflict, and create requirements in different directions. Economic and regulatory incentives have shaped the status quo mechanisms, and will continue to shape the evolution of this space.

The technical community, and the various stakeholders in the ecosystem, play an important role in deciding how to handle these pressures and drive the change in the space of IP geolocation.

5.2. In what ways could IP geolocation change?

Two high-level categories of changes were discussed.

First, there are a number of ways in which geofeeds themselves can be improved:

* Add the ability to express infrastructure vs. user locations
* Get beyond the assumption that an IP address always maps to a single location
* Better handle the dynamic nature of geolocation (time-to-live indications, timestamps, live updates to feeds)
* More accurately represent the granularity and specificity of geolocation mappings; be able to express certainty levels
* Improve tooling for publishing, validating, and consuming geofeeds
* Improve measurements for determining accurate geolocation
* Rely more on the RPKI to more reliably verify location claims

Second, and more ambitiously, the community can consider alternative solutions to the use cases behind IP geolocation that do not rely on IP address mapping. [SZAMONEK], [LAOUAR], and [PAULY] propose various ways forward here. These explore ways to let users provide location hints with consent, and involve trying to provide explicit signals that involve trust and verifiability.

Across both of these categories, communicating information with more intentionality and clarity is a key change.

5.3. Considerations for future work

When looking toward future work, the workshop discussion raised some key points to consider:

* The community should work to explain clearly what geofeeds and IP geolocation are able to solve, and what problems they are ill-suited for.
* As new technologies are introduced (either updated geofeeds or new alternative mechanisms), there need to be clear plans for transitions and incremental adoption.

* New solutions need to avoid "ossification" and build in ways to continue to evolve and update.

* New solutions should be careful designed to avoid creating worse privacy problems. For example, a pressure to have explicit signals for location could lead to increased sharing of more specific user location coordinates (such as from GPS data).

* It is unlikely that any one new technical solution can address the various use cases that currently passively use IP geolocation. Different technical solutions will be fit for purpose for different use cases, and will not be one-size-fits-all.

5.4. Further work and consideration is needed

A final conclusion of the workshop was that collaboration and discussion amongst the various stakeholders in this space will be a necessary part of making technical improvements. Not all of the stakeholders in this space are currently actively participating in standards discussions within the IETF, but standards work would benefit from working on improvements in this space.

Some of the stakeholders include, but are not limited to:

* IP geolocation providers

* Client device platforms

* Content publishers

* Network operators

* Data brokers

* Enterprises

* Firewall operators and vendors

* VPN / proxy operators and vendors

* IP address leasers

* Policymakers

* End users

The exact shape of a forum for this community is not yet determined, but this report encourages further work and discussion in this space.

6. Security Considerations

This document is a workshop report and does not impact the security of the Internet.

7. IANA Considerations

This document has no IANA actions.

8. Informative References

[ABLEY] Abley, J., "Geo-Network Operations at Cloudflare", November 2025, <https://www.ietf.org/slides/slides-ipgeows-paper-geo-network-operations-at-cloudflare-00.pdf>.

[BARNES] Barnes, R., "IP Geolocation is Critical for Compliance", November 2025, <https://www.ietf.org/slides/slides-ipgeows-paper-ip-geolocation-is-critical-for-compliance-01.pdf>.

[BROWN] Brown, J., "Moving Beyond Geographic Inference", November 2025, <https://www.ietf.org/slides/slides-ipgeows-paper-moving-beyond-geographic-inference-00.pdf>.

[CLARK] Clark, J., "geocomply.com", November 2025, <https://www.ietf.org/slides/slides-ipgeows-paper-geocomplycom-00.pdf>.

[CROGHAN] Croghan, T., "The Geolocation Conundrum for Small ISPs", November 2025, <https://www.ietf.org/slides/slides-ipgeows-paper-the-geolocation-conundrum-for-small-isps-00.pdf>.

[DUTKOWSKA-ZUK] Dutkowska-Zuk, A., Hounsel, A., Morrill, A., Xiong, A., Chetty, M., and N. Feamster, "How and Why People Use Virtual Private Networks", August 2022, <https://www.usenix.org/system/files/sec22-dutkowska-zuk.pdf>.

[ELKINS] Elkins, N., Nguyen, M., and B. Jouris, "Bridging the Gaps in IP Geolocation: Strengthening Detection and Defense Against Cyber Threats", December 2025, <https://www.ietf.org/slides/slides-ipgeows-paper-bridging-the-gaps-in-ip-geolocation-strengthening-detection-and-defense-against-cyber-threats-00.txt>.

[FAYED] Fayed, M., "Does IP geolocation answer the right questions?", November 2025, <https://www.ietf.org/slides/slides-ipgeows-paper-does-ip-geolocation-answer-the-right-questions-00.pdf>.

[GAO] Gao, P., Lee, E., and Y. Zhang, "On the Use, Challenges, Alternatives of IP Geolocation Data", November 2025, <https://www.ietf.org/slides/slides-ipgeows-paper-on-the-use-challenges-alternatives-of-ip-geolocation-data-00.pdf>.

[GASSER] Gasser, O., Leung, W., and M. Mouchet, "On the Use, Challenges, Alternatives of IP Geolocation Data", November 2025, <https://www.ietf.org/slides/slides-ipgeows-paper-challenges-of-working-with-geofeeds-00.pdf>.

[GEOFEED] Kline, E., Duleba, K., Szamonek, Z., Moser, S., and W. Kumari, "A Format for Self-Published IP Geolocation Feeds", RFC 8805, DOI 10.17487/RFC8805, August 2020, <https://www.rfc-editor.org/rfc/rfc8805>.

[HOSFELT] Hosfelt, R., Haberman, B., Jaeggli, J., and S. Strowes, "Position Paper by Fastly", November 2025, <https://www.ietf.org/slides/slides-ipgeows-paper-position-paper-by-fastly-for-iab-workshop-on-ip-address-geolocation-00.pdf>.

[HOWARD] Howard, L., "IP geolocation paper", November 2025, <https://www.ietf.org/slides/slides-ipgeows-paper-ip-geolocation-paper-00.pdf>.

[HUSTON] Huston, G., "Geolocation and Starlink", September 2025, <https://www.ietf.org/slides/slides-ipgeows-paper-geolocation-and-starlink-00.txt>.

[IZHIKEVICH] Izhikevich, K., Du, B., Tran, M., Rao, S., Ukani, A., and L. Izhikevich, "Trust, But Verify, Operator-Reported Geolocation", November 2025, <https://www.ietf.org/slides/slides-ipgeows-paper-trust-but-verify-operator-reported-geolocation-00.pdf>.

[KATIRA] Katira, D. and G. Grover, "Incorporating user agency in internet geolocation", November 2025, <https://www.ietf.org/slides/slides-ipgeows-paper-incorporating-user-agency-in-internet-geolocation-00.pdf>.

[KHAN] Khan, K., "From Surveillance to Consent: A Privacy-First Approach to IP Geolocation", November 2025, <https://www.ietf.org/slides/slides-ipgeows-paper-from-surveillance-to-consent-a-privacy-first-approach-to-ip-geolocation-00.pdf>.

[KISTELEKI] Kisteleki, R., "RIPE IPmap - The RIPE NCC's Approach to Infrastructure IP Geolocation", November 2025, <https://www.ietf.org/slides/slides-ipgeows-paper-ripe-ipmap-the-ripe-nccs-approach-to-infrastructure-ip-geolocation-00.pdf>.

[KLINE] Kline, E., "Anecdotal History of RFC 8805", November 2025, <https://www.ietf.org/slides/slides-ipgeows-paper-anecdotal-history-of-rfc-00.pdf>.

[LAOUAR] Laouar, A., Desgeorges, L., Schmitt, P., and F. Bronzino, "Rethinking Geolocalization on the Internet", November 2025, <https://www.ietf.org/slides/slides-ipgeows-paper-rethinking-geolocalization-on-the-internet-00.pdf>.

[MATHUR] Mathur, S., "Improvements Ideas from an IP Geolocation API Provider", November 2025, <https://www.ietf.org/slides/slides-ipgeows-paper-improvements-ideas-from-an-ip-geolocation-api-provider-00.pdf>.

[MUKHERJEE] Mukherjee, D., "Gaps and problems in current IP-Geolocation Approaches", November 2025, <https://www.ietf.org/slides/slides-ipgeows-paper-gaps-and-problems-in-current-ip-geolocation-approaches-00.pdf>.

[NYGREN] Nygren, E. and R. Dhanidina, "Akamai Position Paper for 2025 IAB Workshop on IP Address Geolocation", November 2025, <https://www.ietf.org/slides/slides-ipgeows-paper-akamai-position-paper-for-iab-workshop-on-ip-address-geolocation-ip-geo-00.pdf>.

[OWENS] Owens, N., "Starlink", October 2025, <https://www.ietf.org/slides/slides-ipgeows-paper-position-paper-starlink-00.pdf>.

[PAN] Pan, J. and J. Zhao, "GeoFeed in the wild: A case study on StarlinkISP.net", November 2025, <https://www.ietf.org/slides/slides-ipgeows-paper-geofeed-in-the-wild-a-case-study-on-starlinkispnet-00.pdf>.

[PAULY] Pauly, T., Schinazi, D., McMullin, C., and D. Mitchell, "The IP Geolocation HTTP Client Hint", November 2025, <https://www.ietf.org/slides/slides-ipgeows-paper-the-ip-geolocation-http-client-hint-00.pdf>.

[RAMANATHAN] Ramanathan, A. and S. A. Jyothi, "Systematic Detection and Correction of IP Geolocation Anomalies in Network Measurements", November 2025, <https://www.ietf.org/slides/slides-ipgeows-paper-systematic-detection-and-correction-of-ip-geolocation-anomalies-in-network-measurements-00.pdf>.

[RFC6973] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", RFC 6973, DOI 10.17487/RFC6973, July 2013, <https://www.rfc-editor.org/rfc/rfc6973>.

[RFC9614] Khlewind, M., Pauly, T., and C. A. Wood, "Partitioning as an Architecture for Privacy", RFC 9614, DOI 10.17487/RFC9614, July 2024, <https://www.rfc-editor.org/rfc/rfc9614>.

[RFC9632] Bush, R., Candela, M., Kumari, W., and R. Housley, "Finding and Using Geofeed Data", RFC 9632, DOI 10.17487/RFC9632, August 2024, <https://www.rfc-editor.org/rfc/rfc9632>.

[SCHATTE] Schatte, D., "IAB Workshop on IP Address Geolocation", December 2025, <https://www.ietf.org/slides/slides-ipgeows-paper-iab-workshop-on-ip-address-geolocation-daniel-schatte-00.pdf>.

[SHARMA] Sharma, O. P., "Position Paper for IAB Workshop on IP Address Geolocation", November 2025, <https://www.ietf.org/slides/slides-ipgeows-paper-position-paper-for-iab-workshop-on-ip-address-geolocation-ipgeows-00.pdf>.

[SZAMONEK] Szamonek, Z., "The Need for an Alternative to IP-Based Geolocation", November 2025, <https://www.ietf.org/slides/slides-ipgeows-paper-the-need-for-an-alternative-to-ip-based-geolocation-00.pdf>.

[TARIQ] Tariq, M., "IP Address Geolocation Use Cases, Gaps, and Future Directions", November 2025, <https://www.ietf.org/slides/slides-ipgeows-paper-ip-address-geolocation-use-cases-gaps-and-future-directions-00.pdf>.

[VERMEULEN] Vermeulen, K., "IP geolocation through the lens of an academic: Where do we stand?", November 2025, <https://www.ietf.org/slides/slides-ipgeows-paper-ip-geolocation-through-the-lens-of-an-academic-where-do-we-stand-00.pdf>.

Appendix A. Position Papers

30 position papers were accepted to the workshop. All papers are available at https://datatracker.ietf.org/group/ipgeows/materials/ (https://datatracker.ietf.org/group/ipgeows/materials/).

The position papers are listed here:

* J. Abley: Geo-Network Operations at Cloudflare [ABLEY]

* R. Barnes: IP Geolocation is Critical for Compliance [BARNES]

* J. Brown: Moving Beyond Geographic Inference [BROWN]

* J. Clark: geocomply.com [CLARK]

* T. Croghan: The Geolocation Conundrum for Small ISPs [CROGHAN]

* N. Elkins, M. Nguyen, B. Jouris: Bridging the Gaps in IP Geolocation: Strengthening Detection and Defense Against Cyber Threats [ELKINS]

* M. Fayed: Does IP geolocation answer the right questions? [FAYED]

* P. Gao, E. Lee, Y. Zhang: On the Use, Challenges, Alternatives of IP Geolocation Data [GAO]

* O. Gasser, W. Leung, M. Mouchet: Challenges of Working With Geofeeds [GASSER]

* R. Hosfelt, B. Haberman, J. Jaeggli, S. Strowes: Position paper by Fastly [HOSFELT]

* L. Howard: IP geolocation paper [HOWARD]

* G. Huston: Geolocation and Starlink [HUSTON]

* K. Izhikevich, B. Du, M. Tran, S. Rao, A. Ukani, L. Izhikevich: Trust, But Verify, Operator-Reported Geolocation [IZHIKEVICH]

* D. Katira, G. Grover: Incorporating user agency in internet geolocation [KATIRA]

* K. Khan: From Surveillance to Consent: A Privacy-First Approach to IP Geolocation [KHAN]

* R. Kisteleki: RIPE IPmap - The RIPE NCC's Approach to Infrastructure IP Geolocation [KISTELEKI]

* E. Kline: Anecdotal History of RFC 8805 [KLINE]

* A. Laouar, L. Desgoerges, P. Schmitt, F. Bronzino: Rethinking Geolocalization on the Internet [LAOUAR]

* S. Mathur: Improvements Ideas from an IP Geolocation API Provider [MATHUR]

* D. Mukherjee: Gaps and problems in current IP-Geolocation Approaches [MUKHERJEE]

* E. Nygren, R. Dhanidina: Akamai Position Paper for 2025 IAB Workshop on IP Address Geolocation [NYGREN]

* N. Owens: Starlink [OWENS]

* J. Pan, J. Zhao: GeoFeed in the wild: A case study on StarlinkISP.net [PAN]

* T. Pauly, D. Schinazi, C. McMullin, D. Mitchell: The IP Geolocation HTTP Client Hint [PAULY]

* A. Ramanathan, S. A. Jyothi: Systematic Detection and Correction of IP Geolocation Anomalies in Network Measurements [RAMANATHAN]

* D. Schatte: IAB Workshop on IP Address Geolocation [SCHATTE]

* O. P. Sharma: Position Paper for IAB Workshop on IP Address Geolocation [SHARMA]

* Z. Szamonek: The Need for an Alternative to IP-Based Geolocation [SZAMONEK]

* M. Tariq: IP Address Geolocation Use Cases, Gaps, and Future Directions [TARIQ]

* K. Vermeulen: IP geolocation through the lens of an academic: Where do we stand? [VERMEULEN]

Appendix B. Workshop Participatns

The workshop participants were Alagappan Ramanathan, Andrew Chen, Augustin Laouar, Bill Jouris, Bob Hinden, Brian Haberman, Calvin Ardi, Carlos Martinez, Christopher Luna, Cindy Morgan, Daniel Schatte, David Schinazi, Debayan Mukherjee, Dhruv Dhody, Divyank Katira, Elizabeth Cronan, Enock Lee, Erik Kline, Erik Nygren, Francesco Bronzino, Gannon Barnett, Geoff Huston, Glenn Deen, Gurshabad Grover, Haniel Abrasos Malik Hayato Kazama, Hiroki Kawabata, James Clark, Jamie Sherry, Jana Iyengar, Jason Livingood, Jeff Brown, Jianping Pan, Jinwei Zhao, Joe Abley, Joel Jaeggli, Jordan Holland, Julien Gamba, Kaitlyn Pellak, Katherine Izhikevich, Kevin Phair, Lee Howard, Loc Desgeorges, Marwan Fayed, Matthew Wilder, Max Mouchet, Md. Kamruzzaman Khan, Mudassar Tariq, Nalini Elkins, Nathan Owens, Nobuhiro Takamizawa, Oliver Gasser, Om Prakash Sharma, Paul Gao, Richard Barnes, Ricky Hosfelt, Rob Seastrom, Robert Kisteleki, Sid Mathur, Stephen Strowes, Suresh Krishnan, Tommy Croghan, Tommy Pauly, Warren Kumari, William Leung, Yaozhong Zhang, Yoshiki Ishida, and Zoltan Szamonek.

Appendix C. Workshop Program Committee

The workshop program committee members were Glenn Deen, Jana Iyengar, Mirja Khlewind, Warren Kumari, Jason Livingood, and Tommy Pauly.

Acknowledgments

Thanks to all of the workshop participants who attended and contributed papers to this effort!

Authors' Addresses

Jana Iyengar
Email: jri.ietf@gmail.com

Jason Livingood
Email: Jason_Livingood@comcast.com

Tommy Pauly
Email: tpauly@apple.com