

The Need for an Alternative to IP-Based Geolocation

by Zoltan Szamonek

IP-Geo High Level Use Cases



Improve User Experience

Providing defaults (language, timezone, currency) or local content customization



Network Optimization

Connecting to the closest server (performance)



Legal & Regulatory Compliance

Determining jurisdiction, legal content filtering or geographical licensing

For UX and optimization, a best effort location is typically sufficient and low risk. Mistakes in compliance carry notable risk for service providers.

Fundamental Limitations

- Inaccuracy: IP addresses are not meant for geolocation; accuracy rapidly diminishes beyond the country level.
- VPNs/Proxies/PETs hide IP, breaking location (causing issues for web services) or needing costly workarounds (60k ipv4 addresses for APR)
- Location Ambiguity: The legal location (origin vs. egress) is often unclear (e.g. VPNs), yet service providers must apply regulations correctly.
- An IP Address carries more information than just location.



Alternatives Beyond IP Geolocation

- Device-based: GPS, cell towers, Wi-Fi access points, timing information.
- Verified Credentials: Postal addresses, credit card details, government IDs.

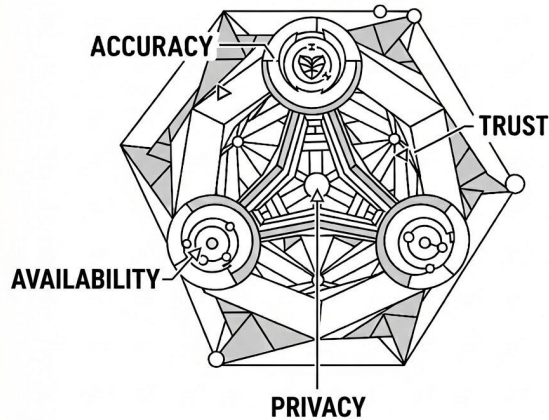
Challenges:

Cost, Coverage, User friction, Spoofability

IP-Geo remains the default for high-stakes compliance due to its high coverage and relatively high country accuracy.



Requirements for a new location signal



- High accuracy, preferably also useful for regional/state-level compliance
- Hard to spoof signal for critical compliance use cases
- Always available, low cost, low friction at least for essential use cases
- Privacy preserving

A Better Trusted Location - Proposal



One potential way:

1. Trusted Verifier checks/attests location (potentially with access to sensitive data)
2. The Verifier issues a certificate with the location (bound to the requester)
3. The location with the certificate is then communicated to the web service

Instead of the Web Service figuring it out on its own (e.g., based on IP).

Does it actually solve the problems?

- High accuracy: location provider can be accurate, as it can have access to sensitive data (IP, internet connection, billing address or more)
- Hard to spoof: location provider can implement further measures against spoofing (e.g. check proximity to verifier, ensure device integrity), certificate should be bound to the requester to avoid sharing
Web services may remove trust from location providers if spoofing is detected.
- Always available, low cost, low friction: no user involvement needed (potentially other than one-time registration), can be implemented at scale for all impacted requests
- Privacy preserving: other than location, the certificate refers to the location provider
fix: proxy location verifiers may rewrite the certificate to hide this information.

Open Questions

Q: Who should serve as the trusted location provider?

A: ISP? Apple? Google? Other entities?

Q: How to ensure honesty and trust?

A: Spoofing is often detectable, trust can be revoked.

Q: Should access to location data depend on its granularity?

A: High level location should be available.

Finer granularity locations: explicit user consent may be needed, or provider only verifies finer locations.



Conclusion: Time to Replace IP-Geo



IP-Geo is an outdated technology that creates conflicts between utility, legal necessity, and user privacy.

Better Solutions are feasible, but the community needs to implement and standardize.

Moving away from IP-Geo benefits user privacy, web services and network operators