IAB Workshop on IP Address Geolocation (ipgeows)

Submitted by: Daniel Schatte, Charter Communications

Introduction

From an ISP perspective, IP-geolocation serves important operational purposes, but it also raises significant privacy concerns that must be addressed. ISPs sit at the intersection of technical necessity and customer trust: while we facilitate access and provide the infrastructure, we also bear responsibility for protecting the privacy of millions of subscribers.

The comments focus on the dual priorities of supporting legitimate operational use cases while ensuring that geolocation practices do not compromise end-user privacy.

Current ISP Use Cases

ISPs encounter IP-geolocation in several domains:

- **Fraud prevention and account security**: Assisting customers and partners in detecting unusual login or access patterns.
- **Customer experience**: Enabling generalized localization (e.g., delivering regional content or directing traffic to the closest CDN node).

Importantly, ISPs often do not directly consume geolocation data themselves but instead see its use by third-party partners, over-the-top platforms, and advertisers who rely on commercial geolocation providers.

Challenges and Gaps

From an ISP perspective, several challenges persist:

- **Accuracy**: Geolocation databases are often inaccurate, especially in dynamic addressing environments or when carrier-grade NAT (CGNAT) is deployed as IP space is being optimized around different areas of the network for utilization efficiencies. Errors lead to misclassification of users and degraded service experiences.
- **Granularity pressure**: Commercial stakeholders increasingly demand more precise location data (down to city or zip code), creating tension with privacy protections.
- **Trust and validation**: There is no standardized or transparent method to validate the accuracy or provenance of geolocation data across the multiple geolocation service providers.

Privacy and Ethical Considerations

Customer privacy is central to ISP operations and customer trust. Current geolocation practices raise several concerns:

- **Secondary use and overreach**: Advertisers, data brokers, and other third parties frequently use fine-grained geolocation for targeting or surveillance, well beyond the original purpose.
- **Risk of deanonymization**: As granularity increases, geolocation data can be combined with other identifiers to pinpoint individuals.

For ISPs, this creates a conflict: while we must comply with operational requirements, we must also safeguard privacy by minimizing data disclosure.

Improved Technical and Policy Approaches

To address these challenges, I propose the following:

1. **Coarse-grained or tiered disclosure**: Limit data disclosure to city-level granularity by default, with finer granularity only where required and justified.
2. **Privacy-preserving formats**: Standardize mechanisms for “blurred” or generalized location data, possibly incorporating differential privacy approaches.
3. **Clear governance and limitations**: Define acceptable use cases (e.g., fraud prevention, emergency services) and restrict commercial or advertising applications unless explicit customer consent is obtained.

Distribution and Operational Concerns

From a practical ISP perspective:

- **Automation is essential**: Any proposed system must allow automated, scalable updates for dynamic IP pools in a near real-time construct.
- **Standardized schemas**: JSON or similar machine-readable formats with clear definitions for granularity levels would reduce interoperability issues.
- **Federated or opt-in models**: Instead of public geolocation databases, consider federated approaches where ISPs selectively provide verified data under strict access controls.

Future Vision

An ideal geolocation ecosystem would:

- Have geolocation databases being updated near real-time for geolocation feeds produced by ISPs instead of multiple weeks post feed update.
- Protect end-user privacy by default, ensuring coarse-grained disclosure unless finer resolution is explicitly justified.
- Serve legitimate and narrowly defined operational and security use cases.

- Prevent misuse by advertisers, data brokers, and unauthorized actors.
- Integrate with broader identity and trust frameworks that may ultimately reduce dependence on raw IP-based geolocation.

This vision prioritizes **trust**—customers must believe that their ISP protects their privacy rather than exposing it.

Recommendations to the Workshop

I encourage the workshop to:

- Prioritize **privacy-preserving standards** in any technical proposals.
- Establish clear **guidelines on data granularity, consent, and secondary use**.
- Promote collaboration among ISPs and geolocation service providers to balance needs fairly and ingest ISP geolocation feeds in a timelier manner.
- Increase transparency so that customers understand how IP-geolocation is used and for what purposes.

Conclusion

Our position is that IP-geolocation must balance utility with **customer trust and privacy**. While geolocation enables important operational functions, the current ecosystem lacks safeguards against misuse, overreach, and timeliness of provider database updates.

I strongly recommend that the workshop prioritize privacy by design, support standardized mechanisms for coarse-grained disclosure, and place clear limits on commercial exploitation while being updated in near real time based upon the ISP geolocation feed.