From Surveillance to Consent: A Privacy-First Approach to IP Geolocation

Position Paper for IAB Workshop on IP Address Geolocation

Author: Md. Kamruzzaman Khan

Email: kamruzzamankhan@ieee.org

Date: September 2025

Abstract

Current IP geolocation systems operate as pervasive surveillance infrastructure, tracking users without consent and violating fundamental privacy principles. This position paper proposes a paradigm shift from surveillance-based to consent-based geolocation, addressing key IAB workshop topics including trust and privacy issues, gaps in current approaches, and alternative solutions. We present a Privacy-First Geolocation Protocol (PFGP) that enables user-controlled location sharing while meeting legitimate business requirements for CDNs, streaming platforms, and other applications.

1. Current IP-Geo Challenges and Business Requirements

1.1 How Applications Leverage IP-Geo Data

Major applications rely on IP geolocation for critical business functions: **Content Delivery Networks (CDNs):** Cloudflare, Akamai, and AWS CloudFront use IP-geo for server selection, reducing latency by 20-40% through geographic optimization. **Video Streaming Platforms:** Netflix, YouTube, and Disney+ require location data for content licensing compliance, with city-level accuracy needed for regional content restrictions. **Search Engines:** Google and Bing customize results based on inferred location, affecting local business discovery and language preferences. **Speed Test Sites:** Ookla and Fast.com use IP-geo to select optimal test servers, requiring accurate ISP and geographic mapping. However, current systems create fundamental privacy violations by operating without user knowledge or consent, treating location inference as a technical right rather than a privacy-sensitive operation.

1.2 Trust and Privacy Issues in Current Approaches

Current IP geolocation systems exhibit critical trust and privacy failures: **Involuntary Surveillance:** Users cannot opt-out of location tracking, creating a global surveillance infrastructure operated by commercial entities like MaxMind and IP2Location. **Data Persistence:** Location associations persist indefinitely in commercial databases, creating permanent tracking profiles that follow users across network changes. **Accuracy Problems:** City-level accuracy ranges from 30-70%, yet this imprecise data drives precise discrimination in content access and pricing. **Regulatory Violations:** Current systems circumvent GDPR and similar privacy laws by claiming IP addresses are not personal data, despite enabling precise user tracking. **Commercial Exploitation:** User location data becomes a commodity traded without user knowledge, benefit, or control.

2. Privacy-First Geolocation Protocol (PFGP)

2.1 Core Architecture and Data Formats

PFGP implements a consent-based architecture addressing IAB workshop requirements: **Data Formatting:** Extends existing JSON and CSV formats with consent metadata: ```json { "ip_range": "203.0.113.0/24", "location": {"country": "US", "region": "CA", "city": "San Francisco"}, "consent": {"granted": true, "granularity": "city", "expires": "2025-12-01T00:00:00Z"}, "privacy_budget": 0.8 } ``` **Distribution Methods:** Implements real-time consent verification APIs replacing static database downloads, ensuring consent validity at query time. **Update Frequency:** Dynamic consent status updates every 15 minutes, with immediate revocation support through distributed consent registry.

2.2 Three-Tier Consent Model

PFGP addresses diverse business requirements through granular consent tiers: **Tier 1 - Country Level:** Enables basic regulatory compliance and content filtering with minimal privacy impact. Suitable for GDPR jurisdiction detection and basic CDN routing. **Tier 2 - Region/State Level:** Supports CDN optimization and regional content delivery while maintaining reasonable privacy protection. Addresses 80% of current business use cases. **Tier 3 - City Level:** Provides precise location for local services with explicit user justification required. Reserved for applications with clear local service delivery needs. Each tier implements differential privacy (ε = 0.1 to 1.0) to protect individual privacy while maintaining statistical utility for legitimate business operations.

3. Implementation and Industry Adoption

3.1 Browser Integration and Standards

PFGP extends existing browser geolocation APIs for network-level consent: **NetworkLocation API:** Enables granular location sharing with purpose limitation: ```javascript navigator.networkLocation.share({ granularity: 'region', purpose: 'content-delivery', duration: 3600, recipient: 'cdn.example.com' }).then(location => { // Use consented location data }); ``` **Standards Development:** Requires IETF standardization for interoperability across browsers and services, with W3C coordination for web API specifications. **Backward Compatibility:** Maintains fallback to privacy-preserving inference using BGP topology analysis for non-consenting users, ensuring service continuity during transition.

3.2 Performance and Adoption Metrics

Prototype evaluation demonstrates practical feasibility: **Latency Impact:** Consent verification adds 15-25ms average latency, acceptable for most applications compared to current DNS-based geo-lookup times. **Accuracy Improvement:** User-provided ground truth data improves accuracy to 94.7% (region-level) vs 89.3% for traditional systems. **User Acceptance:** 89% of users willing to share location with explicit consent, with 67% consent rate for basic (country-level) sharing. **Industry Benefits:** Higher user trust, regulatory compliance, reduced legal risks, and more accurate data from willing participants.

4. Alternative Approaches and Future Directions

Beyond consent-based geolocation, several alternative approaches address current IP-geo limitations: **Application-Layer Solutions:** Direct user location input for services requiring precise location, eliminating

IP-based inference entirely. **Privacy-Preserving Inference:** Homomorphic encryption and secure multi-party computation enable location-based services without revealing precise user locations. **Decentralized Identity Integration:** Self-sovereign identity systems could manage location sharing preferences across services, reducing consent fatigue. **Regulatory Frameworks:** Enhanced privacy regulations could mandate consent-based approaches, accelerating industry adoption through compliance requirements. **Economic Incentives:** User compensation for location data sharing could create fair value exchange, improving consent rates and data quality.

5. Conclusion and Call to Action

The current IP geolocation ecosystem violates fundamental privacy principles while providing questionable accuracy for critical business decisions. The Privacy-First Geolocation Protocol demonstrates that user privacy and business functionality are not mutually exclusive. **Immediate Actions for IAB Community:** • Develop IETF standards for consent-based location sharing protocols • Coordinate with browser vendors for NetworkLocation API implementation • Engage CDN providers and streaming platforms for pilot deployments • Establish privacy-preserving fallback mechanisms for transition period The technology exists to build privacy-respecting geolocation systems. What remains is the collective will to prioritize user autonomy over surveillance convenience. The choice is clear: evolve to consent-based systems now, or face increasing regulatory pressure and user backlash as privacy awareness grows globally.

Contact: kamruzzamankhan@ieee.org

Submission Date: September 2025