IAB Workshop on IP Address Geolocation

Moving Beyond Geographic Inference

Jeff Brown - jeffbr@apple.com - October, 2025

Content Delivery Networks (CDNs) have long relied on IP address geolocation (geo-IP) for traffic routing and content optimization decisions. However, the implementation of geo-IP usage varies significantly across providers, with substantial implications for user privacy and network performance. While Apple's CDN infrastructure is an example of geo-IP usage that addresses current operational needs without compromising sensitive data, CDNs are evolving beyond exclusively using geographic inference. For example, there are emerging standards like Service Binding (SVCB) record-based routing[1] that can eliminate server-side location inference entirely. This would allow CDNs to shift decision-making from server-side geo-IP lookups to client-side service selection. Other techniques such as network performance-based routing[2], differential privacy applications[3], and user-controlled location disclosure[4] would allow CDNs to improve performance and reliability while providing guarantees of user privacy protection.

Performance Requirements and Global Challenges

Modern CDNs must support diverse services spanning global internet infrastructure. Data synchronization and backup services require reliable, high-throughput connections across multiple geographic regions. Application and software update distribution demands efficient delivery of large files to millions of users simultaneously, particularly during peak periods. Streaming content requires high bandwidth capacity and consistent quality of service, while real-time services need sub-100ms latency for interactive applications and live communications. High-bandwidth content delivery for 4K and HDR streaming requires substantial bandwidth capacity and consistent throughput to prevent buffering during peak usage. Global load balancing across distributed CDN infrastructure must account for varying regional demand patterns, network capacity constraints, and service availability during traffic spikes.

In order to meet these challenges, the current generation of Apple's CDN employs geo-IP practices that minimize sensitive data exposure while maintaining operational effectiveness. The system uses coarse-grained geographic routing with only country or region-level location data, avoiding collection or storage of precise location information. Real-time routing decisions are made without

[1] Schwartz, B., Bishop, M., and E. Nygren, "Service Binding and Parameter Specification via the DNS (SVCB and HTTPS Resource Records)," RFC 9460, November 2022.

[2] Flavel, A., et al., "FastRoute: A Scalable Load-Aware Anycast Routing Architecture for Modern CDNs," USENIX NSDI, 2015.

[3] Dwork, C. and Roth, A., "The Algorithmic Foundations of Differential Privacy," Foundations and Trends in Theoretical Computer Science, 2014.

[4] Pauly, T., Schinazi, D., McMullin, C., and D. Mitchell, "The IP Geolocation HTTP Client Hint," draft-pauly-httpbis-geoip-hint-01, October 2024

persistent storage, with geo-IP lookups performed solely to determine appropriate serving locations, discarded immediately after use to prevent long-term location tracking. This approach satisfies existing legal compliance requirements for content licensing and data residency while maximizing user experience.

However, global CDN operations face increasingly complex regulatory compliance challenges varying across jurisdictions. Data residency requirements mandate that user data be stored and processed within specific geographic boundaries, complicating globally distributed system design. GDPR Article 25 "Privacy by Design"[5] requires privacy protection built into systems from the ground up, affecting every aspect of CDN design from data collection to transmission protocols. User consent and transparency requirements have evolved beyond simple opt-in mechanisms to include granular control over data usage. Data localization laws create additional complexity, as different countries impose varying requirements on data storage[6], processing, and cross-border transfers[7]. These requirements conflict with distributed CDN systems and require careful architectural planning. Varying national security and surveillance requirements add complexity, as governments may require data access or impose restrictions on encryption measures that impact privacy-preserving CDN operations.

Evolving CDN Optimization Techniques

Service Binding (SVCB) records, defined in RFC 9460, provide a mechanism for services to advertise connection and configuration information through DNS. Unlike traditional approaches that rely on IP geolocation inference, SVCB records enable explicit declaration of service capabilities, connection parameters, and optimization hints directly in the DNS response. SVCB records represent a new approach to CDN optimization that aligns with privacy-first design principles while enhancing performance capabilities. By enabling declarative service discovery and connection optimization through DNS, SVCB records can reduce the reliance on IP geolocation for CDN routing decisions by supporting the user-controlled location disclosure model. This enables clients to select appropriate service endpoints based on content requirements, user preferences or regulatory compliance without relying on server-side inference.

Network performance-based routing represents a shift from geographic location to network characteristics for CDN optimization. Round Trip Time (RTT) measurements provide direct indicators of network performance between users and potential servers, enabling routing decisions based on connectivity quality rather than assumed geographic proximity. This approach often yields better performance results compared to IP geolocation methods, as network topology does not always correlate with geographic distance.

[5] European Union, "General Data Protection Regulation (GDPR)," 2018.

[6] Standing Committee of the National People's Congress, "Cybersecurity Law of the People's Republic of China," Order No. 53, November 7, 2016

[7] Government of India, "The Digital Personal Data Protection Act, 2023," Act No. 22 of 2023

Differential privacy enables usage pattern analysis by adding calibrated noise to user behavior data, providing mathematical guarantees that individual user privacy is protected while preserving the statistical utility needed for understanding aggregate demand patterns. This differentially private data can then be encrypted and processed using homomorphic encryption[8]. This allows CDN systems to perform complex optimization computations—such as cache placement algorithms and performance analysis—directly on the encrypted payload.

User-controlled location disclosure offers another approach to reconciling the tension between sensitive data protection and legitimate geo-blocking requirements. The IP Geolocation HTTP Client Hint specification enables browsers to voluntarily provide location information to servers through standardized HTTP headers, shifting control from passive server-side inference to explicit user consent. This approach allows users to specify the granularity of location information shared with different services - providing country-level data for content compliance or more precise location data for generating a local weather report.

Conclusion

Apple's experience in operating global CDN infrastructure while maintaining strict data-protection standards demonstrates that high-performance content delivery and user privacy protection are not mutually exclusive. CDN providers can achieve optimal service delivery without compromising user location data while still meeting legitimate geo-blocking requirements. This can be accomplished by reducing reliance on geo-IP through techniques like Service Binding DNS records and network performance characteristics, implementing differential privacy for aggregate insights, and leveraging user-controlled location disclosure.

The industry has an opportunity to move beyond the usual geo-IP approaches toward privacy-first CDN architectures that respect user data while maintaining the performance expectations of modern internet services. Commitment to this transition, combined with open collaboration on standards and technologies, can drive industry-wide adoption of privacy-preserving CDN solutions. Migrating from explicit server-side inference based solely on geo-IP will be challenging on many fronts because it requires modifications to both the server's service advertisement and the client-side decision process[9]. The path forward will require coordinated standardization efforts, with industry leaders contributing real-world experience and technical expertise to create robust, interoperable standards for the next generation of safe and high-performance internet infrastructure.

[8]Fan, J. and Vercauteren, F. "Somewhat Practical Fully Homomorphic Encryption," IACR Cryptology ePrint Archive, 2012.

[9]J. Zirngibl, P. Sattler, G. Carle. 2023. A First Look at SVCB and HTTPS DNS Resource Records in the Wild. International Workshop on Traffic Measurements for Cybersecurity 2023. WTMC.