IP Geolocation is Critical for Compliance

Richard Barnes <rlb@ipv.sx>

There are an increasing number of legal requests for operators of Internet applications to change their behavior. For example:

- Several jurisdictions have imposed age-based restrictions on content availability. For example, a law in the US state of Mississippi requires operators of websites that allow user-generated content to implement age verification and block access for users under the age of 18. In response, the Bluesky social network disabled service in Mississippi.
- DNS resolver operators regularly receive demands to block certain domains. In 2024, a court in France ordered major DNS resolver operators to block certain sports streaming sites. In response, Google blocked the sites in question, and OpenDNS disabled service in France entirely.
- Recent revisions to the German telecommunications law require operators of telecommunications service to provide lawful intercept capabilities. The definition of telecommunications services explicitly includes number-independent interpersonal communications services, i.e., over-the-top services.

Because these changes are business- and rights-impacting, operators want to scope their compliance narrowly, only implementing changes for users in affected jurisdictions. Some legal requirements even have geographical boundaries. For example, German regulation that governs lawful intercept explicitly requires that if the targeted endpoint is outside of Germany, then communications must not be intercepted unless the targeted endpoint is communicating with a party in Germany.

The privacy and openness properties of certain applications exacerbate this problem. In many applications, an end user can connect to the application anonymously, with no account or profile information. In such situations, a server doesn't know anything about a connected endpoint other than its IP address and any other observable factors, e.g., latency to measurement points. In these situations, compliance decisions still need to be made.

The combination of geographically-scoped compliance requirements and private service access mean that IP-based geolocation results have important real-world impacts — not just whether the user gets content in the wrong language or the wrong ads but whether the user can even access the content they need to or be secure in their communications.