Workgroup: HTTPBIS
Internet-Draft:
draft-pauly-httpbis-geoip-hint-02
Published: 30 September 2025
Intended Status: Experimental
Expires: 3 April 2026
Authors: T. Pauly
Apple Inc.
D. Schinazi
Google LLC
C. McMullin
Google LLC
D. Mitchell
Google LLC

The IP Geolocation HTTP Client Hint

Abstract

Techniques that improve user privacy by hiding original client IP addresses, such as VPNs and proxies, have faced challenges with server that rely on IP addresses to determine client location. Maintaining a geographically relevant user experience requires large pools of IP addresses, which can be costly. Additionally, users often receive inaccurate geolocation results because servers rely on geo-IP feeds that can be outdated. To address these challenges, we can allow HTTP clients to actively send their network geolocation to an HTTP server via an HTTP header field. This approach will not only enhance geolocation accuracy and reduce IP costs, but it also gives clients more transparency regarding their perceived geolocation. This is also particularly useful in the case of HTTP intermediaries that hide client IP addresses, such as Oblivious HTTP (OHTTP) relays.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://tfpauly.github.io/privacy-proxy/#go.draft-pauly-httpbis-geoip-hint.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-pauly-httpbis-geoip-hint/.

Discussion of this document takes place on the HTTPBIS Working Group mailing list (mailto:ietf-http-wg@w3.org), which is archived at https://lists.w3.org/Archives/Public/ietf-http-wg/.

Source for this draft and an issue tracker can be found at https://github.com/tfpauly/privacy-proxy.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 3 April 2026.

Copyright Notice

Table of Contents

1. Introduction
  1.1. Requirements
2. IP Geo Header
3. Client Behavior
4. Server Behavior
5. Security Considerations
6. Privacy Considerations
7. IANA Considerations
  7.1. HTTP Headers
8. References
  8.1. Normative References
  8.2. Informative References
Authors' Addresses

1. Introduction

This document defines an HTTP header field that can be used to send a geolocation entry based on the client's determined location. This location can be used to influence server behavior, such as by causing the server to return responses relevant to the client's location. The format of the geolocation hint is the same as that defined for IP geolocation feeds in [GEOFEED]. It only allows for coarse-level location specification.

This header aims to provide rough geolocation hints to servers based on the client’s network location, shifting geolocation from a passive IP-based approach to an active client-controlled one. This not only allows the client to influence how their location is interpreted, but it also reduces the need for extensive IP address pools when clients

mask their IP addresses through VPNs or proxies. Typically, VPN or proxy providers need to manage egress IPs for each region to maintain accurate geolocation. With a client-provided location hint, the hint can minimize the number of IP addresses needed while still supporting location-specific content such as weather, local news, and search results. In addition, the hint reduces most servers' reliance on geo-IP feeds that often come with limitations such as outdated IP-to-location mappings and ongoing maintenance costs.

Due to the inherent privacy risks in sharing location data, this mechanism is not designed for general-purpose use, and is instead defined for specific scenarios where the client's IP address is hidden from an HTTP server and the sharing of coarse information is deemed appropriate. As an example, OHTTP relays [OHTTP] are designed to hide the client's IP address from OHTTP gateways and targets, but they may wish to reveal some level of coarse information about the client's location to the gateway and target. For example, there are cases where regulation requires the target to know which country the client appears to be in. This can be accomplished today by using a different IP address on the HTTP connection from relay to gateway, and encoding the location in a geolocation feed. Alternative, this document describes a way to encode the coarse location in the HTTP request headers instead.

The geolocation of the client is determined via a geo-IP database lookup of the client's IP address.

1.1. Requirements

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. IP Geo Header

The "Sec-CH-IP-Geo" is an Item Structured Field [STRUCTURED-FIELDS]. The field's value is a String. The string uses the format defined in Section 2.1.1 of [GEOFEED], with the IP Prefix element removed. Thus, this contains a comma-separated list of Alpha2code, Region, and City. The value SHOULD NOT contain a Postal Code.

For example, the header for an entry "192.0.2.5,US,US-AL,Alabaster" would be:

```
Sec-CH-IP-Geo = "US,US-AL,Alabaster"
```

Given that the Sec-CH-IP-Geo is a high-entropy client hint (i.e., a client hint that is not in the low-entropy hint table), the server needs to explicitly opt-in in order to receive the Geo Client Hint as defined in [RFC8942]. It will not be sent by default and the server

MAY indicate support for this hint via the Accept-CH header in the initial response:

```
Accept-CH: Sec-CH-IP-Geo
```

Servers SHOULD indicate for any cacheable content if the geo hints will influence the cached content, using the 'Vary' header. This will indicate that the server may have used this header as a determining factor when choosing a response:

```
Vary: Sec-CH-IP-Geo
```

3. Client Behavior

The client MUST determine geolocation using a cooperating server that looks up the client's IP address in a geo-IP database. The client MUST NOT use GPS. The client hint value MUST NOT be more precise or detailed than what can be inferred from the user’s IP address. When the client is routing traffic through a proxy or a VPN, the IP address used to generate this geolocation hint MUST be an address that is presented upstream beyond the proxy or VPN (in other words, the "egress IP address"). The proxy or VPN's selection of this egress IP address MAY have been based on the client's original un-proxied IP address, but any hints that the client presents to servers beyond a proxy or VPN MUST NOT reveal more geolocation information that would be possible to determine from looking up information about the egress IP address itself.

The client MAY include the client hint header in requests to the server after the server has explicitly opted in to receiving the hint, or if the client knows of specific server configurations, such as proxy settings, that support including the hint.

4. Server Behavior

Upon receiving a Geolocation Client Hint, a server can use the information to influence its behavior in various ways, such as determining the content of HTTP responses.

Servers can choose to use the hint value in one of several ways, including:

* Using the client hint information instead of consulting IP-based geolocation feeds.

* Recognizing a mismatch between the client hint information and the server's current result from its IP-based geolocation feed as a reason to schedule an automatic refresh of its geolocation feed information. This can help ensure that changes to feeds are adopted quickly, improving results for clients that don't send the client hint.

* Serving content that corresponds to the client's indicated location, including delivering region-specific news, weather forecasts, and relevant advertisements.

The server MUST be able to handle situations where geolocation is not provided in a request. Since not all web clients will send a Geolocation Client Hint, the server MAY defer to alternative methods such as IP-based geolocation feeds to provide said value.

5. Security Considerations

Servers MUST NOT use Geolocation Client Hints for security or access-control decisions, as the value is provided by the client without additional authentication or verification. Servers that offer services restricted to clients in a specific country or administrative region might already rely on geoIP databases to determine the client's location for access control purposes. However, the Geolocation Client Hint can be used to customize responses based on where the client claims to be within that restricted region.

6. Privacy Considerations

Any value provided in this hint MUST NOT be more specific than the information that could be obtained from the client's IP address and a well-maintained map of IP ranges to locations. In particular, when a privacy technology such as a VPN is in use, the value MUST NOT reveal information about the user's location that would otherwise be hidden.

To prevent disclosing private information, this value cannot be based on other sources of geolocation data, such as GPS or physical latitude and longitude coordinates. Providing overly precise location information could expose sensitive user information especially when combined with other identifiable signals. Furthermore, when a client designates a location different from that derived from their IP address, the combination of designated location and IP can create a unique identifier, increasing the risk of cross-site tracking.

The hint MUST NOT be sent by default or in an always-on manner. It should only be included in response to explicit server requests (e.g., via the Accept-CH header) and in contexts where sharing location data serves a clear purpose, such as for location-based services.

7. IANA Considerations

7.1. HTTP Headers

This document registers the "Sec-CH-IP-Geo" header in the "Permanent Message Header Field Names" registry <https://www.iana.org/assignments/message-headers>.

Header Field Name	Protocol	Status	Reference
Sec-CH-IP-Geo	http	exp	This document

8. References

8.1. Normative References

[GEOFEED] Kline, E., Duleba, K., Szamonek, Z., Moser, S., and W. Kumari, "A Format for Self-Published IP Geolocation Feeds", RFC 8805, DOI 10.17487/RFC8805, August 2020, <https://www.rfc-editor.org/rfc/rfc8805>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC8942] Grigorik, I. and Y. Weiss, "HTTP Client Hints", RFC 8942, DOI 10.17487/RFC8942, February 2021, <https://www.rfc-editor.org/rfc/rfc8942>.

[STRUCTURED-FIELDS] Nottingham, M. and P. Kamp, "Structured Field Values for HTTP", RFC 8941, DOI 10.17487/RFC8941, February 2021, <https://www.rfc-editor.org/rfc/rfc8941>.

8.2. Informative References

[OHTTP] Thomson, M. and C. A. Wood, "Oblivious HTTP", RFC 9458, DOI 10.17487/RFC9458, January 2024, <https://www.rfc-editor.org/rfc/rfc9458>.

Authors' Addresses

Tommy Pauly
Apple Inc.
One Apple Park Way
Cupertino, California 95014,
United States of America

Email: tpauly@apple.com

David Schinazi
Google LLC

Email: dschinazi.ietf@gmail.com

Ciara McMullin
Google LLC

Email: ciaramcmullin@google.com

Dustin Mitchell
Google LLC

Email: djmitche@gmail.com