# Cornell University Library (CUL) Browser IP Obfuscation Task Team
# Recommendation Report

January 2024

## Background

Internet privacy and the ability to access electronic resources safely and reliably are fundamental concerns for libraries and their users. In 2024, a significant change is anticipated in the form of a new browser IP obfuscation setting. The setting aims to enhance user privacy by obfuscating their true IP addresses by transparently routing queries for online content through secure proxies. While this may benefit user privacy, it also raises important questions about its impact on libraries and their ability to provide access to electronic resources efficiently, given our reliance on IP-based authentication in licensing.

## Committee Charge

The Browser IP Obfuscation Task Team is charged by AUL Simeon Warner.

1. **Research and Assessment:**
    - Investigate and assess the implications of the new browser IP obfuscation setting on library services, including but not limited to:
        - User authentication processes
        - The impact on patrons' ability to access electronic resources seamlessly
2. **Privacy Considerations:**
    - Examine the potential impact of IP obfuscation on library patron privacy
    - Explore how the Library can promote patron data privacy while adapting to this setting
3. **Technical Implications:**
    - Understand the technical changes required to adapt to the new setting
    - Identify potential challenges and opportunities in implementing this technology in public computing
4. **Vendor Relations:**
    - Investigate the stance and readiness of resource vendors and publishers in response to this change
5. **Recommendations:**
    - Provide a set of recommendations for consideration to effectively adapt to the new browser IP obfuscation setting, ensuring the balance between privacy and access
    - Propose strategies for library advocacy to protect the interests of library users in this evolving landscape

## The Committee:

- Adam Chandler, co-chair
- Debra Howell, co-chair
- Pete Stergion, CUL IT
- Peter McCracken, LTS
- Amy Blumenthal, CUL IT
- Jim Morris-Knower, Public Services
- Erica Johns, eCommons

## Overview of Concerns

Companies like Apple (Safari browser), Google (Chrome browser) and Mozilla (Firefox browser) are responding to various policies and regulations like the General Data Protection Regulation (GDPR) and others around the world regarding the protection of user privacy. These policies and regulations impact some of the possible ways an individual may be tracked across the web, including via their IP address and through “cookie” information written into the browser’s local storage. Within the academic publishing industry, users’ IP addresses are leveraged as a common means for authorizing access to scholarly resources.[1] While IP obfuscation enhances user privacy, it could significantly impact library services that rely on IP authentication, particularly in the following areas:

1. eCommons Access:

    - Some eCommons users may be unable to verify their eligibility based on their IP address, hindering access to subscribed resources.
        - If a visiting scholar, without a NetID, is working on a personal computer on campus and using a public Cornell network for their internet service, previously they would have been granted access to “Cornell-only” collections in eCommons based on their IP range. This is in keeping with our land grant mission. Now, without a NetID to login to shibboleth, and the obfuscation of their IP range, they will be unable to access Cornell-only materials. They will need to use a public computer to browse the entirety of the eCommons collections or temporarily opt-out of IP obfuscation on their personal computer.

2. Public Computing:

    - Our IP based authentication licensing includes library space IP address ranges. Our CUL public computers are intentionally setup not to require a campus NetID to use them. Coupled together, these practices permit community members to access licensed resources. It also offers a tracking-free computing environment for scholars researching sensitive topics.

3. EXProxy Access:
    - EZProxy is the application used by the Library for off-campus authentication to library resources.
    - OCLC, the company behind EZProxy, has been actively involved in discussions with browser developers regarding IP obfuscation. They remain committed to supporting libraries and ensuring continued access to scholarly resources. Here's what OCLC says:
        - "[OCLC] has been very involved in the upcoming browser changes related to authentication and IP addresses. As an advocate for libraries and scholarly resources, [OCLC] will continue to work with browser developers like Google and others."

[1] A good primer on library authentication and authorization is the whitepaper written by Sunshine Carter and Cody Hanson in 2022: http://publish.illinois.edu/licensingprivacy/files/2022/06/Electronic-Resource-Authentication-and-Authorization.pdf

- "[EZProxy] remains the leading access method to connect users to e-content and keeps libraries in control of their data. [OCLC] will continue to support IP proxying via [EZProxy] for the foreseeable future."

4. Vendor Support and Alternative Authentication:

   - There is an emerging trend for publishers and vendors moving away from IP-based authentication to SAML-based solutions. SAML is “Security Assertion Markup Language,” an open standard that allows identity providers (IdP) to pass authorization credentials to service providers (SP). When offered by a vendor, this means that users can employ their Cornell campus single-sign on credentials to log into many different websites without first starting in a library website such as the catalog.
   - CUL has privacy concerns regarding SAML-based solutions as outlined in a white paper titled, “Improving Off-Campus Access to Electronic Resources” by Peter McCracken, Jesse Koennecke, Adam Chandler, Amy Blumenthal, Phil Robinson, Jerry Shipman (CIT) (August 30, 2019). Therefore, CUL should monitor the emerging trends but not make any sudden changes in authentication. It is worth noting that the roll-out of IP obfuscations may accelerate the move to SAML solutions, because vendors may find that IP authentication no longer meets their users’ needs. Thusly, we need to work in this space with other libraries to address privacy concerns within SAML.

**Task Team Recommendations**

- **Acknowledge the change in the use of EZProxy.**
  - The upcoming browser changes will not affect the core functionality of EZProxy. EZProxy will still be able to connect users to e-content regardless of whether their browser IP address is masked.
  - Currently EZProxy authentication is only required for off-campus connections. Post-IP obfuscation, EZProxy will be used for on-campus connections, as well.
- **Opt Out of IP Obfuscation for public computers.** This will allow for continuation of anonymous access to our resources.
- **Communicate with Patrons and Staff:** Develop clear communication strategies to inform patrons about potential access issues and train staff on handling related queries.
  - We recommend working with Library Communications to develop messaging for patrons.
  - We recommend creating a LibGuide for staff reference.
  - We recommend involving liaisons in this communication plan to academic departments and units.
  - Update the Public Computing Privacy web page with details.
  - Note: it is important that we consider multiple paths of communication (ie: a banner on the web site, directions to LibGuide, etc)
- **Stay Informed:** Follow developments in browser IP obfuscation and updates from the global library community, browser developers, library resource vendors, and EZProxy.
  - We recommend sending at least one person from CUL to the InCommon TechEx conference

**Resources:**

- Google Chrome IP Protection: https://www.nytimes.com/2022/02/16/technology/google-android-privacy.html
- ALA Federated Authentication Committee: https://www.ala.org/rusa/strategic-priorities/access
- Ezproxy Information on Browser Privacy Features: https://help.oclc.org/Library_Management/EZproxy/Troubleshooting/Will_EZproxy_be_supported_with_the_planned_browser_privacy_features_being_introduced_by_Google_and_others
- Seamless Access: https://seamlessaccess.org/

====================================

**Browser Specific Information Breakdowns:**

**Chrome IP Obfuscation:**

Google Chrome announced plans for IP obfuscation in 2024, calling it "IP Protection." It's currently in an early testing phase and not yet available to the public.
**Details:**

- **Opt-in feature:** Users can control whether to activate IP obfuscation. Enterprise level controls on the roadmap.
- **Phased rollout:**
  - Phase 0 (current): Google proxies requests to its own domains, available only in the US.
  - Future phases: Two-hop approach for improved privacy through external proxies.
- **Functionality:** Chrome routes website requests through proxy servers, hiding the user's actual IP address from the visited website.
- **Purpose:** Enhance user privacy by preventing websites from directly identifying users through their IP address.

**Safari, Firefox, and Edge:**

**Safari:**

- iCloud Private Relay, offered as part of iCloud+, already obfuscates IP addresses for Safari users on Apple devices.

**Firefox:**

- No official announcements about implementing IP obfuscation like Chrome or Safari.
- Focuses on alternative privacy features like blocking third-party trackers and fingerprinting techniques.

**Edge:**

- No official announcements about IP obfuscation either.
- Integrates with Microsoft Defender for Browsing, which blocks malicious websites and trackers, but doesn't explicitly hide IP addresses.

**Overall:**

- Chrome is leading the charge with its IP Protection feature, currently in testing.
- Safari offers IP obfuscation through iCloud Private Relay, but only for Apple users.
- Firefox and Edge prioritize other privacy features, though future plans for IP obfuscation are unknown.

**Additional Research:**

- Google Chrome Blog: https://support.google.com/blogger/answer/6284029?hl=en
- Google IP Protection: https://github.com/GoogleChrome/ip-protection/issues
- Apple iCloud Private Relay: https://support.apple.com/en-us/102602
- Mozilla Privacy Blog: https://blog.mozilla.org/en/category/privacy-security/
- Microsoft Edge Security Whitepaper: https://learn.microsoft.com/en-us/deployedge/ms-edge-security-for-business