The Browsers Are A'Changing: Lessons from the Aftermath (?) of Browser Changes

Michelle Elaine Colquitt

Abstract

Internet browser companies are implementing changes in their products as a result of strict laws and regulations in the European Union (EU). Building on previous panel discussions presented at the 2023 Core Forum and Charleston Conference, my goal was to have a lively discussion about the basics of browser changes, focusing on why and what has changed, specifically over the last quarter or two. I sought and provided real-world examples of messaging and workflow changes, specifically from public-facing personnel at smaller libraries. Although I am an active member of the American Library Association's Authorization and Access Committee and this work was built off information created in the scope of that committee, this presentation was tailored for a NASIG audience, specifically focusing on the *Core Competencies for Electronic Resources Librarians.* One of my main aims was for the electronic resources management community to know that we are weathering changes together and to build a resource network of like-minded professionals so we can successfully navigate the impending browser changes.

Keywords: browsers, electronic resources, *Core Competencies for Electronic Resources Librarians*, third-party cookies, IP obfuscation, link decoration

https://doi.org/10.3998/nasig.7744

NASIG *Core Competencies for Electronic Resources Librarians*

When pondering the topic of impending browser changes, I found that it was important to frame my thoughts around this topic in the context of the NASIG *Core Competencies for Electronic Resources Librarians*, specifically Competency Two, Technology. This Competency states that the Electronic Resources Librarian's "depth of knowledge far surpasses the generalists' knowledge of technology."[1] Given our surpassing knowledge of technology, it is important for those of us who work with electronic resources on a regular basis to have a foundational knowledge of authentication and access to electronic resources.

It is also essential for us to understand authentication and the impact of browser changes in terms of the lifecycle of electronic resources, mainly regarding licensing (1.2) and information organization (1.3). In section 2.3, the *Core Competencies* further call for a "conceptual and practical knowledge of standards, protocols, and structures, such as . . .Central authentication services (Shibboleth) and EZproxy."[2] Shibboleth, according to its own documentation, is "one of the most widely used identity management systems in the world. After emerging as an Internet2 middleware activity in 2000, it was quickly adopted by academic institutions, identity federations, and commercial organisations all over the world."[3] The other mentioned technology is EZproxy, which according to parent organization OCLC, "was built to advance the crucial role libraries play in protecting patron privacy and influencing learning outcomes, making it a trusted e-resource access and authentication solution. Thousands of libraries in over 100 countries use EZproxy to facilitate secure, reliable access to e-resources."[4] Regardless of what solution the electronic resources librarian's library uses, it is critically important that they become familiar with the basics of authentication so that they can relate these scenarios to provide high-quality customer service experiences both internally to their colleagues and externally to their patrons.

Authentication Background and Definitions

As a practical example of authentication, consider the late, great Meanie Lenie's (aka Jolene's) journey to log into her library's electronic resources. Lenie (pictured in Figure 1) had a bad attitude about electronic resources, and life in general. Her shelter name was Barbara Stripesand, if that gives you any indication of her personality.

In order to understand Lenie's journey navigating the internet, we need to have a working understanding of access and authentication in the context of web browsers. Cookie technology is at the essence of understanding access and authentication. I am sure that we all have our favorite cookies—Crumbl red velvet, I'm looking at you. The authentication related cookies are "a small piece of text that stores information about your interaction with a website."[5] Browser cookies have timeframes associated with them—either short-term, session

Figure 1. Meanie Lenie Navigates the Internet

cookies, or longer persistent cookies. These cookies contain personalization information, and possibly credential information, which, of course, is not recommended.[6]

Cookies are not limited solely to a resource provider who has only your authentication in mind. Some advertisers, for example, deposit third-party cookies into your browser. In the past, advertisers frequently did so without your knowledge. These cookies can provide customization down to the look and feel of the user's web browsing experience. These cookies can also be used for nefarious purposes to provide targeted advertising; this is the reason I receive advertisements for D&D Beyond when I am not the D&D player in my household.

Another aspect of authentication and access is IP address recognition. Defined simply: "IP address authentication is the method of identifying users requesting access to vendor databases. It uses an organization's outward facing IP addresses as a means to identify users coming from a subscribing institution and in turn authenticate access."[7] IP authentication is a stable and well-recognized method of ensuring appropriate access to electronic resources.

Now that we have more of an understanding about authentication, it is important to recognize that users must be authorized to access electronic resources. Licensed resources are often tremendously expensive, and publishers and vendors most often require libraries to agree to protect and secure these resources. Botyriute (2018) states "in the context of accessing digital resources online, authentication and authorisation may occur a number of times before users are presented with the content they are trying to access."[8] Based on the twin processes of authentication and authorization, we can also explore the concept of link decoration.

A concise definition outlines that "link decoration is a tracking mechanism wherein a parameter is added to a URL that allows a user to be tracked across different websites."[9] Another way to view the problem of link decoration is through the lens of privacy; Claburn (2023) states "the practice of appending data to the end of web links, has become more of a privacy problem than most people realize. The

data exfiltration practice is now widely used to send info associated with web users—including email addresses—to ad tracking firms."[10] Privacy is one of the major concerns when it comes to link decoration. However important privacy is, there are still ways in which users' movements can be tracked across the open web and when using electronic resources.

Meanie Lenie's Internet Journey

Now that we have the foundational knowledge of authentication and authorization, we can follow Meanie Lenie's journey across the internet. Meanie Lenie is searching for a topic for her five-page scholarly research paper. When she logs into the library's system, the provider puts a cookie on Lenie's browser to say that she is authorized to access content across multiple resources. This cookie could be a session cookie, or it could be one that is more persistent in nature. Cookies are used more than just for authentication and authorization; in this case, the cookie stored information about Lenie's preference for a larger, darker font. Cookies are used to note Lenie's demographic information, which can allow for targeted advertising and content.

When she was accessing this content, the link Lenie used contained link decoration that identified her with her institution, the fact that she was off-campus when she accessed this resource, and other demographic information. Link decorations have usually been known to contain numerical information about the institution. Munir et al. relate that "a URL is composed of the following key components: scheme, fully qualified domain name (FQDN), resource path, query parameters, and fragments."[11] With this outline, we can determine that the link decoration would more than likely fall in the query parameters area, which in ExLibris Alma's language are referred to as parser parameters. In ExLibris' documentation, "the Linking Parser Parameters contains variables for items such as Username, Password, Customer ID,

and Authentication details that may differ between institutes. These parameters are set by inputting the value at the Linking Parameter fields from the Linking tab of the Electronic Service Editor."[12] As someone who has been responsible for entering and managing parser parameters in the past, I feel as if I have more of a foundational understanding, after over five years of working with parser parameters. As an Alma user, in the past, I have found it difficult to understand the nature of parser parameters and what I should enter and where I should enter this information. I have found the documentation about parser parameters to be murky at best.

Cookies and link decoration can be used in conjunction with IP authentication to provide vendors with a variety of methods to track and learn more about specific users. Advertisers can use your IP address to present target geo-located ads. Additionally, the IP address can be combined with other system information to differentiate Lenie's profile from other people. This is what is known as "browser fingerprinting," which has been defined as "a technique used by websites to track users' online behavior. It allows websites to build up a profile of each user's interests and preferences, which can be used for business purposes."[13] A considerable amount of data is generated during the browser fingerprinting process, which can be used to reveal information about browsing, and can generate a "unique fingerprint that can be used to track the user's online activities."[14] Now that we recognize that users can be tracked while using electronic resources, it is also important to realize that patrons can be tracked for less than reputable, and even nefarious purposes.

After doing her research for her five-page paper, Lenie decided to search for some shoes. The various stores she visited online dropped cookies on her browser. When she checked out, clicking the Purchase link from her shopping cart, more cookies stored the size and items she looked at and decided to purchase. The cookie can remember what is in the shopping cart as well as how long she spent on the website. Website developers use the same link parameters to track your interactions and path across websites.

The Browsers Are A'Changing

In an age of heightened privacy practices, there are some problematic behaviors that need to be addressed. Harding, echoed by Griffey, outlined the browser change situation in terms of cookies by stating that "non-transparent uncontrollable tracking of users across the web needs to be addressed and prevented."[15] As a result of various privacy regulations in place in the European Union, browser vendors are making changes to the architecture of their browsers, specifically in terms of eliminating third-party cookies, enabling IP obfuscation, and eliminating link decoration, as outlined earlier. The American Library Association's Core Federated Authentication Committee compiled information about what browser vendors have said about the forthcoming changes. Committee members, including myself, compiled this information from Apple Safari, Google Chrome, and Mozilla Firefox.

Third-Party Cookies

Changes

Apple Safari, through the creation of their Intelligent Tracking Prevention (ITP) blocked third-party cookie tracking beginning in 2017. In fact, the user has to opt-in and enable third-party cookies. In 2019, Mozilla Firefox introduced Enhanced Tracking Protection (ETP), which blocks third-party cookies by default. Google initially stated that they would phase out third-party cookies in Chrome in the second half of 2024, which then became early 2025, and has again been changed. In a blog post dated July 22, 2024, Anthony Chavez, VP of Google's Privacy Sandbox, noted that the elimination of third-party cookies would require significant action on the part of publishers and advertisers, which "in light of this [amount of work], we are proposing an updated approach that elevates user choice. Instead of deprecating third-party cookies, we would introduce a new experience in Chrome

that lets people make an informed choice that applies across their web browsing, and they'd be able to adjust that choice at any time. We're discussing this new path with regulators, and will engage with the industry as we roll this out."[16]

Implications

The implications of blocking third-party cookies are that certain systems will likely still work for a while, while others would possibly break down or even be rendered obsolete. SAML authentication would possibly still work for one to three years. WAYF (where are you from?) IdP authentication will continue to work, but multiple or previous organizations will probably be forgotten. Services that share information between third parties using frames (Teams, ILS/LMS) will probably have mixed results due to the repeated and multiple issues with frames. OIDC (OpenID Connect), an authentication protocol, will likely break.

IP Obfuscation

Changes

Browser companies will support user privacy by enabling a user to obfuscate or mask their IP address. This happens presently when patrons use an Incognito or private browser session or a VPN (virtual private network). Although this is not moving as quickly as other changes, it is still important for libraries to be aware that IP addresses can be obfuscated, and this obfuscation might be out of control of the patron.

Implications

Cornell University has created robust documentation and recommendations about IP obfuscation. Their documentation outlines the IP obfuscation landscape as "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."[17] Another implication is that IP obfuscation could potentially impact the usage statistics associated with an institution as well as how libraries gather statistics. Ferrante, Hoeppner, and Griffey, at the 2023 Charleston Conference, related that the "Hide my IP" functionality, or IP obfuscation, disables on-site IP access. This is particularly important because library professionals cannot see the user's true IP address anymore, therefore, this can impact statistic gathering because it would be difficult to "see" if the user access resources on-campus or off-campus.[18]

Link Decoration

Changes

Tracking parameters, link decoration, and query strings will be blocked. There will also be certain aspects of URL parameters that will be disabled or blocked. OpenAthens relates that "if link decoration is completely disabled, this will break the world wide web, and therefore, it is very unlikely to happen. It is not clear what browsers have in mind at this point, but we are involved in conversations, and it is our hope that there would be a repository of either trusted sites (a [*sic*] allow list), or bad actors (blacklist) to mitigate the impact on library, academic and research products and services in this space."[19]

Implications

URLs can have parameters that are not specifically link decorations. Browser vendors have communicated that they plan to block known

tracking parameters. Vendors have shared examples of what will be blocked, enabling checking and testing. There are a lot of unknowns in this specific browser change realm.

Workflow Impacts and Communication Strategies

During this portion of the presentation, I asked some open-ended questions, hoping to prompt a thoughtful discussion. I created an anonymous Padlet (https://bit.ly/4c8kS02) for audience feedback about their institutions' responses to the upcoming browser changes. One respondent stated that although they are not in a public-facing role, their electronic resources librarian is closely monitoring the situation, and they are "adding SAML/Shibboleth as an optional authentication method with our major resource providers. This was already done for many of them during 2020 in response to the pandemic." Another anonymous participant stated that their institution does not make users coming from on-campus IP addresses log in; if they mask their IP addresses, they will lose this benefit.

My institution has fewer than five publicly available computers, and we encourage our users to bring their own devices. When our patrons do use one of the public computers, however, they must log in with their Clemson credentials. We do not have generic credentials available for public use. Another aspect of the Clemson browser change landscape is that our campus centralized Computing and Information Technology Division (CCIT) is responsible for an enterprise login solution. We have tried in the past to implement an authentication technology at the Libraries level, but they frowned on this software as a service. What the anonymous participant mentioned is very similar to what is currently happening at Clemson. We are discussing how to market the browser changes with a small group of cross-divisional stakeholders, including the Discovery Cross Functional Team. We believe that we will create an FAQ entry, possibly a blog post, to outline the browser changes.

When specifically asked, selected vendor representatives stated that they were preparing informal training for their teams. This is also in line with what the Discovery Cross Functional Team is exploring at Clemson University Libraries. We want our community to be as well-informed about the upcoming changes as they can be. During the presentation, I shared an example of a notification I received from Chrome in an infrequently used profile. Google's messaging contained information about how I could control my privacy and enhance my experience. I shared this as an example of what students could receive during their browsing experience.

Conclusions: Is This an Aftermath?

I very deliberately chose to subtitle my presentation "Lessons from the Aftermath(?) of Browser Changes." As of now, I am unsure that there will be the massive breakdown that others think might happen when browser changes are ultimately rolled out. Each browser vendor has carefully thought about their response to privacy regulations and the implications of specific changes upon their products. The issue I have reservations about is Google's VP's statement about the Privacy Sandbox, referenced above. I wonder what this will entail in the future, and this could impact my continued usage and reliance upon—and even recommendation of— Chrome for electronic resources.

Being as vendor-neutral as possible, I am pleased with the responses that have been provided to the American Library Association's Core Federated Authentication Committee. Each vendor representative who has provided information to the committee has been candid about what their companies are looking into, as well as candid about how their individual technologies should perform in response to browser vendor changes. It is important to remember that we are all navigating browser changes together in real time. We can easily call upon the greater NASIG community to provide assistance in navigating these challenging waters with grace, kindness, and empathy.

Acknowledgments

This content was adapted from and built upon panel presentations created by the American Library Association's Core Federated Authentication Committee. Specifically created by: Michelle Colquitt, Continuing Resources & Government Information Management Librarian (Interim eResources Coordinator) Clemson University Libraries, Hong Ma, Head of Library Systems, Interim Associate Dean for User Services, Loyola University Chicago, Justine Withers, Electronic Resources Librarian, and other members of the Core Federated Authentication Committee.

Contributor Notes

Michelle Elaine Colquitt is the Continuing Resources & Government Information Management Librarian and Interim eResources Coordinator at Clemson University, Clemson, SC, USA.

Notes

1 "NASIG Core Competencies for Electronic Resources Librarians," NASIG, last revised April 5, 2021, https://www.nasig.org/Competencies-Eresources.
2 Ibid.
3 "The Shibboleth Project," Shibboleth Consortium, last modified August 9, 2021, https://www.shibboleth.net/about-us/the-shibboleth-project/.
4 "EZproxy: Access and Authentication Software," OCLC, accessed January 16, 2025, https://www.oclc.org/en/ezproxy.html.
5 Kristina Botyriute, *Access to Online Resources: A Guide for the Modern Librarian* (Cham: Springer, 2018), https://doi.org/10.1007/978-3-319-73990-8.
6 Ibid., 12.
7 "What Is IP Authentication?" Library Help, Queen's University Belfast, last modified August 31, 2023, https://libraryhelp.qub.ac.uk/faq/46464#:~:text=IP%20address%20authentication%20is%20the,and%20in%20turn%20authenticate%20access.
8 Botyriute, *Access to Online Resources*, 18.

9 "New Privacy Features in Major Browsers and the Impact on Library Authentication," *EBSCOpost* (blog), EBSCO, May 14, 2024, https://www.ebsco.com/blogs/ebscopost/new-privacy-features-major-browsers-impact-library-authentication.
10 Thomas Claburn, "Online Tracking Is Alive and Well in Link Decoration," The Register, October 6, 2023, https://www.theregister.com/2023/10/06/link_tracking_privacy/.
11 Shaoor Munir et al. "PURL: Safe and Effective Sanitization of Link Decoration," arXiv, last revised March 6, 2024, https://doi.org/10.48550/arXiv.2308.03417.
12 "Best Practice Toolkit: Configuring Parser Parameters for e-Resources," Knowledge Center, Ex Libris, last modified November 9, 2023, https://knowledge.exlibrisgroup.com/Alma/Best_Practices_and_How-Tos/Resource_Management/Best_Practice_Toolkits/Best_Practice_Toolkit%3A_Configuring_Parser_Parameters_for_E-Resources.
13 Nupura Ughade, "What is Browser Fingerprinting?" Hyperverge, last modified August 21, 2024, https://hyperverge.co/blog/what-is-browser-fingerprinting/#:~:text=is%20browser%20fingerprinting%3F-,Browser%20fingerprinting%20is%20a%20technique%20used%20by%20websites%20to%20track,be%20used%20for%20business%20purposes.
14 Ibid.
15 Lauren Harding, "The Impact of Cookie Privacy Changes on Identity Services," Open Athens, last modified April 10, 2024, https://www.openathens.net/blog/the-impact-of-cookie-privacy-changes-on-identity-services/; Jason Griffey and Amanda Ferrante, "Browser Changes: What, When, and How to Prepare your Library's Authentication," August 24, 2023, https://fast.wistia.com/embed/medias/z4u2lyhc1c.
16 Anthony Chavez, "A New Path for Privacy Sandbox on the Web," The Privacy Sandbox, July 25, 2024, https://privacysandbox.com/news/privacy-sandbox-update/.
17 Debra Howell et al. "Cornell University Library (CUL) Browser IP Obfuscation Task Team Recommendation Report," eCommons, Cornell University Library, January 2024, https://hdl.handle.net/1813/114212.
18 Amanda Ferrante, Athena Hoeppner, and Jason Griffey, "Are You Ready for a Low Cookie Diet? What Browser Privacy Enhancements Mean for Libraries and Authentication" (presentation, 2023 Charleston Conference, Charleston, SC, November 9, 2023).
19 "Browser Changes FAQ," Open Athens, accessed January 16, 2025, https://www.openathens.net/faq/browser-changes-faq/.