Marisol Moreno Ortiz

Thinking about a thing called privacy

A reflection through example

Academic librarianship holds in its foundation and core values a very important task—protecting the privacy of everyone who enters the library space. In order "[f]or libraries to flourish as centers for uninhibited access to information, librarians must stand behind their users' right to privacy and freedom of inquiry."[1] Libraries provide access to information to individuals who do not have access to it at their homes. Libraries give people a choice about how to go about their information inquiries, and choice in libraries "requires both a varied selection and the assurance that one's choice is not monitored."[2] Protecting privacy has become a focus in recent years with the emergence of urbane technology and opportunity for greater surveillance. Because of this, privacy and surveillance literacy need to become a core part of information literacy instruction.

Online learning and privacy

As part of this focus, librarians must take time to analytically and critically evaluate online resources through a privacy lens, especially during the ongoing COVID-19 pandemic, with the continuation of remote learning, and the constant threat to privacy in the digital space. For instance, in a webinar hosted by the Scholarly Networks Security Initiative (SNSI), a group created by top academic publishers like Elsevier and Spring Nature, it was recommended to include "spyware into the proxy servers academic libraries use to allow access to their online services, such as publishers' databases" to prevent digital piracy of content by cyber criminals.[3] While academic librarians were involved in the online backlash against SNSI, this was done behind the scenes. It is equally important to include privacy and surveillance literacy in library instruction so students can also take steps to advocate for themselves while doing research online and know to reach out to us, their librarians, when they have concerns about a database or site with questionable data collection. But first, students need to know where to look to know the type of data online platforms are collecting about them.

As an example, I will look at the platform A Starting Point (ASP), that has gained popularity in social media with its creators working to bring it into the educational space. ASP has been marketed as a nonpartisan site that provides access to political information and has the potential to become a starting point of research for political science students and others looking for information about political issues. ASP was launched on July 14, 2020, by Chris Evans, Mark Kassen, and Joe Kiani, with the mission to connect American citizens with the law makers in their state through a video format.[4] This site is more significant than ever as politics and health information with regards to the pandemic continue to be a main focus in the media, which hopefully prompts students' desire to know more about issues that can affect them. As academic librarians, we must be ready to guide students to reputable sources that will help them with this endeavor. It is important to look closely at sites like ASP being promoted through the media to assist students with their information-seeking needs. Guiding students to understand evaluation and use of this and other digital sites must be provided to students because the "critical evaluation of information and its sources directly influence the efficiency and effectiveness of decisions human make about everyday life."[5]

As online learning continues during the pandemic, there emerges an increased danger of online resources that collect data without students knowing the depth of such collection. Some of these students are novices and/

Marisol Moreno Ortiz is reference and instruction librarian at Clark College, email: marisolmorenoortiz2@gmail.com

or members of the digital divide and may not be aware of using strategies to protect their privacy, like using "add-on tools that can block tracking technology."[6]

As an academic librarian, my responsibly is to evaluate and decide if resources like ASP should be recommended to students who are looking for information. As librarians, we earn the trust of our patrons, so we must do our diligence in evaluating the usefulness and credibility of sources that can be accessed by our patrons, especially for those who are new to research and digital sources. Looking beyond ASP's easy interface, which offers brief snippets of videos on various political topics, it remains brief with limited information. Students will still need to move to other search engines or databases to continue learning about those issues. This need to find additional sources increases the vulnerability of information seekers to be tracked through the cookies of the other sources during their research. It is crucial for students to know that ASP does not require them to log in to access the information it houses, but it will still collect personal data when users visit the site where the "[i]nformation necessary to use the [s]ervices"[7] is obtained. Yet, the services are not defined anywhere in the privacy policy of ASP, vagueness is concerning for user privacy because the site can collect any type of information that it wants but may not need to provide users with their service.

It is important for students to look at the privacy policy of this site and other online resources to know what "accepting cookies" really entails. The concern with ASP is more with unknown third parties with which the creators of the site are working as stated in the site's term of service, though no specifics or much detail is given on their identity.[8] This is more concerning as they state in their privacy policy that they might share the personal information of users with third parties, which they call their "'Service Providers'"[9] in order for them do their services. Though required to keep the personal information safe and confidential,[10] this is not a guarantee that they will, and we cannot trust this vagueness for the sake of our students. The third parties can also send cookies to users' computers,[11] and there is also no guarantee that they are not collecting their own data.

The only service provider that ASP mentions in its privacy policy is Google Analytics. They explain how the collection of data can include the ASP-accessed pages, including when and how many times accessed, browser information, Internet service provider used, and the user's operating system type.[12] Google Analytics monetizes its data with pseudonyms but "pseudonymity is quite fragile in protecting identity: discovering a user's identity *once* in a pseudonymous system is sufficient to also identify past and future interactions with the user."[13] Additionally, ASP will share "[p]ersonal [i]nformation in connection with a corporate reorganization or transaction, such as a divestiture, merger, consolidation, or asset sale, or in the unlikely event of bankruptcy."[14] Furthermore, in its terms of service, ASP includes an indemnity statement that those users who use the site "agree to defend, indemnify, and hold"[15] ASP and those that have affiliations with the site "harmless from and against all liabilities, losses, claims, damages, costs and expenses . . . arising out of"[16] using the site.

Obviously these are concerns for all students, but particularly for vulnerable populations, such as the "population of the community that frequently faces unnecessary surveillance and persecution, including groups such as racial and religious minorities, the queer community, journalists attempting to protect their sources, and political activists."[17] ASP will provide the personal information data collected to law and government agencies if they are required to do so by law.[18] Furthermore, ASP includes in its privacy policy that it has the right to disclose users' personal information if it is "necessary to take precautions against liability, to investigate and defend against any third-party claims or allegations, to assist government enforcement agencies, to protect the security or integrity of the Site or our services, or to protect the rights, property or personal safety of A Starting Point, its users, issuers, or others."[19] Even though users are included here, this does not provide confidence that users will be put first, unlike librarians and libraries who aim to place patron's digital safety first.

This is a concern because students do not often read, or even understand the necessity for them to read, the terms of service and privacy policy of sites before beginning their research—or before getting on the web to search for anything—as often their focus is on obtaining the information they need as fast as possible. They may have multiple tabs open and may be dealing with information overload and anxiety, as well. If a platform really wants to accomplish being open and simple for its users to connect with political parties and learn about the discussion going on in politics, it is paramount that it places a focus on privacy, instead of an easily missed link at the bottom of the site to explain what personal information they are giving away. The vagueness of third parties also brings into question whether the political parties are getting the personal information of users as they are helping the site provide the content to users. Even though ASP may not be providing user personal information, parties providing services, potentially including political parties, can send cookies to users and "may exploit a cross-site security vulnerability on a first-party website to learn the user's identity."[20]

Third parties are needed as their "services have tremendous value: they support free content and facilitate web innovation,"[21] where their "services bring tremendous value to the web: they enable first-party websites to trivially implement advertising, analytics, social network integration, and more."[22] But this is at the cost of them having the ability to "track a user's browsing activities across websites"[23] and collect data that the first-party (for instance ASP) would not be aware of, like their users "location, interests, purchases, employment status, sexual orientation, financial challenges, medical conditions, and more."[24] ASP, and other platforms with similar approaches to user data and privacy, leave users vulnerable to digital tracking and data collection without consent. This may not have been the intent of ASP's founders, but in order for academic librarians to feel confident in recommending resources to students, platform providers need to work on their privacy policy and terms of service, because if their "website is untrustworthy, users may decline to visit it."[25]

As librarians it is our duty to work to make sure that our students and other users assessing online resources know the risks they are taking with their personal information and the steps they can take to protect themselves. Nonetheless, students and other web users must balance a resource's benefit based on the reason they are vising the source. As an advocate for privacy in the academic library environment, I am more inclined to recommend other sources that make the user's privacy a priority.

Notes

[1] IFC Privacy Subcommittee, "Privacy and Confidentiality: Library Core Values," ALA, last modified on April 2017, accessed December 7, 2020, http://www.ala.org/advocacy/privacy/toolkit/corevalues.

[2] Ibid.

[3] Gautama Mehta, "Proposal to install spyware in university libraries to protect copyrights shocks academics," Authoritarian Tech, *Coda,* November 13, 2020, accessed December 7, 2020, https://www.codastory.com/authoritarian-tech/spyware-in-libraries/.

[4] Chris Evans, Mark Kassen, and Joe Kiani, A Starting Point, accessed July 16, 2020, https://www.astartingpoint.com/about.

[5] Muhammad Asif Naveed and Mumtaz Ali Anwar, "Towards Information Anxiety and Beyond," *Webology* 17, no. 1 (2020): 71, accessed July 18, 2020, http://www.webology.org/2020/v17n1/a208.pdf.

[6] Lauren Barack, "The Privacy Problem Safeguarding student data in schools and libraries," *School Library Journal* 63, no. 1 (January 2017): 40, accessed May 7, 2020, https://msi.ipublishcentral.com/pdfreader/school-library-journal-january-2017.

[7] "Privacy Policy," A Starting Point, last modified March 3, 2020, accessed July 17, 2020, https://www.astartingpoint.com/static/privacy.html.

[8] "Terms of Service," A Starting Point, last modified March 3, 2020, accessed July 17, 2020, https://www.astartingpoint.com/static/tos.html.

[9] "Privacy Policy," A Starting Point.

[10] Ibid.

[11] Ibid.

[12] Ibid.

[13] Jonathan R. Mayer and John C. Mitchell, "Third-Party Web Tracking: Policy and Technology," (paper presented at 2012 IEEE Symposium on Security and Privacy, San Francisco, CA, 2012), 415, accessed July 20, 2020, https://doi.org/10.1109/SP.2012.47.

[14] "Privacy Policy," A Starting Point.

[15] "Terms of Service," A Starting Point.

[16] Ibid.

[17] Emma Bayle et al., "Patron Privacy: Is the Tor Browser Right for Library Use?" *Computers in Libraries* 37, no. 6 (July/August 2017): 10, accessed May 7, 2020.

[18] "Privacy Policy," A Starting Point.

[19] Ibid.

[20] Mayer and Mitchell, "Third-Party Web Tracking," 416.

[21] Ibid., abstract, 413.

[22] Ibid., 413.

[23] Ibid., abstract.

[24] Ibid., 415.

[25] Ibid., 416.