Chinonso Oguh

Dr. Alex Poole

INFO 505

3 Dec. 2023

Research Essay: Evolving Privacy Policies in Libraries

When it comes to privacy, most people would argue that it is a good thing which keeps them safe from someone using personal information to exploit them. Yet there are still many situations in which people give up their information without thinking of the consequences. Most information professionals, including librarians, express some concern over this removal of the privacy barrier and work to restore it. It is necessary to uphold information privacy in libraries in order to allow patrons to retain their peace of mind and intellectual freedom, as well as keeping them safe from outside parties who would do them harm.

There are many obstacles librarians and libraries face when making sure their patrons' privacy is consistently upheld. Many libraries use third party vendors to offer up content to their patrons online, and these vendors do not always uphold the same privacy policies as the organization they work with. As social media becomes more present and asks for more information from its users there is also the chance some people don't even notice how much of their private information without their consent. Then there is the issue of cybersecurity which is "a form of information security," and whether or not librarians have the ability to thoroughly train patrons on privacy vulnerability (Givens). Unfortunately, lack of funding in libraries can lead to lack of cybersecurity as administration might choose to support a different function of the library. However, libraries and librarians should take on the responsibility of helping their

patrons as a major priority and establish trust between libraries and communities that allow patrons to hold onto their intellectual freedom with fear of exposure or exploitation.

With the growth of the internet and online resources, many libraries these days offer up online libraries which a patron can access remotely using through third party vendors. In the article, “Library Patron Privacy in Jeopardy an Analysis of the Privacy Policies of Digital Content Vendors,” vendors are defined as providing “contractual relationships to provide certain services” in the form of online material to libraries (Lambert et al.). While it might seem like an amazing deal on the surface these vendors can actually cause huge problems with the safety of patron information, because unlike libraries they do not usually have patrons best interest at heart. As Lambert et al. continue in their article, they outline the process of how an e-book would be checked out by a patron and the various organizations a person would come into contact with listing “the library, the service vendor, and the e-reader company” all of which would now have access to at least some extent of that patron’s information. While libraries typically have extensive privacy policies to protect patrons, many of these vendors have less detailed privacy policies which could leave unsuspecting patrons vulnerable. On using third party websites and sharing information previously given in confidence to the library, Sujoy Chatterjee said: “these exchanges of personal information are not inherently problematic as long as there are steps taken to protect patron privacy”. This puts into question whether or not it should be the responsibility of the library, vendor, patron, or a mix to decide how the patron is collected, how, and what is done with it in order to make sure these users stay protected.

Furthermore, no one quite knows what can be done with these third party organizations having access to the private information of these patrons and the results could be disastrous. In the Clark Hunt et al. article, “E-resource Librarians Perceptions on Library Patron Privacy” the

primary focus is on how information is spread online and how it could be sold to a third party vendor in use of targeted ads and tracking a patron even when it would seem the information is actually being obscured. There is a fine line with how much information can be given out to these vendors and many organizations could be in violation of privacy laws, such as FERPA in the case of an academic institution, because of this informational release. Unfortunately, "many librarians are unaware of the extent to which their vendors violate the privacy of their patrons" and do not always have the resources to confront these vendors head on (Farkas qtd. Clark Hunt, et al). Patrons go into libraries and associated vendors expecting there to be a privacy agreement in their favor. No one should be able to access their private information without their permission, however, if libraries aren't capable of handling that it leaves them and their information vulnerable.

In relation with third party vendors is the rise of social media, and, more specifically, how they approach the privacy of their users. In Michael Zimmer's article, "Librarians' Attitudes Regarding Information and Internet Privacy" he reports findings from a survey measuring librarians' views on privacy rights and protecting library users' privacy. One thing Zimmer talks about is how social media affects how privacy is viewed with libraries as they have to face "possible shifts in the social norms about privacy" as these sites become more prevalent amongst library patrons. Many libraries offer access to public computers which their patrons are allowed to use as long as they follow the libraries' policies and there are measures in place to protect patron information from being accessed after they have logged off the computers. However, shifts in social norms about privacy lead to a more casual approach to online sources outside of the library's control, and since "search engines and social media are not protectors of personal information" could compromise work done by libraries to protect patrons (Tsompanakis). For

some people social media's request for information no longer bothers them making the idea of maintaining privacy feel like less of an issue. What they often don't realize is how spreading information on social media could compromise an organization like a library. This unmanaged release of information opens up users to "security threats posed by malware and hackers" which can affect not only the patrons directly involved, but others as well when they use public computers (Givens). The results of Zimmer's survey show a growing concern for companies collecting too much information on individuals. While the majority of librarians still agree libraries have a responsibility to educate the public on privacy issues the percentage dropped from 92% to 77% between 2008 and 2012. One has to wonder if these changes in numbers mean people are less bothered or becoming less sensitized to private information getting out due to how people are often asked to give out information online, particularly by social media sites. When it comes to addressing these issues, it should be the work of information professionals to help patrons with "cybersecurity efforts and educating [them] about information security" (Givens). In doing this, information professionals help to improve the protect of personal information in public and private allowing users to feel safe wherever they go.

Now when it comes to librarians helping to protect their patrons' privacy, there are many steps one should consider. As Edward M. Corrado states in his article, librarians should "take steps behind the scenes to protect personal information" as it will help both librarians and patrons understand cybersecurity and how it can be used to protect them. Taking responsibility is huge as it maximizes the sense of security people want to feel and helps them to better their safety and the safety of others around them. No one wants to lose out on their piece of mind or access to intellectual freedom. They definitely do not want anyone to exploit their private information as they utilize a public service. A problem patrons face is data mining, which is a

practice of analyzing information within a database to uncover new information. This act could require direct access to an individual's personal and private information. As Tsompanakis points out, that despite any positive outcomes "these technologies can be used to harm" a person and protection should be required. It is important for any information professional to understand data mining and its positive and negatives in order to know how it is being used and how it will affect them, especially if it is pulling up information it has no right to access. As Zimmer's survey showed, most "librarians and information professionals possess a concern over privacy" and how that affects patrons. This shows librarians cannot just sit by while patrons are threatened by privacy issues and instead must work to "ensure awareness and practices are consistent" (Zimmer). Qiana Johnson talks about privacy policies and how libraries should be aware of what information is being collected from their patrons, especially those by third party websites and vendors. Librarians should make sure there is an ability for patrons to opt-out of information sharing when possible, and they should educate their patrons any available privacy policies.

Furthermore, when it comes to privacy policies, both librarians and patrons need to be aware of the aspects which they cover. As stated by the American Library Association (ALA), when crafting policies "libraries should consult with legal counsel before abridging any user's right to privacy" to make sure they are meeting the necessary requirements. As a patron, people expect libraries to keep their information private and with accordance to the ALA Library Bill of Rights, however, there are so many details and steps involved with an organization crafting its privacy policy. The article "Preserving Patron Privacy in the 21st Century Academic Library" by Nichols Hess et al. talks about the need to develop a privacy policy and what steps one would have to go through in order to achieve that. The policy must meet patron expectations, legal requirements, response to internal issues, and compliance with any broader institution the library

is a part of. This is especially a problem with university libraries who struggle to come up with "distinct privacy policies separate from that of their parent institution" (Nichols Hess et al). This makes their privacy policies less stable and liable to being exploited with this harder to define policy that doesn't always put patrons first. First it is important to understand why a library would need all of this private information from its patrons. A clear privacy policy would include patron focused language and how this information is being "collected, retained, used, disclosed, stored and ultimately disposed of" (Chatterjee). Of course, these policies need to keep updating and growing to order to continue protecting patrons as technology changes. Zimmer mentions how libraries use limited tracking, temporary data holding, and anonymous searches throughout their system in order to make sure no one has more access than they necessary to patrons' information stating it a "cornerstone of… librarian ethics". In the end, patrons should always be made aware of what is going on with their information and get to decide how their information is used. As Clark Hunt et al. discuss it wouldn't do be safe if the library director or library board are the only people involved with how this information is used. As Nichols Hess et al. continue they point out how "library technology has evolved" and there are more places a patrons' information might be listed. This goes to show how privacy concerns are not stagnant and one's approach to them should not be either and everyone should be involved in the privacy protection game.

When it comes to privacy concerns, people should really be paying special attention to cybersecurity. Now for libraries, the existence of good cybersecurity could make or break how they are able to provide for patrons and keep them confident in the organization. Unlike with Zimmer's survey which found the numbers of librarians who found it their responsibility to educate the public dropping, Givens argues "individuals need training" and talks about important the role of librarians have in "educating others about information security". Although Zimmer's

survey might show the reactions of librarians becoming less severe on educating others on cybersecurity, learning information improves lives across the board. It is an important for any information professional to offer assistance where they can to “can improve privacy and security decision-making” of everyone involved (Givens). Because even if people believe they don’t have an obligation to help, those with knowledge about these privacy protections topics should want to improve our privacy protection at every level leading to wide change and better protection for everyone. Without cybersecurity everyone becomes at risk from patrons to library staff. All of their information is exposed to the world and people could be exploited and taken advantage of which is why cybersecurity in necessary to ensure information privacy in online environments” (Givens). Considering the information people give to libraries wouldn’t they expect that the libraries would have a level of cybersecurity that work to protect their patrons. Not only do data breaches put people’s personal information at risk, but they are also wildly expensive to sort out afterwards. Corrado encourages libraries to consider cybersecurity insurance and making their staff understand how their cybersecurity helps and how to explain it to others to protect the best interests of everyone.

As it turns out money, or lack thereof, can have a large impact on how well a library’s information is protected both internally and from outside sources. As Clark Hunt et al., mentions in their article how librarians face an ethical question “considering budget cuts and environmental pressures” which may have them rethinking their code of ethics in order to ensure the existence of the library. It fascinating to consider the way library ethics would be tied to budget restrictions in whether libraries would even have enough funding to provide proper privacy, or if library leaders decide to put their budgets into something other than privacy. This can further be explored by talking about the way trends for “library funding has remained flat or

only shown modest growth." (Chatterjee). This lack of funding does not allow there to be much development in how libraries are able to maintain themselves or provide better privacy services to their patrons. This can be a major problem with academic libraries as the overarching schools will have the final say on where money goes and how it is used and not always the libraries themselves. These academic libraries may be pressured into "collect[ing] student data for assessment" in order to secure funding or both the institution and the library (Clark Hunt, et el.). Funding has the power to make or break a library and when push comes to shove a library may not make the most ethical choices to protect their patrons in order to preserve their existence within an academic institution. Although "privacy security practices [are] part of ALA's code of ethics," these ethical concerns may be pushed aside by librarians if it believed they are working for a greater good in the library even at the expense of some patrons. Even if a library has funding, the price of data breaches is very high coming in around "$227 a record with a total average cost of $6.5 million per breach" as of 2016 (Corrado). A data breach could potentially expose all sorts of private information to people who might do others, therefore should be taken seriously as a threat. The external pressure of an academic or government organization should not outweigh a librarians' ethics when it comes to making sure patrons are protected, and it unfortunately weighs on the librarians' shoulder to find the funding to see to it that everyone involved in their library system is safe.

If a library cannot maintain the safety of their patrons' private information this can crumble the trust they have in their library. No one wants to work with an organization which cannot guarantee their private information is safe and leaves them vulnerable. As Johnson points out, when "data has been breached… the longstanding trust libraries have built" does not last. These patrons are made vulnerable when there is a security breach because libraries store more

information about their patrons than just what items they check out. They may store private contact info like phone number and email address as well as address which could lead to a person being directly targeted. In general, the information of what someone checks out in a library should be private; although someone may not think their habit of reading fantasy is important until someone uses a particular series or author to track them down in public. This is why it is necessary to protect information from anyone outside of the library and "advocate for "customer" privacy" to ensure people are protected (Chatterjee). Libraries are a pillar of community relations and should work hard to support their patrons in the push for change in "customer" privacy. This shows how people really feel when it comes to their data and helps craft improvements so there will be more protection and thought given to this sharing of private information between organizations. Libraries need to consider the needs of all patrons and how they impact the greater community in order to continue fostering trust and offering protection from those who may do harm. When it comes to trusting outside sources and putting their community into some else's hands it's a necessity to "make sure [librarians] understand the licenses and terms of services they are agreeing to" (Corrado). There is a level of transparency that must be reached between librarians and community which allow everyone to know what is going on and limit the amount of data being collected in case of an unfortunate security breach which threatens not only singular patrons but the community as a whole.

There are a lot of issues a person might face when it comes to privacy anywhere let alone a library. These libraries can face internal and external issues which put pressure on them to release patrons' private information such as lack of funding, third party vendors, or a security breach. In this changing world, it is more important than ever to protect private information because it can spread farther than before and cause unlimited amounts of problems. As one of the

last vestiges of privacy protection it is important that librarians do their duty to the patrons to protect them and their community as a whole by not falling into the trap of information release. This work ensures the peace of mind of everyone individual and allows community connections to remain intact for a long time.

Works Cited:

Chatterjee, Sujoy. “How Your Neighborhood Library Protects Your Privacy.” *IAPP*, 26 Mar, 2019, https://iapp.org/news/a/how-your-neighborhood-library-protects-your-privacy/.

Clark Hunt, Laura K. et al. “E-resource Librarians Perceptions on Library Patron Privacy.” *The Journal of Academic Librarianship*, vol. 49, no. 3, May 2023, https://www.sciencedirect.com/science/article/abs/pii/S0099133323000435.

Corrado, Edward M. “Libraries and Protecting Patron Privacy.” *Technical Services Quarterly*, vol. 37, no. 1, 2020, https://www.tandfonline.com/doi/full/10.1080/07317131.2019.1691761.

Givens, C. *Information Privacy and Cybersecurity,* edited by Sandra Hirsh. Blue Ridge Summit: Rowman & Littlefield Publishers, Incorporated, 2022, pp. 456-470.

Johnson, Qiana. “Privacy Considerations for Library and Information Professionals.” *Information Services & Use*, vol. 40, no. 3, pp. 255-258, 2020, https://content.iospress.com/articles/information-services-and-use/isu200089.

Lambert, April D et al. “Library Patron Privacy in Jeopardy an Analysis of the Privacy Policies of Digital Content Vendors.” *Proceedings of the Association for Information Science and Technology*, vol. 52, no. 1, pp. 1-9, 24 Feb. 2016, https://asistdl.onlinelibrary.wiley.com/doi/full/10.1002/pra2.2015.145052010044.

Nichols Hess, Amanda et al. “Preserving Patron Privacy in the 21st Century Academic Library.” *The Journal of Academic Librarianship*, vol. 41, no. 1, pp. 105-114, Jan. 2015, https://www.sciencedirect.com/science/article/abs/pii/S0099133314001943.

“Privacy: An Interpretation of the Library Bill of Rights.” *American Library Association*, July 7, 2006. http://www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy.

Tsompanakis, Spyros. “A Discussion and Suggestions on Ethical Barriers in Librarianship.” *Wayne State University*, March 7, 2014, https://digitalcommons.wayne.edu/slisfrp/142/.

Zimmer, Michael. “Librarians’ Attitudes Regarding Information and Internet Privacy.” *The Library Quarterly*, vol. 84, no. 2, April 2014, https://www.journals.uchicago.edu/doi/10.1086/675329.