May 2020

I Always Feel Like Somebody's Watching Me: Student Perceptions of Library Data Privacy

Megan Palmer

Amie D. Freeman
University of South Carolina

Jade Geary
University of South Carolina - Columbia

I Always Feel Like Somebody's Watching Me: Student Perceptions of Library Data Privacy

Abstract

Data privacy has emerged as a controversial topic in higher education. As librarians, we recognize the importance of privacy and confidentiality for allowing patrons to learn and explore without unnecessary barriers or fear of repercussions. However, there is a growing trend of data collection and analysis in libraries that impacts a patron's right to privacy. In a presentation given at the 2019 South Carolina Library Association Annual Conference, we explored issues of click-through-consent, data invasion, and awareness of the types of data tracked. We asked for audience engagement as we discussed future directions including a survey on student perceptions of data privacy in libraries.

Keywords

Introduction

Data privacy is an emerging trend in higher education. Librarians have always been keenly aware of the responsibility to protect patron privacy and rights. However, in environments where we are regularly asked to provide information on our users and the quality of our services, it can be challenging to know where to draw the line. How can librarians protect their patrons while also assessing our services and impact? Further, how should we handle vendor collection of patron data?

In this paper, we expand on the issues covered in a presentation given at the 2019 South Carolina Library Association Conference through the framework of a literature and services review. An overview of the historical background of data protection and ethical implications of patron privacy in libraries will be provided. Next, we will examine the current library and library vendor data collection practices and explore potential directions for research into understanding student perceptions of data privacy in libraries.

Historical Background

There are many well-reported examples of libraries fighting to protect the privacy of their patrons. Librarians are likely familiar with conversations surrounding privacy agreements for eBooks and user agreements to access services. A recent example of patron privacy in the news surrounded the proposed requirement of Lynda.com to require library users to create LinkedIn accounts to access their training services (Young, 2019). However, to understand the context surrounding patron privacy, it is necessary to investigate the history of privacy protection in libraries.

Historically, libraries have been proactive in protecting patron privacy. Arguably, this was easier when libraries were simply a place that checked out books to patrons. However, the issue of privacy has become more complicated as patron records are digitized, users agree to terms of service to access electronic databases, and library safety issues have emerged. It has become increasingly difficult to

navigate the protection of patrons' privacy in the era of big data. To provide context for current

practices of patron privacy in libraries, it is necessary to revisit the historical background of libraries

acting or failing to act as stewards of privacy.

The American Library Association has affirmed a right to privacy since 1939, and international

organizations have held similar standards. The rights of patron privacy and confidentiality are explicit in

Article VII of the Library Bill of Rights (American Library Association, 1939) and are expanded in "Privacy:

An Interpretation of the Library Bill of Rights" (American Library Association, 2006). The interpretation

notes that privacy is "essential to the exercise of free speech, free thought, and free association."

Similarly, the National Information Standards Organization (NISO) Consensus Principles on

Users' Digital Privacy in Library, Publisher, and Software-Provider Systems recognizes that "the effective

management and delivery of library services may require the library user to opt into the provision of

personal data in order to access a library resource or receive library services. Users' personal data

should only be used for purposes disclosed to them and to which they consent" (National Information

Standards Organization, 2015, p.7).

While historically, librarians have been advocates of privacy rights for patrons, there have been

times when these rights have been eroded by external forces, notably, the government. For example, in

the post-WWII era, the United States used circulation records in an attempt to locate political dissidents

(Barringer, 2001). Again, in the 1960s, the FBI began collecting information on citizens, including their

personal library records, resulting in renewed efforts among libraries to protect patron data and the

creation of state statutes to protect these records. Nevertheless, again, in the 1980s, FBI agents

regularly requested information on suspected Soviet activities (Ford, 2017). In the post September 11,

2001 era, the Patriot Act was passed. This act allowed the FBI to produce an order

> requiring the production of any tangible things (including books, records, papers, documents,
>
> and other items) for an investigation to protect against international terrorism or clandestine

intelligence activities, provided that such investigation of a United States person is not

conducted solely upon the basis of activities protected by the first amendment to the

Constitution (Uniting and Strengthening America by Providing Appropriate Tools Required to

Intercept and Obstruct Terrorism Act of 2001),

generating much controversy and displeasure among librarians and other privacy stakeholders.

However, the concern has moved beyond the manual or electronic collection of circulation

records towards an era of a much higher potential for improper data collection and misuse. No longer

do patrons simply check out books of interest. Now, patrons may access library resources through

single-sign-on service providers, be required to provide their information to third-party vendors to

access content and participate in a host of other library services intended to further their educational

experience. This shifting method of content and service provision comes with new concerns for the

collection, retention, and use of patron data.

The ALA produced "Privacy: An Interpretation of the Library Bill of Rights" acknowledges the

difficulty of protecting data in the digital age, but notes that:

confidentiality extends to, 'information sought or received and resources consulted, borrowed,

acquired or transmitted,' including but not limited to: database search records, reference

questions, and interview, circulation records, interlibrary loan records, information about

materials downloaded or placed on 'hold' or 'reserve,' and other personally identifiable

information about uses of library materials, programs, facilities, or services (American Library

Association, 2006).

This interpretation makes clear the profession's commitment to upholding high standards for patron

privacy, despite the associated complications of the digital age.

Assessment and Accountability

The last few decades have seen an increasing interest in accountability due to the rising costs of tuition and the increasing emphasis on the importance of education. Historically, evaluations and assessments were done internally to improve teaching and learning outcomes; however, new rules, standards, and regulations are forcing institutions to conduct and make available assessments on performance and effectiveness (Stensaker & Harvey, 2011).

One example of this is Florida's Performance Funding Model (State University System of Florida, n.d.). This funding model began in the fall of 2012 and impacted 11 institutions. There are ten metrics used to evaluate the institution on various issues. The Florida Legislature and Governor then determine the new funding amounts and adjust the recurring state base appropriations.

As evidenced in the comprehensive report produced by ALA in 2010 titled *The Value of Academic Libraries: A Comprehensive Research Review and Report,* the impact of funding tied to performance on libraries have been incredible. Libraries have responded to an increasing interest in accountability over the last few decades. This is shown through the number of positions created related to assessment and position descriptions rewritten to include assessment. In response to demands for accountability and return-on-investment (ROI), libraries are grappling with showing their impact on student success and faculty productivity. In the attempt to demonstrate their value, libraries are collecting data and conducting assessments that often border on the invasion of patron privacy.

Examples of Current Library Patron Data Collection Practices

There are numerous policies and practices relating to data collection practices by libraries and library vendors. Here, we highlight here a few specific areas of concern for patron privacy. These are intended to provoke consideration and to spotlight a few of the more problematic issues. As you reflect on these examples, consider two questions:

1. What type of data does a library or vendor need to collect to provide the desired service or resource?

2. How much data is actually collected, and how long is it stored?

First, we'll consider the use of a proxy server to authenticate a patron's credentials in order to access protected electronic resources. When users sign into a proxy, it holds a snapshot of information about the patron. This snapshot is based on the parameters that a library or institution sets up and could include a user's IP address, username, time and date, and the resources accessed during a session.

Figure 1:

Example of Proxy Server Information Collected

The information collected through proxy logins is kept as a way to investigate and deter illegal downloading of content. However, libraries are also starting to investigate and assess patron actions through proxy use. They may have the technical ability to look at proxy use by discipline and patron status and can see which resources patrons are using in the proxy and compare to usage statistics. This data can then potentially be used to correlate electronic resource use and student retention or other various student success measures.

Traditional services, such as circulation and interlibrary loan, are also susceptible to data collection. Libraries must collect certain patron information for library service platforms and interlibrary

loan software to perform as expected. However, when considering patron privacy, librarians must

consider what types of essential and non-essential data, like browsing and search histories, are collected

and how long this data is stored. We must also carefully consider the security of the platforms.

Marshall Breeding, a library technologist, and consultant, performed a study in 2016 in which he

surveyed many of the major ILS and LSP vendors (Breeding, 2016). In rather encouraging news, he

concluded that:

> the responses given by this selection of vendors and developers of the major automation
>
> products in use in libraries today do not reveal any significant problems or omissions in the way
>
> that they handle security and privacy. Each product has the potential to be configured in a way
>
> to reasonably protect patron privacy, and all follow general industry practices for overall system
>
> security" (Breeding, 2016, p. 27).

However, part of this statement notes that the products aren't necessarily automatically configured to

protect privacy; rather, they must be configured, often by the librarians handling the systems, to protect

privacy and security. This places the responsibility on librarians to ensure that we fully understand the

implications and risks of handling patron data and that we are well trained and competent in our system

administration and usage.

For example, Ex Libris Alma retains information about historical loans. In order to comply with

privacy regulations, patron personal information is anonymized after a certain period, which can be

configured based on library needs. Information about the patron type, group, etc. is kept, even though

that information contains no personal data (Ex Libris, n.d.). Again, the onus is on the library to

anonymize the information and to configure the retention period to protect patron privacy. Similar

processes are in place for most library service platforms, which is reassuring as long as libraries and

librarians are proactive about setting reasonable customizations and regularly anonymizing data.

Interlibrary loan systems, on the other hand, maybe less secure when handling patron data, although there have been recent improvements. For example, in ILLiad, an interlibrary loan system used by the majority of large research libraries, patron histories are retained indefinitely, or until they are manually deleted, or a script is run through the ILLiad database manager (Atlas Systems, n.d.). When reports are exported, sensitive patron data could potentially be included in the reports. So, for example, if a librarian ran a query requesting information on all of the items requested by a certain department, patron names, usernames, addresses, and more would be attached to the items in the resulting report. For these items to be shared or used, the responsibility rests with the librarian to manually strip the sensitive information, leaving it susceptible to mistakes. In Worldshare, as well as OCLC's newest ILL product Tipasa, administrators can set the length of time for patron data to be retained (OCLC, 2019), and librarians should note that patron data is not encrypted in the database.

Secured library entrances are another possible point of concern. There are some libraries that have secured entrances for certain spaces or for the whole building, such as Florida State University and Georgia State University (Florida State University Libraries, 2019; Georgia State University Library, 2019). There are many reasons that a library may choose to use secured entrances. For example, in the case of an emergency, a record of persons inside a library during a particular time could be used for rescue operations or to contact patrons. To create a faculty or graduate student only space, card swipe access to enter the room is a frequently used option. It allows libraries to not only limit who can enter a room but also to know who is in the room and how often. The swipe of a card sends data to a database where it records personal identifying information about whose card was swiped and a timestamp of when the swipe occurred.

This data could be used to record an exact number of entrances and to examine use by discipline or patron status. If libraries have patrons swipe out to leave the building, they could note the total amount of time spent in the building. Since personal identifying information is recorded,

administrators or data specialists could potentially examine correlations between student success

measures and library usage, or time spent in the library. The literature on this subject is lacking, and thus

measures being taken by libraries that have established this policy are purely anecdotal. There is a need

for more research and scholarly communication to be provided on the effects and implications of

secured library entrances.

Privacy and data practices and policies for resource provisioners are another factor to consider

when examining patron data privacy. While there are innumerable vendors that provide resources to

libraries, we'll briefly examine two examples, NexisUni and Springshare. While NexisUni "implement[s]

technical and organisational measures to seek to ensure a level of security appropriate to the risk to the

personal information [they] process" (NexisUni, 2019), parts of the privacy policy warrant further

consideration from astute observers. When logged in to the NexisUni account, NexisUni does not offer

an option for patrons to immediately clear their search history. Although instructions are present, they

are not aligned with the actual options provided through the website. This may be uncomfortable for

patrons performing guided or moderated research (NexisUni, n.d). Like NexisUni, Springshare is

transparent regarding the data that may be collected from patrons (Springshare, 2018). However, this

transparency doesn't necessarily translate into information available at the point of need for patrons.

For example, when a patron elects to chat with a librarian, they are presented with a brief form to fill

out before starting the chat requesting information such as their name and email address. However,

they are not alerted at that time that additional information may be shared with the recipient of the

chat, such as their IP address, device identifier, and location. Again, these practices can be located by a

savvy patron, but if readily presented, might be of concern to a patron seeking information on a

sensitive topic.

Finally, it is necessary to discuss the use of video and audio surveillance in libraries. Many

libraries choose or are directed to use video surveillance throughout or in certain parts of the library to

provide security to patrons and staff. Despite the research that has shown that surveillance in libraries is largely ineffective for preventing crime, there's no question that it can be a useful tool for identifying perpetrators of security incidents and also for protecting those falsely accused of certain actions (Randall & Newell, 2014).

Although many libraries use video surveillance, ALA notes that "high-resolution surveillance equipment is capable of recording patron reading and viewing habits in ways that are as revealing as the written circulation records libraries routinely protect…. Since any such personal information is sensitive and has the potential to be used inappropriately in the wrong hands, gathering surveillance data has serious implications for library management" (ALA, 2019). In fact, one library administrator who was responsible for the implementation of a video surveillance initiative, when asked about the proper role of video surveillance in libraries, commented in 2014 " 'I am at war with myself' due to the competing safety and privacy concerns" (Randall & Newell, 2014, p. 513). It's clear that library use of video surveillance illustrates a prime example of ongoing conversations throughout today's society: do we choose to value privacy or security?

Certain measures can be taken to improve patron privacy, even as surveillance programs are in place. For example, patrons can be provided with written policies and notifications detailing information on access, storage, and footage requests. Additionally, librarians can consider only using cameras in certain locations and by angling cameras to maximize privacy. However, even with measures in place, the privacy of patrons can be violated and may cause patrons to fear that the data collected through video surveillance could be misused. It is not impossible that these concerns could discourage student library usage free from censorship or privacy concerns.

Future Directions

The librarians involved in this presentation are far from the only stakeholders interested in the

topic of student privacy in libraries. Because of the expansive scale of these topics, reviewing all

research would be unrealistic within the scope of this paper. However, it is important to note that

numerous others have written about issues of student privacy within academic institutions, whether on

observational data surveillance (Harwell, 2019), location surveillance (Gardner, 2019), institutional of

learning analytics providers (Reidenberg & Schaub, 2018), library participation in learning analytic

systems (Jones et al., 2019) or directly within the library (Lambert et al., 2015).

A recent dissertation from Laura W. Gariepy explored undergraduate student attitudes

surrounding the collection, use, and privacy of search data within academic libraries and how they felt

this data should be handled by librarians. Gariepy (2019) performed in-person interviews with 27

students and coded the results to uncover themes, discovering that students were generally

comfortable with libraries collecting search data if used for their personal benefit, but were moderately

concerned with their search data being used to assist government agencies. Students also expressed a

desire for greater control of their data. This study provides valuable insights into student perceptions of

library data usage and is an important step towards providing a fuller understanding of these issues.

Gariepy invites researchers to perform further studies into exploring the topic of student attitudes

towards their library search data.

To further understand student attitudes, we have created a brief survey regarding student data

privacy in the library. It is necessary for librarians to understand whether students are aware of the

information collected and used by the library and library vendors through provided resources and

services. Beyond awareness, we hope to understand student perceptions towards the potential use of

their personal data within the library sphere, and whether they are concerned with personal consent.

These topics merit further investigation, and we hope to contribute to the body of knowledge, and,

ultimately, help others to create and evolve informed library data use policies.

References

American Library Association. (2019). *Library bill of rights*.

   http://www.ala.org/advocacy/intfreedom/librarybill

American Library Association. (2006, July 7). *Privacy: An interpretation of the library bill of rights.*

   http://www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy

American Library Association. (n.d.). *Privacy and confidentiality Q&A*. Retrieved February 19, 2020, from

   http://www.ala.org/advocacy/intfreedom/privacyconfidentialityqa

Atlas Systems. (n.d.). *ILLiad database manager.* http://support.atlas-sys.com/hc/en-

   us/articles/360011912453-The-ILLiad-Database-Manager

Barringer, F. (2001, Apr 08). Using books as evidence against their readers. *New York Times (1923-*

   Current File) Retrieved from

   https://login.pallas2.tcl.sc.edu/login?url=https://search.proquest.com/docview/92124952?acco

   untid=13965

Breeding, M. (2016). The current state of privacy and security of automation and discovery products.

   Library Technology Reports, *52*(4), 13–28.

Ex Libris. (n.d.). *Patrons, patron interface (Primo)*. Retrieved February 18, 2020, from

   https://knowledge.exlibrisgroup.com/Alma/Product_Materials/050Alma_FAQs/User_Managem

   ent/Patrons%2C_Patron_Interface_(Primo)

Florida State University Libraries. (2019, April 11). Can the public use Florida State University libraries?

   What are the restrictions? http://fsu.libanswers.com/faq/33635

Ford, C. (2017). *Pro se patrons in the law library: The case for privacy in the digital age*.

Gardner, L. (2019, October 13). Students under surveillance? *Chronicle of Higher Education*.

   https://www.chronicle.com/article/Students-Under-Surveillance-/247312/

Gariepy, L. (2019). *Undergraduate students' attitudes about the collection, use, and privacy of search*

   data in academic libraries. https://scholarscompass.vcu.edu/etd/6077/

Georgia State University Library. (2019, July 16). Can visitors use Georgia State University Library at the

   Atlanta and Perimeter locations? http://answers.library.gsu.edu/faq/79020

Harwell, Drew. (2019, December 24). Colleges are turning students' phones into surveillance machines.

   Washington Post. https://www.washingtonpost.com/technology/2019/12/24/colleges-are-

   turning-students-phones-into-surveillance-machines-tracking-locations-hundreds-thousands/.

Jones, K. M. L., Perry, M. R., Goben, A., Asher, A., Briney, K. A., Robertshaw, M. B., & Salo, D. (2019).

   Student perspectives on privacy and library participation in learning analytics Initiatives.

   Proceedings of the Annual Meeting of the Association of College and Research Libraries, 262–

   274. https://datadoubles.org/wp-content/uploads/2019/04/ACRL_2019.pdf

Lambert, A. D., Parker, M., & Bashir, M. (2015). Library patron privacy in jeopardy an analysis of the

   privacy policies of digital content vendors. *Proceedings of the Association for Information*

   Science and Technology, *52*(1), 1–9. https://doi.org/10.1002/pra2.2015.145052010044

National Information Standards Organization. (2015). *NISO consensus principles on users' digital privacy*

   in library, publisher, and software-provider systems. National Information Standards

   Organization (NISO). https://www.niso.org/publications/privacy-principles

NexisUni. (n.d.). *How do I delete recent searches?* http://help.lexisnexis.com/tabula-

   rasa/totalpatent/deleterecentsearches_hdi-task?lbu=US&locale=en_US

NexisUni. (2019). *Privacy Policy*. https://www.lexisnexis.com/en-us/terms/privacy-policy.page

Oakleaf, M. J. (2010). *The Value of Academic Libraries: A Comprehensive Research Review and Report*.

   Association of College and Research Libraries, American Library Association.

OCLC. (2019, August 24). *Tipasa.* https://www.oclc.org/en/tipasa.html

Randall, D. P., & Newell, B. (2014, March 1). The panoptic librarian: The role of video surveillance in the

    modern public library. *IConference 2014 Proceedings: Breaking Down Walls.*

    https://doi.org/10.9776/14132

Reidenberg, J. R., & Schaub, F. (2018). Achieving big data privacy in education. *Theory and Research in*

    Education, *16*(3), 263–279. https://doi.org/10.1177/1477878518805308

Springshare. (2018). *Springshare Privacy Policy*. https://springshare.com/privacy.html

State University System of Florida. (n.d.). *Performance Based Funding*.

    https://www.flbog.edu/finance/performance-based-funding/

Stensaker, B., & Harvey, L. (Eds.) (2011). Accountability in higher education: Global perspectives on trust

    and power. Routledge.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct

    Terrorism (USA PATRIOT Act) Act of 2001, H.R. 3162, Congress, 107th (2001).

    https://www.congress.gov/bill/107th-congress/house-

    bill/3162?q=%7B%22search%22%3A%22Uniting+and+Strengthening+America+by+Providing+Ap

    propriate+Tools+Required+to+Intercept+Obstruct+Terrorism+Act%22%7D&r=9

Young, J. (2019, November 27). *LinkedIn pauses changes to Lynda.com after libraries raise privacy*

    concerns. EdSurge. https://www.edsurge.com/news/2019-11-27-linkedin-pauses-changes-to-

    lynda-com-after-libraries-raise-privacy-concerns