Information Services & Use 40 (2020) 255–258
DOI 10.3233/ISU-200089
IOS Press

Privacy considerations for library and information professionals

Qiana Johnson*
Collection and Organizational Data Analysis Librarian, Northwestern University, 1970 Campus Drive, Evanston, IL, USA
ORCID: https://orcid.org/0000-0002-9027-2530

Abstract. This paper is based upon a session on privacy that was held during the inaugural NISO+ conference that was held February 23–25, 2020 in Baltimore, MD. It briefly describes the six types of privacy put forth by Daniel Solove in his book, *Understanding Privacy*, and the professional standards held by librarians to ensure that their patrons can access and consume information with little or no observation. It also offers some helpful suggestions for librarians to consider as they work to secure privacy and confidentiality.

Keywords: Privacy, library confidentiality, personal information, privacy policies

"Privacy is dead". "Young people don't value privacy". "I have nothing to hide".

These and similar phrases are often heard in the press and every day conversation. Does privacy mean the same thing to everyone? And how can different groups come to agreement about why privacy is important and what is protected?

A first question is why do we care about privacy - our own and others'? Frequently, people want to control the information they share with others. Rarely do we want to share the same information on all occasions. Instead, it usually depends on with whom we are interacting and to what purpose that information is being put.

A useful concept of privacy comes from Daniel Solove's book *Understanding Privacy*. There he defines six types of privacy [1]:

(1) The right to be let alone.
(2) Limited access to the self - the ability to shield oneself from unwanted access by others.
(3) Secrecy - the concealment of certain matters from others.
(4) Control over personal information - the ability to exercise control over information about oneself.
(5) Personhood – the protection of one's personality, individuality, and dignity.
(6) Intimacy – control over, or limited access to, one's intimate relationships or aspects of life.

The protection of most, if not all, of these types of privacy are part of the professional ethics of libraries and librarians. Which of these types of privacy are values for publishers and library vendors? Are libraries,

*Tel.: +1 847 491 2229; E-mail: q-johnson@northwestern.edu.

publishers, and vendors frequently talking at cross purposes, or is there a way they can come to mutual understanding and agreement?

1. Positioning

I come to the information privacy conversation from a very traditional librarian lens: protect patrons' ability to access and consume information with little to no outside observation. That includes observation by libraries, vendors, and government entities.

In an era of exclusively print and physical items, maintaining patron privacy was easier. Circulation and other usage records were held exclusively by libraries. As more and more content moves online and there are more parties involved in the provision of information resources, maintaining this core library value has become more difficult. But it certainly hasn't gone away. According to the American Library Association, forty-eight states and the District of Columbia have laws to protect the confidentiality of library records. The language varies from state-to-state, but library patron privacy is legislated in almost all locations. Libraries and the organizations with which they work need to familiarize themselves with the current requirements of the state as well as any pending legislation in order to be prepared to make adjustments to their policies and data handling practices.

While there are numerous legal requirements and professional standards underlying those privacy requirements, there is also the ethical value of people being able to consume any content they have appropriate access to through the library without being observed. Personal and professional growth can be a messy and deeply personal enterprise. People who know that they are being watched may change their behavior if they fear any kind of judgement for what they are doing.

2. Who is at risk?

Harm can come from combining or sharing datasets, because it leads to third parties making unexpected discoveries about someone's behavior. Patrons may have varying levels of comfort in terms of sharing of their information. They might have been willing to share or disclose information based on a particular stated use of data and patrons might not have been as willing to disclose that data if they knew that information was going to be used in other ways. Because of its longstanding policies regarding patron privacy, library patrons may have specifically chosen to seek out information through the library in order to maintain privacy around the content of their information seeking.

For example, a patron may be looking for resources about reporting an employer for malfeasance or another patron is looking for resources to leave a dangerous living situation. Sharing of patron information across systems can allow a picture of a patron to be built and those patrons often do not have the ability to correct or delete the picture formulated about them from these different datasets. It is also often the case that more data is collected about those who don't have the financial means to opt out of data collection or the technical skills to limit the amount and type of data being gathered about them.

3. Privacy by design

Companies often default to collecting as much data as possible now, just in case it is needed down the road. The problem is that the more data that is gathered, the more data that has to be secured and protected.

Data breaches are a common occurrence and any data that you store is vulnerable in a breach. According to a March 10, 2020 report, in 2019 there were fourteen hundred and seventy-three data breaches in the United States compromising more than one hundred and sixty-four million records [2]. For vendors, a data breach can have a lasting negative impact on a company's brand. For libraries, if a vendor's data has been breached and patrons learn that their data has been held by a third party previously unknown, the longstanding trust libraries have built in their communities can be permanently broken.

Another problem with just gathering as much data as you can, is that later when an organization goes to use it, the data might not have been gathered in a way that is useful for analysis. A better place to start from is to determine what question needs to be answered, followed by what is the smallest amount of personally-identifiable information that needs to be gathered to answer that question. Additional questions to ask are: who will have access to the raw data versus summary data? How long will the data be kept? How are you articulating to users about what information you are collecting, or that you are allowing others to collect about them?

4. Privacy policies

It is important that the staff charged with reviewing contracts within a library have read the privacy policies for the various products and tools that they license. It is important for libraries to know what information is being gathered about their patrons, with whom that information is being shared, as well as if and how users can opt-out of data being gathered about them. Particular attention should be paid to the ability to opt out - how easy is it to find out how to opt-out, how easy it actually is to then opt out, and can patrons get their data deleted. The ease, or lack thereof, of opting out is a serious barrier to patrons having control of their information.

If the library has negotiated for additional patron privacy protections, libraries should look at how and if they are sharing that information with their patrons. Libraries should also look at how and if they are educating their patrons about the information being collected about them and how they can control that. This is particularly important because patrons may see their relationship as being with the library (through whom they are accessing resources) and not an unknown third party. Libraries have a responsibility to their patrons to know what information is being collected about patrons and how the amount of data collected can be limited. They must communicate that to patrons, and further report any data breaches. A sure-fire way of breaking trust is not to be honest as quickly as possible.

5. Shared privacy values

There are a number of professional statements and agreements about privacy - some library-led and some publisher and vendor-led. The American Library Association has a number of policy documents around privacy, such as The Library Bill of Rights see http://www.ala.org/advocacy/intfreedom/librarybill) and the Code of Ethics (see: http://www.ala.org/tools/ethics). There are privacy statements that groups of libraries have put out, such as The Statement on Patron Privacy and Database Access led by Stanford University Libraries see https://library.stanford.edu/using/special-policies/statement-patron-privacy-and-database-access). And there are statements of consensus principles by organizations across the information landscape, such as The NISO Consensus Principles on Users' Digital Privacy in Library, Publisher, and Software-Provider Systems (see: https://www.niso.org/publications/privacy-principles). There is interest in all corners around patron privacy. These statements

show that there is much in common and the various statements and codes provide a starting point for larger conversations.

References

[1] D.J. Solove, *Understanding Privacy*. Harvard University Press, Cambridge, Mass, 2008, ISBN-13: 978-0674035072.
[2] J. Clement, *Cybercrime: Number of Breaches and Records Exposed 2005–2019 [Internet]*. Statista, New York, 2020, Available from: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/, last accessed June 7, 2020.