



CASE STUDIES

Preserving Patron Privacy in the 21st Century Academic Library



Amanda Nichols Hess*, Rachele LaPorte-Fiori, Keith Engwall

Oakland University Libraries, 2200 N. Squirrel Road, Rochester, MI 48309, USA

ARTICLE INFO

Article history:

Received 9 September 2014

Accepted 31 October 2014

Available online 8 December 2014

Keywords:

Academic libraries

Privacy policy

Patron privacy

ABSTRACT

How do libraries reconcile increasing access to information and encouraging the use of 21st century technology systems and tools while also preserving patrons' privacy? This question is challenging for all libraries to address, but academic libraries must grapple with it while also considering other complex issues: not only do these libraries need to comply with the ALA's Library Bill of Rights and supporting documents, but they must also adhere to federal-, state-, and institution-level policies regarding student privacy and information security. This article presents how one university's libraries worked to both develop a public statement on patron privacy and identify behind-the-scenes issues with the collection, storage, and disposal of library patrons' private information. The strategies used herein may be helpful to other academic libraries as they consider patron privacy in the 21st century.

© 2014 Elsevier Inc. All rights reserved.

INTRODUCTION

For libraries large and small, patron privacy is an important ethical issue. While librarians may espouse privacy and confidentiality as an inalienable individual right, ensuring that this right is upheld across library departments can be challenging, especially when 21st century technology tools are considered. For all libraries, developing a privacy policy or statement is an essential initial step in ensuring that patron privacy and confidentiality are consistently enforced. This article examines how one large Midwestern academic library remedied its lack of a public privacy statement; this case study presents a series of strategies that other libraries can consider for evaluating – or establishing – their own public privacy policies.

LITERATURE REVIEW

LIBRARY PRIVACY AS A PHILOSOPHICAL AND LEGAL RIGHT

When considering library patron privacy and confidentiality, it is important to consider how these issues have been addressed at the professional and legal levels. Libraries have long recognized and protected patrons' privacy and confidentiality. The American Library Association (ALA) asserts that its Library Bill of Rights implicitly protects patron privacy through the statements that libraries should ensure that individuals' rights "to use a library... not be denied or abridged because of origin, age, background or views," and that libraries should resist "abridgement of free expression and free access to ideas" (ALA, 1996). In its interpretation of this guiding document, ALA asserts that "when

users recognize or fear that their privacy or confidentiality is compromised, true freedom of inquiry no longer exists" (ALA, 2014a). Forty-eight states and the District of Columbia have protected this right to privacy and confidentiality in legal statutes that protect patrons' library records from release or disclosure without consent (ALA, 2014b). Michigan's Library Privacy Act, passed in 1982, states that "a library record is not subject to the disclosure requirements of the freedom of information act... [and] a library or an employee or agent of a library shall not release or disclose a library record... without the written consent of the person" (State of Michigan Legislative Council, 1996).

In spite of this legal right, the federal government has frequently challenged library patrons' right to privacy. For instance, Lamdan (2013) notes that many library privacy policies developed in reaction to attempts by the Federal Bureau of Investigation (FBI) to use library surveillance and librarian informants as evidence and the Department of Treasury seeking access to circulation records of patrons who had checked out materials on bomb making. Since 9/11, patrons' library records have again come under scrutiny with the passage of the Patriot Act, which librarians have seen as an attack on intellectual freedom (ALA, 2009; Bowers, 2006; Case, 2010; Jones, 2009). Libraries, then, must be cognizant of these challenges and issues as they plan to keep patron data confidential.

Another consideration in protecting patron privacy is the US Department of Education's Family Educational Rights and Privacy Act (FERPA). While library records cannot be disclosed without a patron's consent through a Freedom of Information Act (FOIA) request, any school that receives funds from the US Department of Education is subject to FERPA; at K-12 and post-secondary institutions, this includes the library (U.S. Department of Education, 2014). So, while patron privacy records are protected at the state and federal levels, there are also exceptions to the rule – and these exceptions can be broad. For instance, student record information can be disclosed to, among other entities, "School

* Corresponding author. Tel.: +1 248 370 2487.

E-mail addresses: nichols@oakland.edu (A. Nichols Hess), laporte@oakland.edu (R. LaPorte-Fiori), engwall@oakland.edu (K. Engwall).

officials with legitimate educational interest,” “appropriate parties in connection with financial aid to a student,” and “Organizations conducting certain studies for or on behalf of the school” (U.S. Department of Education, 2014). Academic and school libraries, then, also need to consider how FERPA impacts their ability to protect patrons’ privacy and confidentiality.

DIGITAL TECHNOLOGIES POSE NEW CHALLENGES

The continuing proliferation of digital technologies poses practical privacy-related challenges for libraries. In a review of how academic libraries address patron confidentiality and privacy in the digital age, Ficarek (2002) asserts that libraries and librarians find it increasingly difficult to ensure privacy with adequate safeguards as technology tools and hardware develop. This is in part because there are myriad factors to consider with digital tools. At the most basic level, academic libraries need to consider privacy as it relates to computing technologies because many libraries provide patrons computer workstations, copiers, scanners, printers, and other hardware available for use. Any statements on the privacy of patron information, then, needs to include information on data and network security, intellectual property and copyright, and workstation security as they relate to patrons’ privacy and use of library equipment (Vaughan, 2004). Another facet of this issue, though, is the proliferation of web-based resources such as social networking sites that ask patrons to share personal information. Griffey (2010) specifically notes the unclear relationship between libraries’ desire to provide patrons with access to these sites and to library resources *through* these channels, and libraries’ privacy concerns. There seems to be a disconnect at the foundational levels of libraries and social networking resources: while social sites seek to find out information about individuals and then provide that information to others, libraries seek to limit the amount of personal information collected and keep that information private (Griffey, 2010).

An added layer to both sides of this issue, though, is that there is no formalized code or legislation that can guide academic libraries’ efforts to ensure privacy, regardless of technological developments (Ficarek, 2002; Jones, 2010). Furthermore, Zimmer (2013) found that while these issues are discussed in the literature, they are done in only a cursory fashion and there is no real roadmap or established set of best practices for librarians. So, despite recognition of an individual’s right to privacy as both a legal and fundamental human right (United Nations, 1948), the path forward for libraries is not always clear.

PATRONS’ PERCEPTIONS OF PRIVACY IN THE LIBRARY

In spite of these difficulties encountered by libraries and librarians, research suggests that patrons consider the library as a place where their personal information remains secure and confidential. In a study of library patrons’ perceptions of trust in the library and its ability to keep personal information private, Sutcliffe and Chelin (2010) found that individuals at a large university are both confident that libraries keep their information private. In fact, this study found that patrons *expect* libraries to protect their personal information. Moreover, participants in this study also asserted that having a clear policy on the confidentiality of library records and the privacy of information helped them to trust libraries and librarians. The researchers make an important point to consider, though: librarians and libraries need to *earn* this trust by protecting patron data and information.

DEVELOPING A PRIVACY POLICY

While there is support, both professionally and legally, for ensuring patron privacy and confidentiality, there is no standard set of guidelines that libraries can apply universally. As such, a critical component in ensuring that we meet patrons’ expectations is to develop statements or policies that enumerate the library’s role in protecting information. Generally, the literature suggests that these policies develop for one of

three reasons (or some combination thereof). First, policies may be crafted as a result of legal concerns. As Lamdan (2013) states, ALA’s privacy requestor policy were developed in reaction to government attempts to track and incriminate library patrons. Similarly, Jones (2009) recounts the actions of a group of Connecticut librarians who worked to protect patron privacy in response to the Patriot Act on ethical grounds. This stance represents the most reactionary position from which a privacy policy may develop.

Second, policies may also grow out of a need recognized through an internal audit (i.e., Adams, 2007). In response to an internal issue with patron privacy, Coombs (2004) notes that patrons’ personally identifiable information can be found in many places, including in integrated library systems, interlibrary loan records, web logs, proxy server logs, and on public computers, among other locations. Auditing these systems and determining where this information exists is perhaps the first step to creating dynamic and effective policies to keep this information confidential (Coombs, 2004). Similarly, Vaughan’s (2007) case study highlights one academic library’s work in developing a record retention policy in response to a recognized internal need rather than a legal challenge. This impetus allowed for the institution to internally audit its existing policies, as well as patron records, proactively through the lens of ALA’s Privacy Toolkit rather than as a reaction, and it therefore had time to have the policy reviewed by many stakeholders (e.g. the institution’s general counsel and library administration).

Third, library-specific privacy policies may also develop as a response to broader institution-wide policies. This stance is taken by academic and school libraries as they work to protect privacy while also complying with FERPA (see, for instance, Adams, 2006). In a 2003 study of patron privacy in the digital environment, Sturges et al. found that very few libraries had distinct privacy policies *separate* from that of their parent institution, but many libraries did in fact have data protection plans (64%) and policies on acceptable Internet use (81%). The researchers believe that, in 2003, this suggested the existence of a priorities hierarchy – and that privacy, a seemingly nebulous construct, was hard to pin down. However, more than ten years later, perhaps these priorities have changed and it is more important for libraries to have separate and distinct privacy policies than their parent institution.

ISSUES IN DEVELOPING PRIVACY MEASURES

There are, of course, issues when it comes to developing effective and enforceable privacy policies and resources. First, there is a lack of systematic regulation of library privacy rights (Case, 2010; Jones, 2010; Zimmer, 2013). Second, there are conflicts between conveniently providing services to patrons and keeping information private and confidential. Sometimes, this concerns specific library services, such as holds or interlibrary loan. For instance, Stevens, Bravender, and Witteveen-Lane (2012) examined whether self-service holds were violating patron privacy; they found that librarians felt that, despite the apparent convenience, placing a book on an open hold shelf with patron information attached had serious privacy implications. This issue is further complicated by the advent of digital technologies that collect and employ patron data and behavior, especially since “library personal data resources are capable of revealing a great deal about the tastes and preferences of the library’s patrons” (Sturges, Teng, & Iliffe, 2001). Zimmer (2013) notes that libraries need to resolve how to preserve privacy while employing these technologies – such as Goodreads, Delicious, and other social networking platforms – to enhance the library experience.

Librarians’ perceptions on privacy policies and practices may also impact the development of meaningful procedures. In 2007, Magi considered the prevalence of library privacy policies at public and academic libraries, and found that smaller libraries often do not have written policies in place. However, she also found that these libraries receive a comparable number of requests for information to their larger counterparts. Librarians’ responses to requests, then, are based on their interpretation of ethical professional behavior. Zimmer (2014) specifically

Download English Version:

<https://daneshyari.com/en/article/358205>

Download Persian Version:

<https://daneshyari.com/article/358205>

[Daneshyari.com](https://daneshyari.com)