The Journal of Academic Librarianship 41 (2015) 105–114

Contents lists available at ScienceDirect

The Journal of Academic Librarianship

CASE STUDIES

Preserving Patron Privacy in the 21st Century Academic Library

Amanda Nichols Hess *, Rachelle 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.

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).

http://dx.doi.org/10.1016/j.acalib.2014.10.010
0099-1333/

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, Fifarek (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 (Fifarek, 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, Sutlieff 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

examined librarians' attitudes toward information and Internet privacy in 2008 and 2012; he found that, in both studies, 97% of librarians felt that personal library information should never be shared. While the majority of respondents felt that libraries do all they can to prevent unauthorized disclosure of records, Zimmer observes a shift from 2008 to 2012 in the percentage of librarians who feel they have a role in educating the public on privacy. And while this analysis found that 69% of respondents had practices or procedures in place to deal with requests, just 51% felt equipped to deal with requests for disclosure. Whatever the reason for developing a privacy policy or procedures, it is important that librarians are properly educated and equipped on its implementation.

INSTITUTIONAL PROFILE AND NEED

Oakland University (hereafter OU) is a Carnegie-classified doctoral research institution in Rochester, Michigan with a current enrollment of more than 20,000 students in more than 240 certificate and degree programs. The University Libraries, comprised of the Kresge Library and OU William Beaumont School of Medicine Library, are committed to fostering academic excellence and promoting information literacy to faculty, students, staff, and community patrons. Housing more than 800,000 print volumes, 75,000 journal titles, Special Collections and University Archives, Kresge Library is open 24/7 and averages 579,023 people annually.

Since the Kresge Library's construction in 1961, OU Libraries have seen an evolution of services, from endless rows of study carrels and stacks of reference books, to its existing role as a technology and information hub. Many of the Libraries' existing policies were written before technology became the predominant function of the library and, as such, are in need of review. In 2013, library administration reached out to a consultant to review the OU Libraries' Access Services operations. While reviewing policies, the consultant noticed several outdated policies; most importantly, no comprehensive policy regarding patron privacy existed.

OU Libraries' *Confidentiality of Library Circulation Records* policy, dating back to 1999, was the only formal policy that addressed patron privacy and confidentiality, and it was specifically designed to protect the identity of any borrower of a library book. Ensuring that any request for specific call numbers or titles checked out by a particular borrower would be denied, this policy had been clearly written prior to the ubiquity of technologically-rich library systems, and was likely in use before OU Libraries' first Integrated Library System (ILS). In response to this policy's need for review, the consultant and the Dean of the Library quickly developed a *Confidentiality and Privacy of Patron Information* policy as a replacement. However, no other privacy policy existed, public or otherwise, and this new policy did not address the myriad issues existing in 21st century privacy concerns.

PRIVACY POLICY TASK FORCE

In response to this need, a task force was established in January 2014 with diverse representation from across OU Libraries' departments. This group's primary goal was to produce a privacy policy statement that would be published on the Libraries' website and would affirm the library's commitment to keep information about Library patrons private and confidential while incorporating applicable federal and state laws, university policies, and professional library standards. This statement would also address all areas of library services and would recognize the new privacy concerns created by digital technologies. From this foundation, the task force would also identify and recommend any corrective steps needed within library procedures to ensure patrons' privacy and confidentiality.

THE PROCESS TO A PRIVACY STATEMENT

While the task force was charged with creating a privacy *policy* for OU Libraries, early in the process it became clear that we, in fact, were *not* creating a policy. As part of a public university where policies are set by the OU Board of Trustees, the term *policy* to designate our work was somewhat of a misnomer. Instead, our work served to explain to our patrons the policies we adhere to and how we interpret these policies to provide library services and resources. Therefore, the group agreed that our final deliverable would be a privacy *statement* rather than a privacy policy.

As we considered how we could most effectively craft such a statement, it became clear that understanding how other academic libraries communicated their privacy and information sharing policies to patrons would be helpful. To this end, our team surveyed the privacy policies made available online via the websites of the other fourteen public universities in Michigan. We found little consistency in how these academic libraries communicated their policies to their patrons. Approximately half had a library-specific privacy policy; within this group, there was a fairly even split between brief and concise policies and those which were lengthy and detailed. Several libraries referred patrons either to the Michigan Library Privacy Act or to their university's privacy policy; three had no mention of a privacy policy at all.

STATEMENT STRUCTURE

After discussing the features of the various policies we found, the task force decided that three policies in particular had aspects the task force wanted to emulate in our public privacy statement: Central Michigan University (CMU) Libraries and the University of Michigan Ann Arbor (UM-AA) Libraries, as well as the Grand Valley State University (GVSU) Privacy Statement. We chose to model the structure of our privacy policy after the easy to use and navigate format of the GVSU Privacy Statement, dividing the policy into four broad library-specific policy areas (see Fig. 1). Also, CMU Libraries' patron-focused language and its use of web links to direct patrons to supporting material helped us as we considered how to phrase our privacy statement (see Fig. 2). And, as we delved deeper into patron privacy in *all* aspects of library services, we felt it was important to include a section on third party resources in our statement; this was modeled on the Contracts and Licenses for Information Resources section of the UM-AA Libraries policy (see Fig. 3).

STATEMENT CONTENTS

PROFESSIONAL STANDARDS AND ETHICS

As we specifically considered the privacy statement's *content*, we recognized the importance of being guided by the underlying principles upheld by our profession. To this end, the task force integrated the ALA Library Bill of Rights, Code of Ethics, and Privacy Toolkit into its work process. The most essential component of these resources proved to be the fifth statement of the Library Bill of Rights, which reads that "A person's right to use a library should not be denied or abridged because of origin, age, background, or views" (ALA, 1996). While this does not directly address patron privacy, it does provide the underlying principle of the right of a person to use the library. Protecting a patron's privacy is one of the fundamental ways in which this right is upheld. This is made explicit in the third statement in the ALA Code of Ethics, which reads, "We protect each library patron's right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired or transmitted" (ALA, 2008).

The means by which libraries can uphold these principles is spelled out in the ALA Interpretation to the Library Bill of Rights (ALA, 2014). The task force reviewed the contents of this document and applied several guidelines for the privacy policy. First, we as an institutional

Privacy Statement for Grand Valley State University

Grand Valley State University has created this statement in order to demonstrate our firm commitment to privacy. The following discloses our practice for gathering and disseminating information for this site.

Information gathering

We use your IP address to help diagnose problems with our server and to administer our Web site by identifying (1) which parts of our site are most heavily used, and (2) which portion of our audience comes from within the Grand Valley State University network. We do not link IP addresses to anything personally identifiable. This means that user sessions will be tracked, but the users will remain anonymous.

Our staff occasionally monitors search terms that users enter into the GVSU Search Engine (http://google.gvsu.edu/), but this tracking is never associated with individual users.

Use of information

The GVSU uses the information gathered above to tailor site content to user needs, and to generate aggregate statistical reports. At no time do we disclose site usage by individual IP addresses.

All contact information (email address) or demographic information (geographic location) that we capture through this web site is voluntarily supplied.

Security

This site has security measures in place to protect the loss, misuse and alteration of the information under our control.

Contacting the Site Administrator

If you have any questions about this privacy statement, the practices of this site, or your dealings with this site, please contact us.

This site contains links to other sites. GVSU is not responsible for the privacy practices or the content of these other Web sites.

Fig. 1. Grand Valley State University privacy statement.

organization should collect the least amount of information for as little time as is necessary to fulfill a particular aspect of the libraries' mission. Second, we needed to keep this information secure and private. And third, our privacy statement should cite and/or link to all relevant laws, policies, and statutes that relate to, influence and/or supersede the above two principles so that our patrons would be fully informed.

CMU CENTRAL MICHIGAN UNIVERSITY | University Libraries

Resources ▾ Services ▾ About Us ▾ Get Help ▾ Global Campus Library Clarke Historical Library

CMU Libraries > Policies > Privacy Policy

Privacy Policy

Last Updated: 8/22/04

Privacy of the Users of the University Libraries

Applies to: All Library Users

It is the policy of the Libraries that the privacy of all library patrons shall be respected. Unless required by law, library staff will not reveal registration or circulation records.

Furthermore, the Libraries subscribe to the Code of Ethics of the American Library Association.

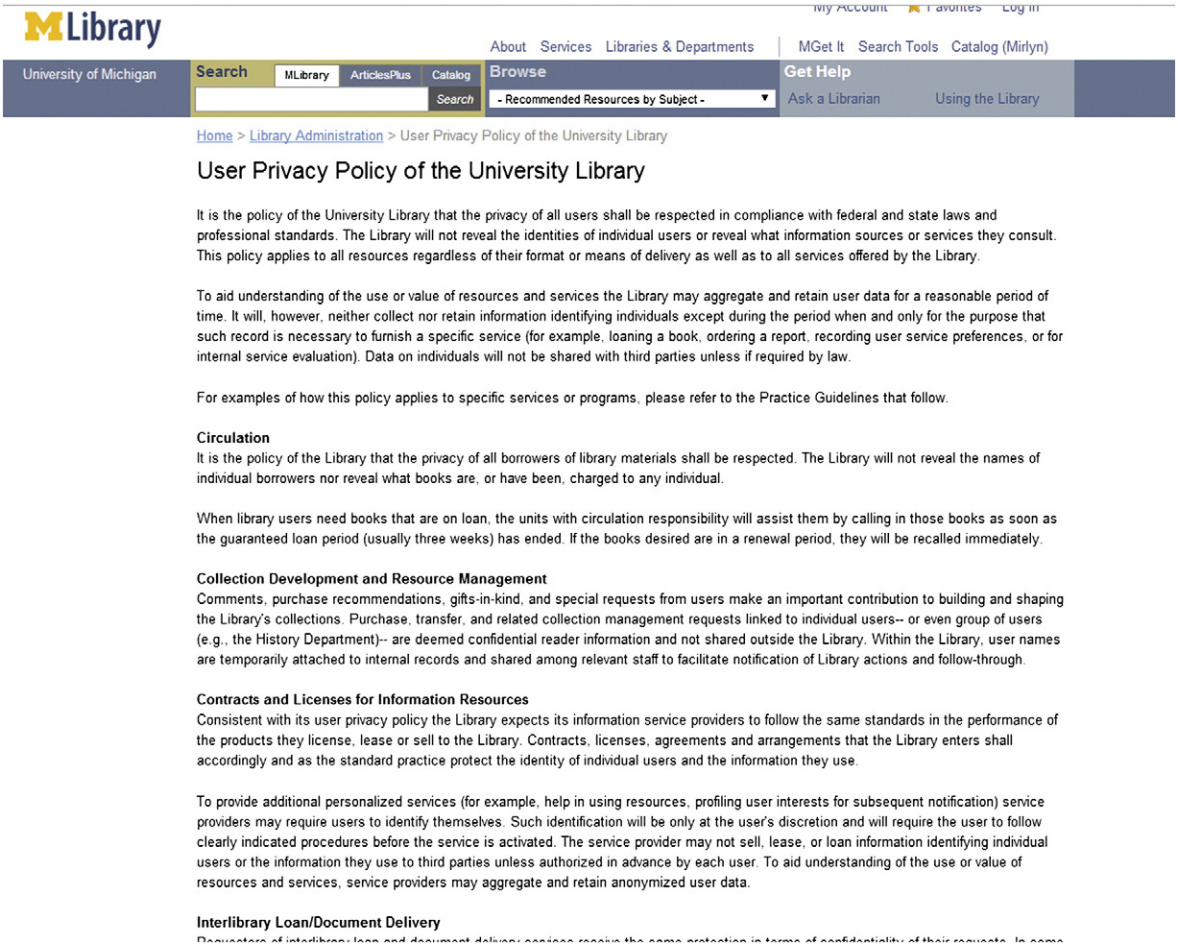
Section III of the Code of Ethics states:

We protect each library user's right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired or transmitted.

Further, library staff are required to respect the privacy of all students in accordance with Family Educational Rights and Privacy Act of 1974 (FERPA).

If you have questions, please contact Kathy Irwin, Associate Dean of Libraries at (989) 774-6421.

Fig. 2. Central Michigan University Libraries' privacy policy.



MLibrary

University of Michigan

About Services Libraries & Departments | MGet It Search Tools Catalog (Mirlyn)

Search MLibrary ArticlesPlus Catalog Search

Browse - Recommended Resources by Subject -

Get Help Ask a Librarian Using the Library

Home > Library Administration > User Privacy Policy of the University Library

User Privacy Policy of the University Library

It is the policy of the University Library that the privacy of all users shall be respected in compliance with federal and state laws and professional standards. The Library will not reveal the identities of individual users or reveal what information sources or services they consult. This policy applies to all resources regardless of their format or means of delivery as well as to all services offered by the Library.

To aid understanding of the use or value of resources and services the Library may aggregate and retain user data for a reasonable period of time. It will, however, neither collect nor retain information identifying individuals except during the period when and only for the purpose that such record is necessary to furnish a specific service (for example, loaning a book, ordering a report, recording user service preferences, or for internal service evaluation). Data on individuals will not be shared with third parties unless if required by law.

For examples of how this policy applies to specific services or programs, please refer to the Practice Guidelines that follow.

Circulation
It is the policy of the Library that the privacy of all borrowers of library materials shall be respected. The Library will not reveal the names of individual borrowers nor reveal what books are, or have been, charged to any individual.

When library users need books that are on loan, the units with circulation responsibility will assist them by calling in those books as soon as the guaranteed loan period (usually three weeks) has ended. If the books desired are in a renewal period, they will be recalled immediately.

Collection Development and Resource Management
Comments, purchase recommendations, gifts-in-kind, and special requests from users make an important contribution to building and shaping the Library's collections. Purchase, transfer, and related collection management requests linked to individual users-- or even group of users (e.g., the History Department)-- are deemed confidential reader information and not shared outside the Library. Within the Library, user names are temporarily attached to internal records and shared among relevant staff to facilitate notification of Library actions and follow-through.

Contracts and Licenses for Information Resources
Consistent with its user privacy policy the Library expects its information service providers to follow the same standards in the performance of the products they license, lease or sell to the Library. Contracts, licenses, agreements and arrangements that the Library enters shall accordingly and as the standard practice protect the identity of individual users and the information they use.

To provide additional personalized services (for example, help in using resources, profiling user interests for subsequent notification) service providers may require users to identify themselves. Such identification will be only at the user's discretion and will require the user to follow clearly indicated procedures before the service is activated. The service provider may not sell, lease, or loan information identifying individual users or the information they use to third parties unless authorized in advance by each user. To aid understanding of the use or value of resources and services, service providers may aggregate and retain anonymized user data.

Interlibrary Loan/Document Delivery

Fig. 3. University of Michigan Ann Arbor Libraries' privacy policy.

EXISTING FEDERAL, STATE, AND UNIVERSITY POLICIES

In its work, the task force also recognized the importance of complying with applicable federal and state laws. As we identified the major service points where personal information may be collected, we sought the identified university policies that impacted our services to, and resources for, patrons. From our understanding of these resources, the task force identified the most relevant policies to refer to within our privacy statement.

At the federal level, FERPA proved to be the most relevant guiding document (20 U.S.C. § 1232g; 34 CFR Part 99). As aforementioned, this statute protects the privacy of student education records, and it impacts how academic libraries represent and protect patron privacy. Because this law applies to all schools that receive funds under an applicable program of the U.S. Department of Education, virtually any academic library must comply with FERPA. Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record, but FERPA does allow disclosure of those records without consent to a variety of parties or under several conditions (34 CFR § 99.31). This includes, for example, school officials with legitimate educational interest, other schools to which a student is transferring, specified officials for audit or evaluation purposes, appropriate parties in connection with financial aid to a student, organizations conducting certain studies for or on behalf of the school, accrediting organizations, compliance with a judicial order or lawfully issued subpoena, appropriate officials in cases of health and safety emergencies, and State and local authorities, within a juvenile justice system.

As one of the 48 states with a statute protecting library patron privacy, the Michigan Library Privacy Act was also relevant to our work. Michigan citizens are protected by Chapter 397, Act 455 of 1982 of the Michigan Compiled Laws. In short, library records are not subject to the Freedom of Information Act except by court order. If someone, either the collective library or any one individual, violates this and can be identified, the wronged may bring about civil action for actual damages or $250 (whichever is greater), reasonable attorney fees, and the costs of bringing about the action. For other academic libraries across the country, considering whether your state has a similar statute is important to include in addressing patron privacy and confidentiality.

And, at the university level, the task force found a number of OU policies that impacted the content of our privacy statement and called for consideration in the Libraries' continued efforts to ensure privacy and confidentiality of patron information. For instance, the

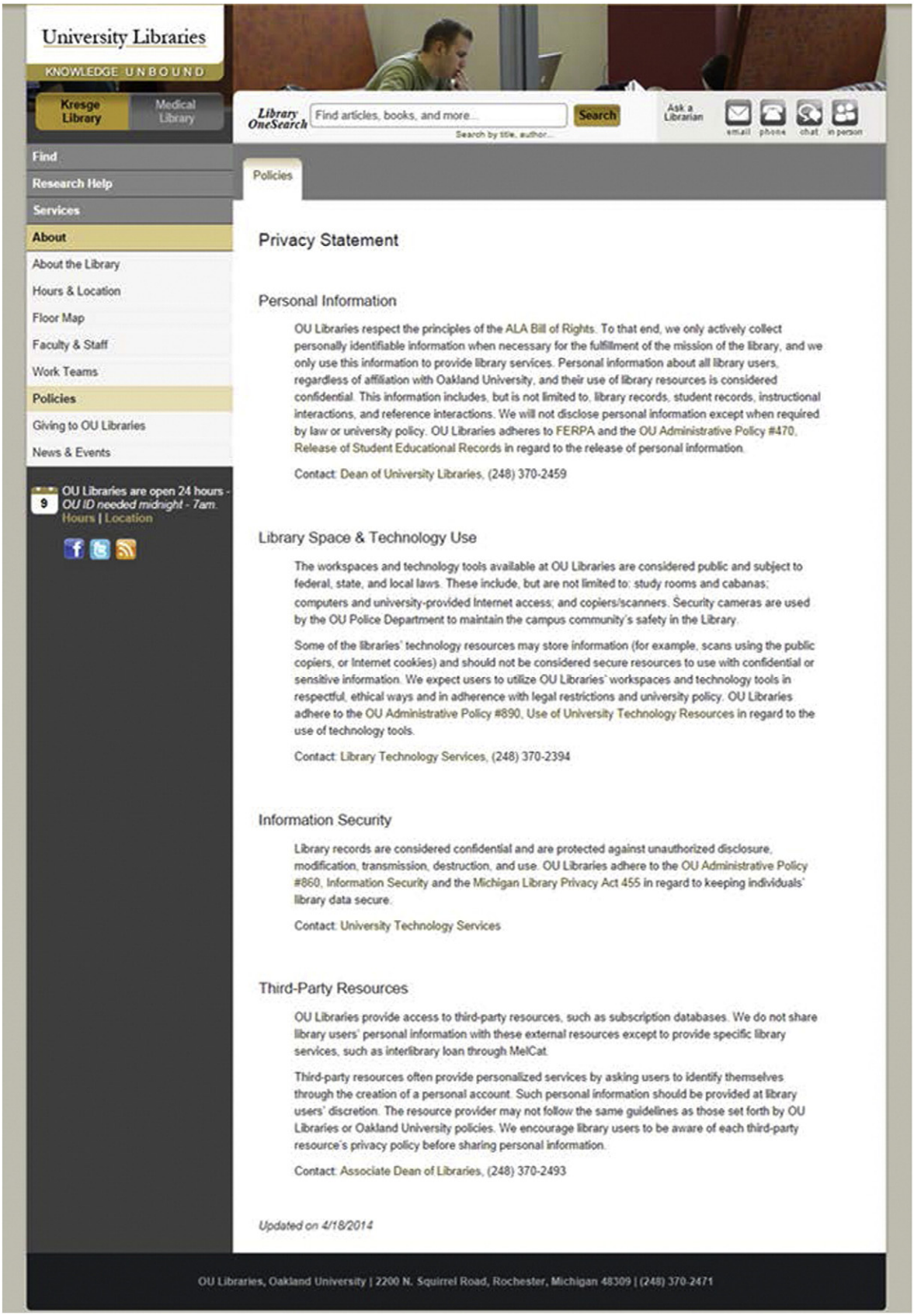


Fig. 4. OU Libraries' privacy statement — image contains identifying information.

university-wide privacy policy, which states its adherence to FERPA and is based on the principles of confidentiality and the student's right to privacy, notes that all members of the faculty, administration and clerical staff must respect confidential information about students which they acquire in the course of their work. Additionally, it gives each of the University's record-keeping administrative units (i.e., University Libraries) the authority to develop additional specific procedures in accordance with University's general policy (Oakland University Board of Trustees, 2001).

Several more specific university policies also guided the task force's development of the Libraries' privacy statement. OU's Release of Student Records policy, created to ensure compliance with FERPA, impacts all university employees who handle student records and was therefore important to address. It states that OU owns educational records and must keep a record of requests for access to and disclosures of personally identifiable information from each student's educational record; this information was relevant to share with library patrons (Oakland University Board of Trustees, 2013b). Also, the university policy on Student Records Retention, which guides all OU departments in the retention and disposal of student records, ensures that the institution and its units meet regulatory and legal requirements, minimize risk, optimize the use of space, and minimize cost. Because library-specific transactions, including purchase orders, circulation bills/fine records, Interlibrary Loan invoices, and reciprocal borrowing agreements, are specifically enumerated in this policy, it was also important to incorporate into the Libraries' public privacy statement (Oakland University Board of Trustees, 2010). OU's Information Security policy also specifically names library records as confidential data that are restricted from open disclosure to the public; stating this in the Libraries' statement helped to demonstrate the institution's strong commitment to patron privacy (Oakland University Board of Trustees, 2013a). And in recognition of the increasing impact of information and digital technology on privacy and confidentiality, the task force referenced OU's guidelines for the Use of University Information Technology Resources. This policy states that technology should not be used to infringe on or limit individual privacy (Oakland University Board of Trustees, 2008). While these particular policies are institution-specific, they represent academic institutions which may have similar guidelines that should be addressed by academic libraries' privacy statements.

SURVEYING STAKEHOLDERS

Once the task force had completed a draft of the public privacy statement, we shared it with the appropriate stakeholders in a series of meetings. These gatherings helped us collect feedback on our work and identify where, in the Libraries' systems and services, the statement would have an impact. In addition, these feedback sessions established buy-in from the Libraries' many departments, which will be essential going forward. Also, these discussions helped us to identify *possible* next steps for each impacted area while recognizing that there is not a one-size-fits-all approach for every impacted service or system.

In the task force's initial identification of the departments affected by a privacy policy, Access Services and Library Technology Services appeared to be the units most impacted by a public privacy statement. After our feedback sessions, though, we realized how concerns of patron privacy and confidentiality permeated virtually every aspect of the Libraries. Stakeholder feedback revealed that, whether through the collection of personal information, the use of library technology tools, third-party resources, or information security concerns, the Libraries' departments affected by a privacy statement included Access Services, Archives and Special Collections, Library Systems, Instruction, Research/Scholarship, Web Services, Research Help/Reference, Library Technology Services, Administration, Medical Library, and the personal use of resources for all library faculty and staff (see Appendix A). From this identification, each affected department was charged with developing appropriate procedures to address gaps between the university's policies, the Libraries' new public privacy statement, and existing procedures.

Once the task force made revisions based on the feedback generated in these meetings, the public privacy statement and list of affected areas were then shared with the OU Libraries' Operations, Assessment, and Management (OAM) group for further review. Comprised of Libraries' staff who have administrative appointments and management or coordination roles, this group's main function is to address cross-team operational issues and projects. Members of OAM asked for one small revision (the re-phrasing of a reference to library donor information); the task force integrated this feedback into our public privacy statement before passing it – along with a full report of work – onto the Libraries' Administrative Leadership Team (ALT), which provides managerial leadership, strategic planning, and directions of the operations for OU Libraries. ALT acted as the final decision-making authority before the privacy statement went from a discussion item to a public statement representing the Libraries' interpretation of policy. While ALT members provided additional points of clarification for both the statement and the areas impacted, they were universally supportive of the statement. Once the statement and impacted areas chart were modified per this feedback, they were resubmitted to ALT and received final approval.

CONCLUSION AND NEXT STEPS

After much collaboration and several rounds of edits, the task force accomplished its aims in April 2014. As for the task force's central goal, an official OU Libraries privacy statement was posted on the Libraries' website and *truly* became public (see Fig. 4). The statement concisely reflects the library's commitment to keep information about Library patrons private and confidential.

The second – and final – step of task force's work is now in the hands of the Libraries' faculty and staff, and it will continue as an ongoing process. Every department received the list of areas affected by the new privacy statement, and each unit is now responsible for determining appropriate next steps based on the task force's suggestions. This approach allows each library group to ensure that they adhere to the Libraries' privacy statement in ways that work for *them*. For example, this may involve appointing an individual/individuals to coordinate each area's efforts or coordinating with other work teams to co-develop and implement procedures, or it may involve team-wide audits of systems and procedures to determine where gaps or break-points exist. Once these work teams have implemented procedures, guidelines, and best practices for adhering to the public privacy statement, it will be important to conduct regular audits. Such a practice will serve to both ensure that procedures, guidelines, and best practices are occurring and to determine if they need to be revised on a regular basis.

While early library policy was in place to ensure that patrons could confidentially access the library collection without shame or embarrassment, library technology has evolved to the point where patron data has grown to include library listservs, library donor information, and even student-grading material — information not considered, or even conceived of, by past policies. Although an Access Services audit prompted action on a public privacy statement, it is evident that ensuring patron privacy is the responsibility of every library department. The task force's work identified areas for immediate next steps and areas where, in the future, ongoing investigation and exploration may benefit OU Libraries. Continuing to ensure patron privacy and confidentiality as technology develops will be an important responsibility *across* library departments.

APPENDIX A. AREAS OF LIBRARY WORK AFFECTED BY PUBLIC PATRON PRIVACY STATEMENT

Work team/GROUP	Area impacted	Personal information	Library technology use	Information security	Third-party resources	Recommended next steps
Access Services	Circulation	X	X	X		Create internal policy and procedures for compliance.
	Fines and fees	X	X			
	Room reservations	X				Identify if information could be limited to directory information. If not, review how user information may be collected and stored, and develop procedures for retention/removal.
	Access Services email	X				Identify if information could be limited to directory information. If not, review how user information may be collected and stored, and develop procedures for retention/removal.
	Access Services shared drive	X				Review current practices. Minimize storage of personal information.
	Guest accounts — library	X	X	X		Identify if information could be limited to directory information. If not, review how user information may be collected and stored, and develop procedures for retention/removal.
	Guest accounts — Bradford					Work with Library Technology Services to adopt their developed policy (see below)
	Course Reserves	X	X	X		Create internal policy and procedures for compliance.
	ILL (including postal program)	X	X	X		Create internal policy and procedures for compliance.
	Paper comments	X				Respond if necessary and shred immediately (current practice)
Administration	Student scholarship information	X		X		Develop procedures for storing and retaining student information; consider whether any information beyond directory information needs to be retained
	Student files and faculty gradebooks for credit-based courses	X		X		Develop procedures for storing and retaining student information and faculty gradebooks
Archives & Special Collections	Donors	X		X		Review how user information may be collected and stored
	Collections	X		X		Setting up access restrictions policies and procedures
	Reference	X		X	X	Develop guidelines/best practices for reference librarians
Instruction	IL sessions feedback	X	X	X		Develop guidelines/best practices for data storage
	IL-related grades	X		X		Review how user information may be collected and stored, and develop procedures for record/information transfer with Administration
	LIB 250: grades, student work	X				Review how user information may be collected and stored, and develop procedures for record/information transfer with Administration
Library Faculty & Staff — personal use of resources	Personal email with library user information	X				Develop guidelines/best practices for retention and disposal; identify if true disposal is possible (Google?)
	Personal calendar with library user information, including subject-specific research consultation appointments	X				Develop guidelines/best practices for retention and disposal; identify if true disposal is possible (Google?)
Library systems	Voyager	X	X			Identify if information could be limited to directory information. If not, review how user information may be collected and stored, and develop procedures for retention/removal.
	Millennium	X			X	Identify if information could be limited to directory information. If not, review how user information may be collected and stored, and develop procedures for retention/removal.
	ILLiad	X	X		X	Identify if information could be limited to directory information. If not, review how user information may be collected and stored, and develop procedures for retention/removal.
	OUR@Oakland	X				Review how user information may be collected and stored

APPENDIX A. *(continued)*

Library Technology Services	Guest accounts — Bradford	X	X			Develop procedures to be adopted by all areas that participate in the service
	Technology loans in exchange for identification (i.e., driver's license)	X				Develop procedures for handling and storing of ID documents at the tech help desks
	Tech Help interactions in person	X				Develop best practices for respecting user privacy
Medical Library	Email reference	X	X			Develop guidelines/best practices for retention and disposal; identify if true disposal is possible (Google). If not, review any changes that should be made to limit personal information shared.
	In-person reference	X				Develop guidelines/best practices for data storage, retention, and disposal
	Instruction sessions feedback	X	X			Develop guidelines/best practices for data storage
	Instruction-related grades	X				Review how user information may be collected and stored, and develop procedures for record/information transfer with Administration
	Web & paper forms	X				Review current practices. Minimize storage of personal information.
Research/Scholarship	Research data	X	X	X	X	Develop guidelines/best practices for handling research data
Research Help/reference	Research Help interactions in person	X				Develop guidelines/best practices for reference librarians
	Research Help interactions via chat	X			X	Develop guidelines/best practices for retention and disposal; identify if true disposal is possible (Trillian). If not, review any changes that should be made to limit personal information shared.
	Research Help interactions via email (ref@oakland.edu)	X				Develop guidelines/best practices for retention and disposal; identify if true disposal is possible (Google). If not, review any changes that should be made to limit personal information shared.
	Research consultations — information in YouCanBook.Me	X			X	Develop guidelines/best practices for retention and disposal; identify if true disposal is possible (Google/YouCanBook.Me). If not, review any changes that should be made to limit personal information shared.
	Research consultations — information in emails	X				Develop guidelines/best practices for retention and disposal; identify if true disposal is possible (Google). If not, review any changes that should be made to limit personal information shared.
	Guest accounts — Bradford	X	X			Work with Library Technology Services to adopt their developed policy (see below)
	RefWorks	X			X	Review how user information may be collected and stored
Web Services	Web forms	X		X		Review current practices. Minimize storage of personal information.
	Certificates of Completion (plagiarism, WRT 160, etc.)	X		X		Review current practices. Minimize storage of personal information.

REFERENCES

Adams, H. R. (2006). Protecting the privacy of student patrons. *School Library Media Activities Monthly*, *23*(3), 35.

Adams, H. R. (2007). Social networking and privacy: A law enforcement perspective. *School Library Media Activities Monthly*, *23*(10), 33.

American Library Association (1996, January 23). *Library Bill of Rights.* (Retrieved from http://www.ala.org/advocacy/intfreedom/librarybill).

American Library Association (2008, January 22). *Code of ethics of the American Library Association.* (Retrieved from http://www.ala.org/advocacy/proethics/codeofethics/codeethics).

American Library Association (2009). *The USA Patriot Act.* (Retrieved from http://www.ala.org/advocacy/advleg/federallegislation/theusapatriotact).

American Library Association (2014, July 1). *Privacy: An interpretation of the Library Bill of Rights.* (Retrieved from http://www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy).

American Library Association (2014b). Privacy tool kit library privacy talking points. *Key messages and tough questions* Retrieved from http://www.ala.org/advocacy/privacyconfidentiality/toolkitsprivacy/library-privacy-talking-points-key-messages-and-tough-questions.

Bowers, S. L. (2006). Privacy and library records. *The Journal of Academic Librarianship*, *32*(4), 377–383.

Case, D. O. (2010). A framework for information policies with examples from the United States. *Library Philosophy and Practice*, *13*(9).

Coombs, K. A. (2004). Walking a tightrope: Academic libraries and privacy. *The Journal of Academic Librarianship*, *30*(6), 493–498.

Fifarek, A. (2002). Technology and privacy in the academic library. *Online Information Review*, *26*(6), 366–374.

Griffey, J. (2010). Chapter 5: Social networking and the library. *Library Technology Reports*, *46*(8), 34–37.

Jones, B. M. (2009). Librarians shushed no more: The USA Patriot Act, the "Connecticut Four," and professional ethics. *Newsletter on Intellectual Freedom*, *58*(6), 195–198.

Jones, B. M. (2010). Chapter 2: Libraries, technology, and the culture of privacy a global perspective. *Library Technology Reports*, *46*(8), 8–12.

Lamdan, S. S. (2013). Why library cards offer more privacy rights than proof of citizenship: Librarian ethics and Freedom of Information Act requestor policies. *Government Information Quarterly*, *30*(2), 131–140.

Magi, T. J. (2007). The gap between theory and practice: A study of the prevalence and strength of patron confidentiality policies in public and academic libraries. *Library and Information Science Research*, *29*(4), 455–470.

Oakland University Board of Trustees (2001, October). *Administrative policy 1130: Family Educational Rights and Privacy Act.* (Retrieved from http://www.oakland.edu/policies/1130).

Oakland University Board of Trustees (2008, June). *Administrative policy 890: Use of university information technology resources.* (Retrieved from http://www.oakland.edu/policies/890).
Oakland University Board of Trustees (2010, November). *Administrative policy 481: Records retention and disposal.* (Retrieved from http://www.oakland.edu/policies/481).
Oakland University Board of Trustees(2013a, March). *Administrative policy 860: Information security.* (Retrieved from http://www.oakland.edu/policies/860).
Oakland University Board of Trustees(2013b, December). *Administrative policy 470: Release of student educational records.* (Retrieved from http://www.oakland.edu/policies/470).
State of Michigan Legislative Council (1982). *The Library Privacy Act.* (Retrieved from http://www.legislature.mi.gov/(S(42r3wj3dbeixfwfc0m5ed555))/mileg.aspx?page=GetObject&objectname=mcl-Act-455-of-1982).
Stevens, R. S., Bravender, P., & Witteveen-Lane, C. (2012). Self-service holds in libraries. *Reference and User Services Quarterly*, *52*(1), 33–43.
Sturges, P., Davies, E., Deamley, J., Iliffe, U., Oppenheim, C., & Hardy, R. (2003). User privacy in the digital library environment: An investigation of policies and preparedness. *Library Management*, *24*(1/2), 44–50.
Sturges, P., Teng, V., & Iliffe, U. (2001). User privacy in the digital library environment: A matter of concern for information professionals. *Library Management*, *22*(8/9), 364–370.
Sutlieff, L., & Chelin, J. (2010). 'An absolute prerequisite': The importance of user privacy and trust in maintaining academic freedom at the library. *Journal of Librarianship and Information Science*, *42*(3), 163–177.
U.S. Department of Education (2014). *Family Educational Rights and Privacy Act (FERPA).* (Retrieved from http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html).
United Nations (1948). *The Universal Declaration of Human Rights.* (Retrieved from http://www.un.org/en/documents/udhr/).
Vaughan, J. (2004). Policies governing use of computing technology in academic libraries. *Information Technology and Libraries*, *23*(4), 153–167.
Vaughan, J. (2007). Toward a record retention policy. *The Journal of Academic Librarianship*, *33*(2), 217–227.
Zimmer, M. (2013). Assessing the treatment of patron privacy in library 2.0 literature. *Information Technology and Libraries*, *32*(2), 29–41.
Zimmer, M. (2014). Librarians' attitudes regarding information and internet privacy. *The Library*, *84*(2).