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

A R T I C L E   I N F O

Article history:
Received 9 September 2014
Accepted 31 October 2014
Available online 8 December 2014

Keywords:
Academic libraries
Privacy policy
Patron privacy

A B S T R A C T

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).

However, 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...
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, Fifearek (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 (Fifearek, 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, Sutliff 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 requester 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.

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 GV/SU Search Engine (http://gvdsu.edu), but this tracking is never associated with individual users.

Use of information
The GV/SU 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. GV/SU 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.

Fig. 2. Central Michigan University 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.
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 Releasing 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, 2013a). 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

<table>
<thead>
<tr>
<th>Work team/GROUP</th>
<th>Area impacted</th>
<th>Personal information</th>
<th>Library technology use</th>
<th>Information security</th>
<th>Third-party resources</th>
<th>Recommended next steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Services</td>
<td>Circulation</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>Create internal policy and procedures for compliance.</td>
</tr>
<tr>
<td></td>
<td>Fines and fees</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>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. 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. 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. Review current practices. Minimize storage of personal information.</td>
</tr>
<tr>
<td></td>
<td>Room reservations</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>Work with Library Technology Services to adopt their developed policy (see below)</td>
</tr>
<tr>
<td></td>
<td>Access Services email</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access Services shared drive</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Guest accounts — library</td>
<td>X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Guest accounts — Bradford</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Course Reserves</td>
<td>X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ILL (including postal program)</td>
<td>X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Paper comments</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Administration</td>
<td>Student scholarship information</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>Develop procedures for storing and retaining student information; consider whether any information beyond directory information needs to be retained</td>
</tr>
<tr>
<td></td>
<td>Student files and faculty gradebooks for credit-based courses</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>Develop procedures for storing and retaining student information and faculty gradebooks</td>
</tr>
<tr>
<td>Archives &amp; Special Collections</td>
<td>Donors</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>Review how user information may be collected and stored</td>
</tr>
<tr>
<td></td>
<td>Collections</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>Setting up access restrictions policies and procedures</td>
</tr>
<tr>
<td></td>
<td>Reference</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>Develop guidelines/best practices for reference librarians</td>
</tr>
<tr>
<td>Instruction</td>
<td>IL sessions feedback</td>
<td>X X X</td>
<td></td>
<td></td>
<td></td>
<td>Develop guidelines/best practices for data storage</td>
</tr>
<tr>
<td></td>
<td>IL-related grades</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>Review how user information may be collected and stored, and develop procedures for record/information transfer with Administration</td>
</tr>
<tr>
<td></td>
<td>LIB 250: grades, student work</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>Review how user information may be collected and stored, and develop procedures for record/information transfer with Administration</td>
</tr>
<tr>
<td>Library Faculty &amp; Staff — personal use of resources</td>
<td>Personal email with library user information</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>Develop guidelines/best practices for retention and disposal; identify if true disposal is possible (Google?)</td>
</tr>
<tr>
<td></td>
<td>Personal calendar with library user information, including subject-specific research consultation appointments</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>Develop guidelines/best practices for retention and disposal; identify if true disposal is possible (Google?)</td>
</tr>
<tr>
<td>Library systems</td>
<td>Voyager</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>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. 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. 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. Review how user information may be collected and stored</td>
</tr>
<tr>
<td></td>
<td>Millennium</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ILLiad</td>
<td>X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>OUR@Oakland</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**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 | | | 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 | | Develop guidelines/best practices for data storage |
| | Web & paper forms | X | | Review how user information may be collected and stored, and develop procedures for record/information transfer with Administration |
| Research/Scholarship | Research data | X | X | Review current practices. Minimize storage of personal information. |
| | Research Help interactions in person | X | | Develop guidelines/best practices for handling research data |
| | Research Help interactions via chat | X | X | Develop guidelines/best practices for reference librarians |
| | Research Help interactions via email (ref@oakland.edu) | 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 consultations — information in YouCanBook.Me | 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. |
| | 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 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**


