Library Patron Privacy in Jeopardy

An analysis of the privacy policies of digital content vendors

April D. Lambert
Graduate School of Library & Information Science
University of Illinois at Urbana-Champaign
501 E. Daniel St.
Champaign, IL 61820
adlambe2@illinois.edu

Michelle Parker
Graduate School of Library & Information Science
University of Illinois at Urbana-Champaign
501 E. Daniel St.
Champaign, IL 61820
miparke2@illinois.edu

Masooda Bashir
Graduate School of Library & Information Science
University of Illinois at Urbana-Champaign
501 E. Daniel St.
Champaign, IL 61820
mnb@illinois.edu

ABSTRACT
While the library profession has long defended readers' privacy, a public library patron's personal information is no longer solely in the hands of intrepid librarians determined to defend intellectual freedom. Libraries use vendors to provide a large portion of their digital content. These vendors gain access to extensive personal information about patrons. Libraries often must negotiate with content providers to ensure privacy protections for their patrons that are in accordance with the American Library Association's Code of Ethics. This paper presents the results of a content analysis of the privacy policies of five of the top digital content vendors of American public libraries. We examined whether these privacy policies (1) meet the privacy standards of the library community, (2) meet other industry standards, and (3) are accessible and understandable to public library patrons. Our results demonstrate that while vendors are largely meeting the Fair Information Practices standards of American industry, the policies fail to meet the heightened standards of the library community.

ASIST 2015,November 6-10, 2015, St. Louis, MO, USA.

Keywords
Privacy; fair information practices; public libraries; digital content.

INTRODUCTION
The American Library Association (ALA) has long held that privacy is a core value of librarianship. Every version of the ALA's *Code of Ethics* since the first in 1939 has included a reference to protecting the confidentiality of patrons' reading records (Magi, 2010). The current version, adopted in 2008, reads: "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." Interpretations of the ALA's Library Bill of Rights have stated that the "privacy of library users is and must be inviolable" (Academic Libraries, 2000). The ALA views privacy as foundational to intellectual freedom because it is essential for free speech, free thought, and free association. Surveillance of library users' behaviors, either directly or by obtaining their records, creates a chilling effect that inhibits the users' rights to free speech and association. Users have full access to information only when they do not have to worry about surveillance, judgment, or ostracism (OIF, 2002; Magi, 2010). The ALA stresses that reading choices are not necessarily a reflection of intended behavior – "Just as people who borrow murder mysteries are unlikely to be

murderers, so those seeking information about terrorism are unlikely to be terrorists" (Privacy Toolkit, 2014).

The ALA's concern about patron privacy is not just hypothetical. In early October 2014, a writer for *The Digital Reader*, a blog dedicated to news and reviews about e-readers and digital publishing, discovered that Adobe was collecting extensive data about readers who used their Digital Editions 4 (DE4) software to read e-books on their computers and other platforms (Hoffelder, 2014). DE4 logged what documents readers added to their local library and the details of what they did with them, and then sent that data back to Adobe *unencrypted*, allowing anyone monitoring network traffic to see and collect the data (Gallagher, 2014). Adobe's initial response to these reports was that their data collection was used solely to manage the rights to documents across multiple platforms, and that the activity was in accordance with their privacy policy. This explanation, however, failed to satisfy the ALA. DE4 is used to manage and read not only e-books purchased by readers, but also e-books borrowed from public libraries, which have a long history of protecting reader privacy. In response to the news of Adobe's data collection, ALA President Courtney Young stated:

"People expect and deserve that their reading activities remain private, and libraries closely guard the confidentiality of library users' records. The unencrypted online transmission of library reader data is not only egregious, it sidesteps state laws around the country that protect the privacy of library reading records" (ALA, 2014).

Adobe eventually agreed to encrypt the data, but the ALA also expressed concern that more data than is necessary to manage licensing rights was being collected and retained.

In the press release on the Adobe DE4 security flaw, the ALA encouraged its membership and library patrons to continue the discussion of privacy and digital content vendors (ALA, 2014). Many public libraries now provide services to their patrons that allow them to borrow all sorts of digital content, including e-books, audiobooks, movies, music, e-magazines, and other digital materials. While libraries have a long and storied history of protecting the privacy of their readers, digital lending services have introduced a number of other service providers – many of which do not have a history of being concerned for privacy – into the process. When a patron borrows an e-book from their local public library, for instance, they usually do so from a vendor contracted by their library to provide this service. In order to read the e-book, the patron must download the book to their computer or other e-book reader. This means that for an e-book, data can be collected by at least three parties: the library, the service vendor, and the e-reader company. Libraries may be committed to protecting their readers' privacy, but are the vendors? Adobe's response to the DE4 issue indicates that libraries and vendors may not be on the same page in regard to reader privacy.

The ALA's Digital Content Working Group and Intellectual Freedom Committee are actively working to develop advice and best practices around patron privacy for digital materials. The patron's personal information is no longer solely in the hands of intrepid librarians determined to defend intellectual freedom. Libraries must work with multiple vendors to negotiate privacy protections for patrons. Libraries are also forced to deal with the privacy policies of entities with which they have no direct relationship, including companies such as Adobe and Amazon, which offers the popular Kindle e-reader. This paper seeks to contribute to the discussion of these issues by conducting a content analysis of the privacy policies of several of the top digital content vendors contracted by American public libraries. We examine the following research questions:

1. Are digital content vendor privacy policies accessible and understandable to public library patrons?
2. Do digital content vendor privacy policies meet the standards of the library community?
3. Do these privacy policies meet other industry standards?

The examination of these three questions is essential in the continuation of the struggle in relation to the discussion on patron privacy rights in an increasingly digitalized world. It is hoped that the findings of this paper will provide librarians with the knowledge of what to look for when negotiation contracts with digital content vendors. It is only through this negotiation process can the librarians assert and fight for the adherence of vendors to the ALA's commitment of library patrons right to privacy when it comes to their lending record.

PATRON PRIVACY IN AMERICAN PUBLIC LIBRARIES

The library profession's commitment to patron privacy

The attitude of librarians toward issues relating to patron privacy and confidentiality revolves around the commitment to privacy espoused in the ALA's *Code*. Bowers (2006) emphasizes, "if individuals do not feel that they can read information regarding controversial or non-controversial topics, their ability to learn and expand their knowledge is infringed and impeded." In her article about patron privacy in regards to their library records, Bowers first attempts to define privacy and discusses the issue that the U.S. Constitution does not explicitly guarantee its citizens a right to privacy. It is only in the penumbras of less specific Constitutional Amendments that any privacy rights are recognized by law, and so professional organizations such as the ALA are left to develop their own guidance for defining privacy rights and responsibilities. Often the efforts of the ALA to protect library patrons' privacy has come in direct conflict with government

surveillance efforts. For almost a century, the federal government has viewed library records as a potential source of intelligence about potential criminals, dissidents, and other targets of government attention (Bowers, 2006). In the 1940s, the FBI sought patron records for individuals under investigation, and the House Un-American Activities Committee sought records in the 1950s. During the 1960s and 1970s, the Alcohol and Tobacco Tax Division of the IRS sought information about patrons who were borrowing books that could provide information about making explosives. In the 1980s the FBI developed the "Library Awareness Program," in which librarians at research libraries were asked to report on the reading and research habits of "foreigners" and other individuals considered to be Cold War security risks (Magi, 2010). The USA PATRIOT Act, passed after the attacks of September 11, 2001, extended the authority for federal agencies to request library patron records (Bowers, 2006).

Beyond making statements about the importance of privacy, librarians have a long history of standing up to efforts from law enforcement and other government agencies to collect confidential patron data. Librarians have repeatedly criticized efforts by federal authorities to collect records and have sometimes been able to successfully resist producing the records (Bowers, 2006). The ALA, at the instigation of Columbia University librarian Paula Kauffman, publicized the FBI's Library Awareness Program and coordinated resistance to it. Some librarians, prohibited by the PATRIOT Act from publicizing government requests for records, posted signs stating how many days had passed *without* a request (Egelko and Gaura, 2003). A library in Washington State contested an FBI subpoena to produce a list of names of all patrons who had borrowed a biography of Osama bin Laden; the FBI eventually withdrew the subpoena (Bowers, 2006).

The ALA has also been successful in lobbying for state laws that protect the confidentiality of patron records. Forty-eight states have laws protecting at least circulation records, while the other two states have statements from their attorneys general indicating the same (Klinefelter, 2007). These state laws however, are overridden or trumped by federal laws that allow federal agencies to seek library records (Bowers, 2006). No federal legislation or case law protects the privacy of library records. Efforts to enact such legislation in the 1980s were opposed by the FBI and failed. The PATRIOT Act actually extended the reach of the federal government to access records of all types, including library records (Bowers, 2006).

Often unable to resist the force of government requests, many libraries protect their patrons' privacy by declining to keep records of patron in-library activity and deleting all circulation records after material has been returned (Estabrook, 1996). Without any records to hand over, libraries can effectively resist government requests. Some have noted that this practice puts libraries at a disadvantage, as they cannot use patron data to improve their services and manage their collections (Estabrook, 1996). Additionally, in the modern digital age, libraries often do not have control over their patrons' records, and cannot delete, modify, or otherwise shield them. As mentioned in the introduction, when users borrow e-books from a public library their data may be collected by the library, the e-book vendor, and their e-reader company. Many libraries, such as the Chicago Public Library system, use third party vendors to manage, or at least provide a user interface, for their websites and catalogs. Even when designed in-house, these websites often integrate a number of so-called "Web 2.0" or "Library 2.0" tools, such as tagging, ratings systems, bookshelves, and social media links (Zimmer, 2013). These tools, helpful as they may be for accessing and organizing information, generate far more data than traditional circulation records ever could. Because sharing is the point of these tools, the FBI no longer needs to collect records from the library. They can simply obtain a library card and then go online to "share" information with their fellow patrons.

Privacy standards applicable to library patron records

The standards that guide the privacy activities of American libraries should, by extension, also apply to the digital content vendors who are collecting patron reading and viewing data, as well. These standards derive from three primary sources (Magi, 2010). The first is the ALA's *Code of Ethics* and the supporting policies that have been developed by the ALA to interpret the *Code* and provide further guidance for American librarians. The second source is the guidelines developed by the International Coalition of Library Consortia (ICOLC), which overlaps the ALA's efforts to some extent but often provides more specific enforcement requirements. The third source, which is particularly applicable in the digital vendor context, is the Fair Information Practices (FIPs) guidelines, developed by industry to address the collection and management of electronic data. An exploration of the three sets of standards demonstrates that, taken together, they provide a robust set of guidelines upon which to evaluate the current privacy practices of public library digital content vendors.

While the ALA *Code of Ethics* refers only broadly to the profession's interests in protecting the privacy and confidentiality of its patrons, the organization has issued a number of policies, interpretations, and regulations that provide far more specific, applied guidance for librarians. The "Policy on Confidentiality of Library Records" requires that libraries explicitly adopt a policy indicating that personally identifiable information in patron records be kept confidential. In "Privacy: An Interpretation of the Library Bill of Rights," the ALA elucidates on patrons' privacy rights, including the right to be informed about why information is collected and the right to be provided with information about how to maintain their privacy. The ALA has also passed a "Resolution on the Retention of Library Usage Records," which instructs libraries to limit the information they collect, to avoid creating unnecessary records, and to maintain the security of these records.

Libraries are also instructed to conduct regular "privacy audits" to ensure that their practices continue to comply with ALA guidelines. The ALA has also issued several policies specifically directing libraries not to produce records to government agencies without a court order.

The ICOLC Guidelines (2002) echo many of the points articulated by the ALA's myriad privacy policies, but the ICOLC also specifically states that its guidelines are applicable to library vendors. The ICOLC Guidelines direct vendors that they must have a written privacy policy located on the website that is easy to locate and easy to comprehend. They also require that vendors explicitly state their adherence to the ALA's *Code of Ethics*. In addition to requiring vendors to limit their data collection, the ICOLC Guidelines direct vendors to regularly review the functioning of their site in light of their privacy policies and to ensure that users may still have access to the site even if they decline to have their information collected. Particularly relevant to digital content vendors, the ICOLC Guidelines state that vendors must retain full control over their website so that third parties, including advertisers and ISPs, cannot violate patron's privacy.

The third set of standards, FIPs, are not library-specific but rather were developed by the technology industry and government agencies to provide guidance for companies managing data (Magi, 2010). Though none of the FIPs standards have been adopted as law in the United States, many companies refer to these standards when developing their privacy policies. FIPs emphasize five principles: (1) Notice/Awareness, (2) Choice/Consent, (3) Access/Participation, (4) Integrity/Security, and (5) Enforcement/Redress. Many American companies focus their efforts only towards the first two, concluding that notice and consent suffices for fulfilling their privacy obligations (Bashir, Hoff, Hayes and Kesan, 2014). Each of the FIPs emphasizes providing users with sufficient information and opportunities to self-manage their privacy. Thus, applied to the library context, FIPs place few explicit responsibilities on the vendors, but rather require opportunities for library patrons to access and manage data collected about them. This is in stark contrast to the library profession's policies, which impose positive duties on constituent libraries. FIPs are still relevant to this analysis, however, because digital content vendors may operate more broadly as technology companies, not just library service providers. Thus, FIPs may be the guiding principles relevant to the development of their privacy policies.

METHODOLOGY

To answer our research questions, we needed to identify the digital content vendors used most frequently by American public libraries and review their privacy policies. We began with the ALA's list of the top twenty-five libraries by size of population served.[1] This list enabled the authors to then put together a list of outside resources used by these libraries by manually going to their websites and searching for the resources linked to on the library websites. In some cases the list outside resources was easy to find, often in one centralized location. In other cases the resources had to be found through exploring the website in detail. There were, at the time this data was collected, 287 outside resources (or specific services provided by larger companies) found using publicly available information from the homepages of the top twenty-five libraries. Resource usage exhibited a long-tail structure, with 246 of these resources used by just one library system.

During this process we identified that there were two main types of outside resources used by libraries. The first group, which we have termed "vendors," is companies with which the libraries appear to have contractual relationships to provide certain services, such as e-book or audiobook borrowing or video streaming. The most frequently used vendor was OverDrive, an e-book and audiobook vendor, used by twenty-two of the twenty-five library systems. The second group are resources provided by other companies or institutions to which the libraries referred the users of their website, but with which the libraries appear to have no formal relationship. Examples of these resources include Project Gutenberg and Ancestry.com. This paper to examines in-depth the policies of the first group, the vendors that appear to be providing services for the libraries. This limitation yielded six vendors, though one of these vendors, a streaming music and video service called Freegal, did not have a privacy policy. Thus, five vendors are assessed in-depth in this paper. Table 1 lists the vendors reviewed in-depth in this paper, their services, and how many library systems use their services. These five vendors offer a diverse range of services and overwhelmingly represent the companies with which large library systems are negotiating service contracts (save for the vendor without a privacy policy). An additional fourteen outside resources were also reviewed to assess whether the privacy protections offered by those companies differed than those with which libraries have contractual arrangements.

For each vendor, the authors accessed the privacy policy by navigating to the vendor through a library website. Once on the page, the authors used observation to determine the shortest route to access the privacy policy. As discussed below, three of the vendors included links to their privacy policy clearly labeled on the vendor's landing page. The policies, once located, were copied and pasted into both a PDF document and a text file, and the details of when and how they were accessed were recorded.

[1] Retrieved from http://www.ala.org/tools/libfactsheets/alalibrary factsheet13#toppopulation

Vendor	Service(s)	Number of Libraries Served
Axis 360	E-Books	7
Hoopla	Videos, Music, Audiobooks	9
OneClickDigital	Audiobooks	12
OverDrive	E-Books, Audiobooks	22
Zinio	Magazines	18

Table 1. Vendors and services.

The coding book used to conduct this analysis was based largely on the rubric used by Trina Magi in her 2010 article in which she examined whether academic research services vendors met library privacy standards. Readers interested in the specific coding questions may contact the authors to request the book, which Magi requested we keep confidential. To ensure that the questions on the survey were understood completely by the coders, there was a test run of the coding template performed on two policies outside of the focus population. The results of the test run allowed for greater refinement of the coding template. The authors also added several questions to Magi's codebook relating to security and data storage. Two of the authors, graduate students, evaluated each policy using the codebook. While the percentage of intercoder agreement is reported, it was difficult to calculate an intercoder reliability index due to the small sample size, the limited number of coders, and the nature of the coding questions, most of which offered only two or three coding choices (Lombard, Snyder-Duch, and Campanella, 2008). Where there was disagreement between the coders, the option most generous to the vendor was recorded. Any question for which there was less than 80% agreement between the coders across the five policies was eliminated from the results on the basis that the question was ambiguous. Thus, two of the original questions were rejected.

To answer these research question regarding ease of access and readability, the Flesch-Kincaid readability tools in Microsoft Word were employed. The ease of access was determined based on the number of clicks to access the policy from the vendor's landing page, as recorded when the policies were collected.

RESULTS & DISCUSSION

Accessibility & Comprehension

Each vendor's website was accessed through the website of a public library. A link from the library's site leads users to a landing page for the vendor, sometimes branded with the library's name and logo but often clearly a third party's website. Those sites that retain the home library's branding may confuse patrons, who may believe they are still on their library's website and thus subject to the privacy policy of their library's site, rather than the vendor's. To evaluate the accessibility of vendor policies, the number of clicks required to access the policy from the vendor's landing page from a library portal was recorded. Three of the vendors -- Axis 360, Hoopla, and OneClickDigital -- had links to their privacy policy on their landing pages, requiring just one click to get to the policies. OverDrive and Zinio each required three clicks to reach the privacy policies. One of the vendors determined to be in the top five of those used by public libraries, Freegal, which provides streaming music and video services, had no privacy policy available at its website at all. These results indicate that, while there are inconsistencies in this small sample, most vendors had policies, and they are available within several clicks from the vendor's landing page.

The comprehensibility of the digital content vendors' privacy policies was evaluated using word count and the Flesch-Kincaid Readability Tests, using the tools provided by Microsoft Word. Table 2 presents the results of this evaluation. The Flesch Reading Ease scale calculates the number of words, sentences, and syllables in a document to determine the difficulty of the material (Wolfe, 2003). The lower the number, the more difficult the passage is to read and comprehend. Two of the policies scored less than a 30.0, indicating that they are best suited to be understood by university graduates. The other three were similarly advanced. All five scored as being written at a twelfth-grade reading level, the highest level available in the measure. These results are concerning, as they indicate that the policies may be too difficult for the average library patron to understand. In her study of academic vendor policies, Trina Magi (2010) determined that those policies also averaged at a twelfth-grade level. The alarm Magi expressed over the readability challenges for academic vendor policies is heightened here. The users of the vendor services Magi explored were university students who presumably read at least a twelfth-grade level; the average public library patron is likely lower than that of university students.

Vendor	Wordcount	Flesch Reading Ease	Flesch Grade Level
Axis 360	694	34.5	12.0
Hoopla	1094	35.4	12.0
OneClickDigital	1249	40.0	12.0
OverDrive	1705	28.5	12.0
Zinio	1851	29.5	12.0

Table 2. Comprehensibility factors.

	# of Vendors	% of Vendors
Advertising	5	100
Processing sales/ transactions	5	100
Research & development	5	100
Facilitate communication	5	100
Monitor compliance	3	60
Other	1	20

Table 3. Vendors' stated reasons for collecting PII (Intercoder agreement = 87%)

Privacy Policy Content Analysis

The content analysis of the digital content vendors' privacy policies generated extensive data regarding the extent to which the vendors were meeting library profession and industry standards. After evaluating the data, we determined that the vendors were largely meeting industry standards – at least those standards, such as a notice and consent, typically adopted by American companies. The vendors overwhelmingly were not meeting the heightened standards of the library profession, however. The overall conclusion is that these vendors are operating just as any other digital companies, with little regard for any special expectations for library patrons.

One area in which all five vendors were deficient was in their stated efforts to enforce their privacy policies and regularly conduct audits. None of the five vendors provided an explanation of how they enforce their policies, nor did any state that they conduct privacy audits. Also none of the vendors referenced the ALA *Code of Ethics*, as required by the ICOLC Guidelines. Only one vendor included an assertion that the enforcement of the privacy policy was regularly reviewed; the other four were silent as to whether or how the policy was actually enforced. In fact, there were almost no references at all in the policies to libraries. For the most part, the policies seemed to have been drafted ignorant of library professional standards.

Vendors were more successful in informing users that personally identifying information (PII) would be collected and for what purposes. All five vendors' policies explained what user information was collected and why. Table 3 lists the reasons given by vendors for collecting PII. None of the vendors, however, provided advice to the users on how to protect their privacy, which is required by the ALA's interpretation of the library user's Bill of Rights. Vendors also generally failed to state whether they took steps to avoid creating unnecessary personally identifying records or whether they dispose of unneeded records, both of which are required under ALA guidelines. In fact, the only vendor to mention either of these topics indicated that it *did not* dispose of unneeded records. In accordance with industry practices under FIPs, the digital content vendors seem to believe that they are responsible only for providing notice to their users, not for taking affirmative steps to ensure that user privacy is maintained.

As with notifying users about what PII was being collected, vendors were also forthcoming about what PII was shared with third parties. Table 4 shows the myriad reasons why vendors would share users' information. Most of the policies were drafted quite broadly in this area, providing few limits on when and with whom user information may be shared. Several of the policies claimed that they would protect users' information and not share it, unless otherwise described in the policy. This intention was typically undercut by the fact that the policy would then go on to list a number of contexts in which information actually *would* be shared. There seemed to be a disconnection between espoused intentions and allowances made for possible information sharing. The myriad reasons given by vendors for sharing information appear to have been drafted to avoid liability if information were to be shared, intentionally or unintentionally, rather than with the protection of patrons in mind.

	# of Vendors	% of Vendors
To monitor compliance	4	80
For advertising & promotion	2	40
To process commercial transactions	3	60
For research and/or production development	2	40
To protect the safety of employees or public	4	80
To administer or protect the website/server	1	20
In relation to a legal proceeding	3	60
In connection with a sale or merger	3	60
Other general reasons	1	20
Other	0	0

Table 4. Vendor reasons for sharing PII (Intercoder Agreement = 86%)

	# of Vendors		% of Vendors	% Inter-coder Agreement
Contact info provided	5		100	100
Giving of PII voluntary	1		20	80
User may view PII held by vendor	Yes	2	40	100
	Doesn't say	3	60	
User may contest accuracy or completeness of PII held by vendor	Yes	3	60	80
	Doesn't say	2	40	
User may delete all PII held by vendor	Yes	1	20	100
	Doesn't say	3	60	
	No	1	20	
Vendor allows access when user denies permission to distribute PII	Yes	1	20	80
	Doesn't say	4	80	

Table 5. User consent and access.

The theory behind FIPs is that users should take control of protecting their own privacy. To be able to exercise this control, users must have opportunities to view, contest the accuracy of, and delete PII held by a vendor. Table 5 shows that vendors were particularly vague when it came to defining the rights users have to control their data. Many of the policies did not address these issues, and those that did often provided users only with limited access, revision, and deletion rights. All of the policies, however, did provide contact information so that users could initiate efforts to try to achieve some of these goals.

The last significant topic addressed in the content analysis was whether vendors took steps to ensure the security of the data they hold, whether they inform users about where they store their data, and whether they use third party cloud storage service providers. While four of the five vendors state that they take steps to ensure the security of users' information, none provided much information about where records were stored or whether they used cloud services. The one policy that referenced where they stored records was vague, indicating only that records may be transmitted across borders. This was clearly in an effort to satisfy the European Union's safe harbor requirements for transborder information transfers, not to provide users with information about where their data is located. Four of the policies mentioned that they used encryption, with three specifically referencing the Secure Socket Layer protocol. It is possible that some of these issues are addressed in separate security policies, but library patrons concerned with where their information is being stored are unlikely to find much guidance in these privacy policies. With more and more storage depending on the cloud, and the attendant privacy issues with that, users would likely desire to get some of this information in the relevant privacy policy.

Policies of other outside resources

While five policies is a small number, these are the vendors that are actually being used by public libraries to provide digital services to their patrons. We also reviewed of the policies of an additional fourteen outside resources that were used by at least one-fourth of the top twenty-five library systems. All of these resources had privacy policies in some form, though their length and coverage varied. While the data for these policies is not yet been reviewed in depth, the trend seems to be holding that the vendors are meeting industry standards but not library standards. For example, none of the additional fourteen policies reference the ALA Code of Ethics, but thirteen of the policies do state that the vendor collects PII and give reasons for both collection and sharing. The one aberrant policy is for Project Gutenberg, which claims not to collect any PII and disclaims the user's IP address as PII, a conclusion that seems problematic. Future work in this area should examine further the privacy policies of these resources and other websites to which libraries refer their patrons.

CONCLUSION

This project identified some areas where public library digital content vendors are failing to meet the library profession's privacy standards. Vendors generally fared poorly regarding the comprehensibility of their policies based on readability measures, but all vendors (except the one with no policy at all) made their privacy policies easily accessible on their sites. Overall, vendors were more likely to meet the information technology industry standards articulated in the FIPs guidelines than library-specific guidelines. Thus, librarians who do negotiate contracts with vendors may need to educate them on the library profession's privacy expectations and how they differ from broader information technology industry expectations. Research into the actual negotiation process would provide useful information for libraries that will most likely face similar negotiations in the defense of patron privacy.

If libraries are not able to negotiate more privacy protections, patrons should be clearly notified when they are no longer being protected by their home library's privacy policy. Patrons will likely have difficulties understanding when they are using a service provided by their home library, when they have been linked to a vendor's website, and when they have been linked out to the wider Internet. This would be solved by libraries adding

a portal page between the website that is library controlled and the vendor's page to warn patrons that they are no longer being protected by the library's privacy policy. There is a need for research for research into whether patrons suffer such confusion, what libraries are doing to ameliorate the confusion, and the implications for patron privacy.

Other areas for future research include going beyond privacy policies to gather more information about vendors' security efforts, negotiation techniques to ensure that future third party adhere to the ALA Code of Ethics, and examining how e-reader platforms treat the privacy of library patrons. Even if libraries and digital content vendors take steps to protect patron privacy, these efforts could be for naught if e-reader services like Adobe violate patron privacy. These future research projects, coupled with our work, the work of Trina Magi, and others who have examined library privacy policies, could be used to paint a full picture of how patron privacy is protected in the age of cloud service providers. Equipped with this information, librarians responsible for protecting their patrons would have the tools to educate vendors and negotiate contracts that are more reflective of the profession's standards.

ACKNOWLEDGMENTS

Thank you to Trina Magi of the University of Vermont Libraries for graciously sharing her codebook with us. Thank you also to Hsiao-Ying Huang and Megh Patel who assisted with some of the coding.

REFERENCES

American Library Association. (2014). Adobe responds to ALA on egregious data breach; some action expected by week of Oct. 20 [Press Release]. Retrieved from http://www.ala.org/news/press-releases/2014/10/adobe-responds-ala-egregious-data-breach-some-action-expected-week-oct-20.

American Library Association. [Academic Libraries] (2000). Intellectual freedom principles for academic libraries: an interpretation of the library bill of rights. Retrieved from http://www.ala.org/advocacy/intfreedom/librarybill/interpretations/intellectual.

American Library Association. [Code of Ethics] (2008). Code of ethics of the American Library Association. Available at http://www.ala.org/advocacy/proethics/codeofethics/codeethics.

American Library Association. [Privacy Tool Kit] (2014). Privacy Tool Kit. Available at http://www.ala.org/advocacy/privacyconfidentiality/toolkitsprivacy/privacy.

American Library Association. [ALA Fact Sheet 13] (2014). Available at http://www.ala.org/tools/libfactsheets/alalibraryfactsheet13.

Bashir, M., Hoff, K.A., Hayes, C.M., and Kesan, J.P. (2014). Knowledge-based Individual Privacy Plans (KIPPs): A Potential Tool to Improve the Effectiveness of Privacy Notices. Carnegie Mellon University, CyLab Workshop on the Future of Privacy Notice and Choice, June 27th, 2014. Pittsburgh, PA. Available at https://www.cylab.cmu.edu/news_events/events/fopnac/pdfs/bashir.pdf.

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

Burkell, J., and Carey, R. (2011). Personal Information and the Public Library: Compliance with Fair Information Practice Principles/Les renseignements personnels dans les bibliothèques publiques: le respect des principes d'équité dans les pratiques de collecte de renseignements. *Canadian Journal of Information and Library Science*, *35*(1), 1-16.

Corrado, E. Privacy and library 2.0: how do they conflict. In *Sailing into the Future: Charting Our Destiny: Proceedings of the Thirteenth National Conference of the Association of College and Research Libraries, March 29-April 1, 2007, Baltimore, MD*. Ed. Hugh Thompson. Chicago, IL: ACRL.

Egelko, B. and Guara, M.A. (2003, Mar. 10) Libraries post Patriot Act warnings. *San Francisco Gate*. Available at http://www.sfgate.com/news/article/Libraries-post-Patriot-Act-warnings-Santa-Cruz-2664869.php.

Estabrook, L. S. (1996). Sacred Trust or Competitive Opportunity: Using Patron Records. *Library Journal*, *121*(2), 48-49.

Gallagher, S. (2014, Oct. 7). Adobe's e-book reader sends your reading logs back to Adobe—in plain text [Updated]. *Ars Technica.* Available at http://arstechnica.com/security/2014/10/adobes-e-book-reader-sends-your-reading-logs-back-to-adobe-in-plain-text/.

Gressel, M. (2014). Are libraries doing enough to safeguard their patrons' digital privacy? *The Serials Librarian, 67*(2): 137-142. DOI: 10.1080/0361526X.2014.939324.

Hoffelder, N. (2014, Oct. 6). Adobe is spying on users, collecting data on their ebook libraries. *The Digital Reader.* Retrieved from http://the-digital-reader.com/2014/10/06/adobe-spying-users-collecting-data-ebook-libraries.

Holley, R. (2013). Are libraries compromising reader privacy with circulation reminders? *Indiana Libraries, 32*(1): 42-44.

International Coalition of Library Consortia. (2002). Privacy Guidelines for Electronic Resource Vendors.

Available at http://icolc.net/statement/privacy-guidelines-electronic-resources-vendors.

Johnston, S.D. (2000). Rethinking privacy in the public library. *International Information and Library Review, 32*: 509-517.

Kesan, J. P., Hayes, C. M., and Bashir, M. "Information Privacy and Data Control in Cloud Computing: Consumers, Privacy Preferences, and Market Efficiency", Washington and Lee Law Review, Forthcoming, Illinois Program in Law, Behavior and Social Science Paper No. LBSS12-11, Illinois Public Law Research Paper No. 11-20. Jan 11, 2013.

Klinefelter, A. (2007). Privacy and library public services: or, I know what you read last summer. *Legal Reference Services Quarterly, 26*(1-2): 253-279. DOI: 10.1300/J113v26n01_13.

Klinefelter, A. (2009). Library Standards for Privacy: A Model for the Digital World. *NCJL & Tech.*, *11*, 553.

Lombard, M., Snyder-Duch, J., and Campanella, B. (2008). Practical Resources for Assessing and Reporting Intercoder Reliability in Content Analysis Projects. Available at www.temple.edu/sct/mmc/reliability/.

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 & Information Science Research, 29*: 455-470.

Magi, T.J. (2008). A study of U.S. library directors' confidence and practice regarding patron confidentiality. *University of Vermont Libraries Faculty and Staff Publications*, Paper 16. Available at http://scholarworks.uvm.edu/libfacpub/16.

Magi, T. J. (2010). A content analysis of library vendor privacy policies: do they meet our standards?. *College & Research Libraries*, *71*(3), 254-272.

Nicholson, S., and Smith, C. A. (2005). Using lessons from health care to protect the privacy of library users: Guidelines for the de-identification of library data based on HIPAA. *Proceedings of the American Society for Information Science and Technology*, *42*(1).

Office for the Intellectual Freedom of the American Library Association (OIF). (2002). *Intellectual Freedom Manual*. Chicago, IL, American Library Association.

Rubel, L. (2014). Libraries, electronic resources, and privacy: the case for positive intellectual freedom. *The Library Quarterly, 84*(2): 183-208.

Sturges, P., Davies, E., Dearnley, J., Iliffe, U., Oppenheim, C., and Hardy, R. (2003). User privacy in the digital library environment: An investigation of policies and preparedness. *Library Management*, *24*(1/2), 44-50. DOI: 10.1108/01435120310454502.

Wolfe, M.B.W. (2003). Readability Indices. In *Encyclopedia of Education*, 2d edition. Ed. James Guthries, vol. 6. New York: MacMillan Reference USA.

Zimmer, M. (2013). Assessing the treatment of patron privacy in library 2.0 literature. *Information Technology and Libraries, 32*(2). DOI: 0.6017/ital.v32i2.3420.

Zimmer, M. (2014). Librarians' attitudes regarding information and internet privacy. *The Library Quarterly, 84*(2): 123-151.