Developing a Consensus Framework to Support Patron Privacy in Digital Library and Information Systems

A Grant Proposal to the Andrew W. Mellon Foundation

From the National Information Standards Organization (NISO)

Submitted by
Todd A. Carpenter, Executive Director (Principal Investigator)

and

Nettie Lagace, Associate Director, NISO

Lisa Hinchliffe, Professor & Coordinator for Information Literacy Services & Instruction, University of Illinois at Urbana-Champaign

Bonnie Tijerina, Fellow, Data & Society Research Institute

Michael Zimmer, Associate Professor, University of Wisconsin-Milwaukee, and Director of the Center for Information Policy Research

January 22, 2015

Proposal Summary

This proposal outlines a request by the National Information Standards Organization (NISO) for $47,956 to undertake an early-stage consensus process among librarians, publishers, and systems suppliers to craft a framework of principles by which these communities might better understand and effectively manage potentially sensitive personally identifiable patron data. If approved and funded, this project will consist of four preparatory webinar discussions, an in-person day-and-a-half-long meeting in San Francisco during which a framework of principles will be developed and agreed upon. Following publication of the framework, another public webinar and several publicity efforts will be undertaken to disseminate information about the framework. It is anticipated that the framework will be considered for greater formalization via a NISO consensus process and publication as a NISO Recommended Practice, if the NISO Voting Membership approves such a move.

Awareness and interest in online privacy is growing rapidly following a number of significant data breaches that have occurred over the past year. There has been a growing concern regarding the effects of living in a data-saturated world on our rights to privacy at work, in our homes, and in places where we seek information. Several dozen data breaches involving universities, publishers, and libraries have been made public just in the past three years, with many more that likely have gone unreported or unacknowledged because disclosure requirements vary widely across the country.

Libraries have long been stalwart advocates for protection of patron privacy, but as the complexity of libraries' digital services has grown, the challenges of protecting that privacy have grown as well. Patron activity data is no longer held exclusively by the library, nor is it necessarily controlled by providers themselves. Compounding these problems is the tension created by the fact that real benefit can be achieved through the application of usage data as a tool for improving library services. When and in what ways can these data be used to improve services or build new services that might improve patrons' experiences? And how does one balance that against the need to protect privacy?

This delicate balance is one that NISO hopes to address through a process of engaging community consensus to develop a framework for addressing patron privacy in digital library systems, which will be considered for further formalization after the grant work is complete. By bringing together thought leaders and engaged members of the publishing, library, and systems vendor communities, this project will provide a forum for perspectives to be shared and benefits and drawbacks of various approaches to be discussed from multiple angles. Common and diverse viewpoints will better inform uptake of the output, which can be used by the entire community.

Background

The digital infrastructure through which content is provided via libraries to patrons involves a number of suppliers, including publishers and library systems providers. These systems generate a tremendous amount of activity and usage data, much of which can be tied back to a particular user. The complex web of systems interactions, of necessary data exchange to provide services, and the myriad providers of information necessitates a community effort and agreement on principles around patron data protection.

The library community has been a very vocal and ardent supporter of library patron privacy and has been very active in supporting privacy-related issues in the information community. This commitment is at the core of the American Library Association's *Code of Conduct*,[1] which stipulates: "III. 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." As institutions that provide their communities with intellectual resources, libraries consider respecting patrons' privacy about the content they receive a core service. No patron would want to be in the position of having his or her reading behavior monitored and shared without his or her consent. As the digital environment continues to grow, we do not expect that this commitment to privacy will diminish, but rather to expand as libraries join with other privacy organizations in advocating for legal protections.. Such political activities by the library community are an important part of the landscape of information policy.

However, libraries are no longer the sole actors on the stage of library services. Many core functions of libraries, such as lending and discovery and delivery of content—particularly digital content, but even physical content as well—are being managed externally by publishers and library systems vendors. For many of these providers, the notions of privacy, internal data protection, and data use are conceptualized significantly differently than those conceptualizations in the library profession. Commercial organizations are looking to add to their stores of "big data" and find ways to use it for product analysis, product development, and marketing.

Such data use is not always intrusive, especially when aggregated to separate out personally identifiable information, and can serve non-commercial purposes as well. Many libraries are potentially doing themselves and the communities they serve a disservice by failing to utilize data on patron activity in ways that could improve or enhance services. In some cases, this is due to the belief that such utilization may intrude on the patron's privacy. Newer information systems offer many opportunities for libraries to learn from this usage data if methods can be found for it to be used while still respecting the expectations of patron privacy.

A new generation of discovery tools that incorporate user behavior in ranking algorithms is one example. Other systems specifically focus on analyzing session log

data to surface relevant content to users. Many user interface and design activities incorporate patron activity analysis to improve the user experience. More intrusive data collection, such as personal file monitoring to ensure rights compliance and prevent piracy, or monitoring reading behavior to assess patrons' personal preferences for marketing purposes are also available. Beyond this, from a patron's perspective or even that of a library (as a customer of these systems), it is difficult to know precisely what companies or third parties are doing with the secondary or tertiary activity data being generated. In a presentation at NISO's 2014 virtual conference on *Library Data in the Cloud*, Eric Hellman illustrated that a single page load from the New York Public Library's Bibliocommons system connected to 10 different third-party sites, each of which has its own privacy policy about sharing the data that was collected,[2] which may or may not align with the Library's policy.

This proliferation of personal and business data has expanded the opportunities for hacking and the exposure of sensitive data in recent years. Data breaches among academic institutions and non-profit organizations—while generally less prominent and headline-catching than corporate data hacking—have become increasingly frequent. According to the Privacy Rights Clearing House, there have been 76 reported data breaches, by institutions as large as Johns Hopkins University, the University of Maryland, and Indiana University to smaller community colleges and even public school systems.[3] Breaches in the library domain may be less lucrative and therefore less frequent because of the relative lack of financial data, but they have occurred. A great deal of attention was directed at the Adobe Digital Editions data security issue in the fall of 2014, where reading and content use data was exchanged via an unencrypted data exchange protocol.[4] While this was the highest profile exposure of library data, it was by no means the only breach. In 2010, Delray Beach Public Library was the target of a cyber attack impacting its payroll system involving the theft of more than $160,000. The Wyoming State Library reported in November 2014 that its statewide online catalog was breached. [5] LibraryThing, a social cataloging web application, informed its users in February 2011 that it had been impacted by the breach of its online password system.[6] Data breaches among publishers and service providers have also occurred. In 2014, JSTOR issued a security notice indicating the compromise of approximately 800 user records.[7]. A recent breach of West Publishing House was reported to the New Hampshire Attorney General.[8] There are far more reports of data breaches than can be listed here, but the frequency of their occurrence is increasing.

There is a significant real cost of these breaches as well. The Ponemon Institute's research places average cost per record for data breaches in the US at $188-$198 for direct and indirect costs associated with a data breach.[9] While the costs vary by industry, the figures are still considerable for those communities involved in scholarly communication. For the education industry classification, Ponemon's report estimated the per capita cost of each record lost to be $111. Within the media market, the figure was slightly less at $103 and for the research market segment it was a bit higher at $125 per record lost.

NISO is well positioned to advance a discussion about patron privacy among the library community, the publishing community, and their system and service supplier communities because of the neutral third party forum it provides. Each of these communities plays an important role in delivering digital content and patron services, and as such each needs to be meaningfully engaged in these discussions, on equal footing, to explore a potential framework for privacy. Similarly, each of these systems and services relies on data exchange with other systems to function, creating a digital network that generates a tremendous amount of secondary usage and activity data, much of which is—or could be—personally identifiable.

NISO's neutral forum would be critical for any such framework to find successful adoption in the vendor communities. While libraries have a certain "power of the purse" and can negotiate favorable terms protecting patron privacy, not every institution is in a position to bargain with providers to achieve the same privacy protections. In addition, as libraries increasingly combine third-party services, they are losing control over what happens to their patrons' data.

Scope of the Proposal

NISO is seeking funding to support a series of virtual meetings, a facilitated day-and-a-half meeting in San Francisco in conjunction with the ALA Annual Conference in June 2015, the creation and distribution of a white paper that serves as a framework on privacy practices, and follow-up discussions of the recommendations in the white paper. This project will take place over a 12-month period beginning in early April 2015 and will carry through to the first quarter of 2016. The project will bring together 40-50 thought leaders in electronic library systems, library services, publishing, and other content provision for the in-person meetings and smaller subgroups of the larger community for the online pre-meeting discussions. Additional participants will be able to engage in the conversations virtually via live streaming of the meeting. Following the production of the report from these discussions, a series of presentations will be made at industry meetings to further advance the conversation and position the framework for advancing it to NISO Recommended Practice status, should it be approved as such by the NISO voting membership.

NISO frequently takes well-formulated existing documents through a consensus process, such as what is envisioned as an output from this thought leader initiative. This process would consist of a recommendation by NISO's Business Information Topic Committee[10] and a ballot to the NISO Voting members who would then be responsible for approving the effort. If approved, a working group would be organized to reach consensus and produce a final recommendation. In the case of a Recommended Practice—which this framework is expected to be—that document is then brought back to the Topic Committee for final approval. The development of this resulting framework as a NISO Recommended Practice would be a follow-up project not supported by this grant.

Existing Work

Privacy has long been near the forefront of the policy efforts focused on by the library community. The American Library Association (ALA) has done yeoman's work fighting in support of the right of privacy for library patrons, and for electronic data privacy more generally. Broadly speaking, much of ALA's activities related to privacy can be described as advocacy. While advocacy certainly has its place and can be (and has been) used effectively, there are other ways to accomplish similar goals. One such approach is through consensus development and adoption of recommended practices with interested parties. These approaches are complementary and can be used in tandem to achieve consistent goals.

Recently, a new group focused on these issues emerged when the Library Information Technology Association (LITA) division of ALA launched the Patron Privacy Technologies Interest Group. This group "will promote the design and implementation of library software and hardware that protects the privacy of library users and maximizes user ability to make informed decisions about the use of personally identifiable information by the library and its vendors."[11]

While there is some overlap with the work of this interest group—which includes among its goals to publish "recommendations on data security practices for library software"—this proposed NISO project is meaningfully different because of the broader scope and participation of the NISO membership and community. The LITA group's focus is primarily on library systems and comes at these questions strictly from a library perspective. Because, as noted above, many of the systems and services used today are operated outside of the library without library control or even potentially library influence, a strictly library-focused initiative will capture only one segment of this complex ecosystem.

The Center for Information Policy Research (CIPR) at the University of Wisconsin-Milwaukee also recently announced a project to begin in 2015.[12] According to its website, CIPR intends to undertake a "pilot research study to help us understand how libraries are implementing third-party cloud computing services, how these implementations might impact patron privacy, and how libraries are responding to these concerns."[13] In conversations with CIPR leadership, NISO has learned the project they are undertaking is focused on the data generated by social media services developed by some libraries and privacy issues related to those projects. CIPR's work is not focused *per se* on a library's own resource management infrastructure or the library systems that store or process content for patrons.

Beyond the library community, there is a broader movement toward incorporating greater privacy measures into various electronic systems due to recent security breaches and mass surveillance revelations. Privacy has been taken up at a governmental level for online activities of children in the U.S. (COPPA[14]). In early

January 2015, President Obama highlighted cybersecurity, data protection, and student data privacy as national priorities of his administration in the coming year.[15] Much more stringent privacy protections exist outside of the United States, such as those in Europe and in Canada. Organizations like the Electronic Frontier Foundation (EFF),[16] the Electronic Privacy Information Center (EPIC),[17] and the American Civil Liberties Union (ACLU)[18] have each been engaged to a greater or lesser degree on broader privacy and technology issues, sometimes partnering with libraries or library organizations sometimes partnering with libraries or library organizations.

While the privacy issues of these non-library organizations cut across the broad scope of data protection and privacy, which have some implications on the library and publishing communities, the areas of concern for this project are much more narrowly focused on the particulars of libraries, library systems, and information resources. Although they are important to overall data protection, broader information security issues, such as the security of WiFi systems, of payment processing and credit card services, and of data encryption standards are outside of the scope of NISO's work and the scholarly communications community generally; therefore these security themes are not topics that will be covered in this grant. While the larger political and social context of online information and the internet do impact on libraries and vendors, particularly vendors that provide services in an international context, the publishing and library systems market has its own digital workflows and traditions that deserve special consideration.

Project Description

This project will consist of three phases. The first will be a pre-meeting discussion phase, which will consist of four webinar discussion sessions. These will be organized and led by a steering committee under the direction of Todd Carpenter, the Principal Investigator of this project and NISO's Executive Director, as well as Nettie Lagace, NISO's Associate Director for Programs. Todd Carpenter's CV is included in Appendix C of this proposal. The proposed members of the project's steering committee will include:

- Marshall Breeding, Consultant, Library Technology
- Lisa Hinchliffe, Professor/Coordinator for Strategic Planning/Coordinator for Information Literacy Services & Instruction, University of Illinois at Urbana-Champaign
- Michael Zimmer, Associate Professor, University of Wisconsin-Milwaukee, and Director of the Center for Information Policy Research
- Bonnie Tijerina, Fellow, Data & Society Research Institute
- Peter Brantley, Director, Digital Library Applications, The New York Public Library

- Eric Hellman, President, Gluejar

Each of the webinars will be a three-hour discussion session designed to lay the groundwork for a productive in-person meeting. The sessions will focus on privacy in four specific areas related to library systems and information provision. A brief description of some of the issues to be discussed in each session is noted below. More detailed descriptions and agendas will be developed by the steering committee and in consultation with the invited participants.

1. **Privacy of internal library systems**
   Libraries host and maintain a variety of data systems to manage their workflows and services, particularly those related to electronic resources. These include traditional services such as catalog, circulation, and access control systems, but also reference systems, course and instructions tools, as well as the library's public facing website. Each of these systems generates data on use and patron activity. Patron activity data has been mined to improve web design and interfaces, improve discovery, assess collections use, and monitor for abusive activity.
2. **Privacy of publisher systems**
   As electronic content is increasingly licensed rather than purchased, these resources are provided by publisher web systems rather than directly from libraries. Publishers are responsible for tracking IP address information or user IDs to authorize access to content. The logs of this access are outside the control of libraries, and publishers compile these data using standards such as COUNTER19 to provide usage statistics. The analysis of logs and tracking of user behavior have long been used to improve systems activity, but few practices exist for how that data should be managed and cleared. As the demand for article and item level metrics grows, the granularity of use data is creating situations where usage is so narrow in some fields as to be personally identifiable among small niche communities. Publishers may not be constrained or bound by the same motivations as libraries in the use and disposition of these data once collected.
3. **Privacy of provider systems**
   Like publisher systems, a vast array of library systems are now outsourced to vendors who are responsible for catalog maintenance, discovery services, link resolvers, authentication systems, and even repository and circulation systems. These data streams contain a great deal of patron activity information, which may or may not be subject to library control. Additionally, e-book systems monitor specific user behavior for a variety of digital rights management purposes, usage tracking, and systems improvement reasons. To what extent is user behavior tracking acceptable under terms of use of digital systems? While data ownership of the primary data contained in these systems is well

stipulated, who owns the secondary data and how it may be utilized is frequently more ambiguous. Many service providers use these secondary usage data to support discovery systems and other tools or services.

4. **Legal aspects influencing data sharing, policies**
   The legal framework for data sharing, data breach reporting, and responsibility for the costs of a data breach vary greatly from jurisdiction to jurisdiction. Expectations of data privacy and data stewardship within the public also vary by community. While a great deal of activity is governed by licenses and online systems' terms of use, the role of legal protections is an important element and the question of whether contract or regulation takes precedence in areas of data privacy and data breaches isn't always clear.

Each of these sessions will explore the following core questions:

- What patron data is collected and shared by systems used by libraries?
- To what extent are these data shared with third parties or internal business units of unrelated service provision?
- How are or can these data be used to improve value in ways that improve patron experience or service?
- What is current practice regarding data shared between these systems to optimize their functionality?
- What interdependencies of data and services exist?
- Are there useful best practices for data cleansing and/or anonymization, or any existing controls for what data should "look like" when shared?
- Are there any privacy-related problems with these systems based on known data breaches in related systems?
- Should there be an ongoing mechanism for sharing best practices on breach prevention/information security in our community?

Each conversation will include approximately 8-12 people invited to participate to the in-person meeting (listed in Appendix A), who have expertise in the specific topic of the meeting. Prior to the online meeting, a public invitation will be circulated to encourage an additional 20-30 participants from the wider community to listen to the session though they will not engage directly in the conversation. Feedback from the audience will be gathered after the session via an online survey and these results will contribute to the in-person meeting discussions. These remaining virtual seats will be offered on a first-come, first-served RSVP basis. Each of these sessions will be recorded and the recordings posted to the NISO website for this project.

The project will also support hosting a day-and-a-half long meeting on June 29 (half day) and June 30 (full day) at the conclusion of the American Library Association meeting in San Francisco, CA. The meeting will consist of roundtable discussions on each of the four topics outlined in the webinars, based on a summary of the webinar discussions, and the implications of each component for a privacy framework. Following each discussion session, there will be an open discussion of the issues to obtain agreement on proposed key takeaways or action items related to that topic area, as proposed by the participants in the webinar discussion, and an exploration in total of those topics and how they fit with the other discussions. On the final day, the group will revisit all of the framework draft principles to assess any overlap or areas of agreement or disagreement and craft their recommendations.

A list of prospective participants for the in-person meeting is listed in Appendix A. A draft agenda for the in-person meeting is included in Appendix B.

After the draft is complete, the NISO staff, with support from the steering committee, will draft the report of the meeting. This draft will contain a summary of the discussions as well as a series of consensus points agreed to in the in-person meeting. It will also describe the areas of complexity where consensus could not be reached and that will require further work.

After the framework report is released, there will be another 2-hour free public webinar to review the preliminary results of the project. The NISO staff and the steering committee members will lead that final session.

Once completed, the patron privacy framework will be the topic of several presentations and peer-reviewed articles. We anticipate presenting this framework at the Digital Library Federation's fall meeting, the Charleston Conference on Issues in Book and Serial Acquisition, and the 2016 American Library Association Midwinter meeting. We will also seek to publish articles in *D-Lib Magazine*, *portal: Libraries and the Academy*, *Journal of the Association for Information Science and Technology (JASIST)*, or other appropriate library journals. We will also seek coverage of the project in *Library Journal*, *American Libraries*, *Information Today,* and other library media outlets.

Deliverables and Benefits of the Project

It is NISO's mission and commitment to make our activities as publicly available as possible. In support of this commitment, all of the outputs of this project will be captured and shared with the community free of charge with a liberal re-use license. The proposed meetings and webinars will be recorded and the resulting framework white paper will be distributed electronically for free via the NISO website. If the report is developed carefully with the right mix of involved people and organizations, it will serve as a coordination mechanism for those providing patron services to build more robust protections of patron privacy into their operations and systems. We envision the specific benefits of this project to be:

1. Raising awareness of the complexities surrounding digital systems, the personally identifiable data that they generate, and how those data are or can be used for various business or service-provision purposes, including improving or creating new services.
2. Furthering the conversation among libraries, publishers, and systems vendors around the proper balance between privacy and acceptable uses of patron data. Involvement of the publishers and vendors is particularly important as they have been less engaged in privacy discussions and their implications.
3. Ensuring that the needs and requirements of a diverse community of stakeholders are gathered and considered in the development of a privacy framework for libraries, content providers, and information vendors. This framework might also find additional applications outside of the traditional library community.
4. Streamlining the process of consensus development of a privacy framework for libraries, library systems, and publishers by highlighting areas of agreement regarding prioritization of data privacy.
5. Identifying areas where further conversations through a subsequent consensus process are necessary to address challenging problems.
6. Developing a checklist for libraries to enable them to more readily and easily assess their library-related services, content management systems, and collections development activities in regards to protection of patron privacy.

Once completed, the patron privacy framework will be the topic of several presentations and peer-reviewed articles. As noted above, the framework will be promoted through presentations at conferences and publications in library journals and more general library media outlets. These activities will position the framework for consideration by the NISO Business Information Topic Committee for possible advancement to NISO Recommended Practice status. This would require the approval by the NISO voting membership. The development of this resulting framework as a NISO Recommended Practice might require additional consensus development work, which would be a follow-up project that is not an aspect of this grant proposal.

Project Schedule

ACTION	Date	Staff Lead
Grant submission by NISO staff	February 2015	Carpenter
Grant determination by the Mellon Foundation	March 2015	Mellon Directors
Securing Location & Logistics	March 2015	Wood
Planning teleconference call led by NISO staff with steering committee members	April 2015	Carpenter/Steering Committee
Series of four webinars led by NISO staff and steering group members with teams of experts in each of 4 systems areas to provide input and planning for in-person meeting	May – June 2015	Steering Committee/Lagace/ Wood
Face-to-face meeting with invited participants to be held in conjunction with ALA Annual meeting (San Francisco, CA)	June 29/30, 2015	Carpenter/Lagace/ Wood
Preparation of public report and draft framework by NISO staff	July-August 2015	Carpenter/Lagace/ Hodgson
Release of public report and framework	September 2015	Carpenter/Lagace
Public discussion webinar of the draft framework, its details, and next steps.		
Public reporting by NISO staff and steering committee members at library conferences & papers submission to relevant publications	October 2015 - January 2016	Carpenter/Lagace
Final report/narrative submitted to Mellon Foundation prepared by NISO staff	March 15, 2016	Carpenter/Lagace/ Greenlun

NISO Staff

NISO staff that will be engaged in this project include:

Todd A. Carpenter, NISO Executive Director, Principle Investigator
Nettie Lagace, NISO Associate Director for Programs
DeVonne Parks, NISO Membership Engagement Manager
Juliana Wood, NISO Educational Programs Manager

Cynthia Hodgson, Technical Editor (outsourced)
Aaron Greenlun, Accountant (outsourced)

Intellectual Property

NISO is committed to the broad dissemination and allowable re-use of the content it generates. Consistent with this commitment, NISO will make the outputs of this project available to the community under a CC-BY-NC license. If a subsequent recommended practice is generated using the framework developed as a result of this work, NISO will distribute it freely under a liberal re-use license, but copyrighted to NISO so as to ensure the consistent representation of agreed community consensus. There will be no software code, data, or digital products, save the recordings of the webinars and the policy framework document.

Long Term Sustainability

NISO is committed to the long-term preservation of all the content and reports generated by our work. NISO has partnered with Portico for long-term preservation and availability of these documents, as well as with the University of Maryland for preservation of NISO's archives.

Subsequent development of the principles described in the framework white paper resulting from this project will be under the auspices of the NISO Business Information Topic Committee. If it chooses to advance this output as a NISO Recommended Practice, that would be subject to the approval of the NISO Voting Membership. Further development and consensus of additional standards or recommended practices related to privacy would be advanced by NISO as part of its mission to serve the library and vendor communities.

It is possible that the project might not receive sufficient support from either the Business Information Topic Committee and/or the NISO Voting Membership to advance to the status of a Recommended Practice. Within NISO's publication structure, there are several options for outputs of development work. These include White Papers, Technical Reports, Recommended Practices, and formally designated (ANSI/NISO Z39) standards. These documents constitute a sliding scale of lessor to greater consensus and increasing formality in approval of the document based on its path toward publication. Conceivably, if there is no consensus on a framework that is achieved or outlined during the meeting, NISO could publish the outcome of the meetings and the discussions simply as a grant report, which will be provided to the Foundation and made available on the NISO website. If the Framework is adopted by the participants, but not advanced by the Topic Committee, it would be published as a NISO White Paper. If the Business Information Topic Committee adopts the resulting Framework, but the recommendation to start a working group is not approved by the Voting Members, or if the working group once formed does not

reach consensus, the Topic Committee can publish the document either as a white paper or technical report. This publication structure aligns with all NISO efforts.

NISO is considering a separate proposal related to privacy as it relates to scientific data. That entirely separate project will likely focus on activities related but tangential to this proposed initiative. Specifically, that initiative is presently conceived as exploring best practices of sharing of personally identifiable data, anonymization of data, and practices for tracking the usage of scientific data in repository systems. Both projects, if approved, would proceed on separate, if parallel development tracks.

Reporting

NISO will comply with all reporting requirements described in the award letter if this grant is funded. Following completion of the project, NISO will submit a report to The Mellon Foundation by March 30, 2016. The report will summarize the work completed and the themes surfaced during the webinar discussions and during the in-person meeting. The framework white paper will also be prepared for submission to the NISO Business Information Topic Committee for consideration for further consensus development as a NISO Recommended Practice after the work on this grant is completed. The final report will contain the financial reports and commentary covering all of the expenditures made under the grant. Todd Carpenter and the NISO staff will compile the narrative report. The financial reports will be created and prepared by NISO's accountant.

References

[1] Code of Ethics of the American Library Association. Last amended January 22, 2008. http://www.ala.org/advocacy/proethics/codeofethics/codeethics

[2] Hellman, Eric. "Privacy in the Cloud." Presented at *NISO Virtual Conference: Library Data in the Cloud*, September 24, 2014. http://www.slideshare.net/BaltimoreNISO/sept-24-niso-virtual-conference-library-data-in-the-cloud-39486486?

[3] *Chronology of Data Breaches***.** Compiled and maintained by Privacy Rights Clearinghouse. http://www.privacyrights.org/data-breach/new

[4] Hoffelder, Nate. "Adobe is Spying on Users, Collecting Data on Their eBook Libraries." The Digital Reader Blog, October 6, 2014. http://the-digital-reader.com/2014/10/06/adobe-spying-users-collecting-data-ebook-libraries/

[5] "Hackers breach Wyoming library system." *The Washington Times*, November 8, 2014. http://www.washingtontimes.com/news/2014/nov/8/hackers-breach-library-system/

[6] "Security Notice and LibraryThing Password Reset." *The LibraryThing Blog*, February 4, 2014. http://blog.librarything.com/main/2014/02/password-reset/

[7] *JSTOR notifying 800 users that account information was accessed by unauthorized individual(s)*. Office of Inadequate Security, April 1, 2014. http://www.databreaches.net/jstor-notifying-800-users-that-account-information-was-accessed-by-unauthorized-individuals/

[8] *Memo from West Publishing to New Hampshire Office of the Attorney General RE: Legal Notice of Information Security Breach*. November 3, 2014. http://doj.nh.gov/consumer/security-breaches/documents/west-publishing-corporation-20141103.pdf

[9] *2013 Cost of Data Breach: Global Analysis*. The Ponemon Institute, May 28, 2013. http://www.ponemon.org/library/2013-cost-of-data-breach-global-analysis

[10] NISO Business Information Topic Committee. http://www.niso.org/topics/businfo

[11] Patron Privacy Technologies Interest Group. Library and Information Technology Association. http://www.ala.org/lita/about/igs/public/lit-Pp

[12] Center for Information Policy Research (CIPR). http://cipr.uwm.edu/

[13] *Privacy and Cloud Computing in Public Libraries.* Center for Information Policy Research. http://cipr.uwm.edu/?page_id=508

[14] Children's Online Privacy Protection Rule ("COPPA"). 16 CFR Part 312. http://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

[15] "Obama to Call for Laws Covering Data Hacking and Student Privacy." *The New York Times*, January 11, 2015. http://www.nytimes.com/2015/01/12/us/politics/obama-to-call-for-laws-covering-data-hacking-and-student-privacy.html?_r=0

[16] Electronic Frontier Foundation. https://www.eff.org

[17] Electronic Privacy Information Center. http://www.epic.org/

[18] "Rein in the Surveillance State." American Civil Liberties Union. https://www.aclu.org/rein-surveillance-state