2015–2016 ALA CD#19.3-CD#19.9_62716_ACT
2016 ALA Annual Conference

ALA Intellectual Freedom Committee
Report to Council
2016 ALA Annual Conference
Orlando, FL
Tuesday, June 28, 2016

The ALA Intellectual Freedom Committee (IFC) is pleased to present this update of its activities.

INFORMATION

Journal of Intellectual Freedom and Privacy

The new *Journal of Intellectual Freedom and Privacy*, the successor to the *Newsletter on Intellectual Freedom*, is now a reality. On June 6, Volume 1, Number 1 became available on the JIFP website at journals.ala.org/JIFP.

The inaugural issue includes articles, essays, and book reviews, as well as the usual reliable news on censorship incidents, court cases, and news reports about free expression, academic freedom, and privacy affecting libraries, educational institutions, and society.

The first issue of the *Journal of Intellectual Freedom and Privacy* will be freely available for all to sample online, and OIF has printed a limited number of the first issue for those interested in reviewing its contents. The editorial board's goal is to craft a quarterly journal dedicated to research, discourse and practice concerning intellectual freedom, academic freedom, and privacy that provides a free-wheeling venue for our profession's ongoing conversations about these topics.

The *Journal of Intellectual Freedom* needs your support to succeed. Please consider contributing an essay or an article, and please consider purchasing a personal subscription and encouraging your institution to subscribe. The costs are reasonable — $50.00 a year for online access to four issues that includes access to the archives for the only journal dedicated to both professional discourse and current news about intellectual freedom. Please contact Deborah Caldwell-Stone of the ALA Office for Intellectual Freedom (dstone@ala.org) with your inquiries and interest.

Challenges to Library Materials Update

Since ALA Midwinter Meeting in 2016, OIF has worked on many challenges to library materials. The following are a sample of some of the public cases:

The Perks of Being a Wallflower by Stephen Chbosky	Pasco County Schools, Florida
Reason: Homosexuality, Drug Use, Sexually Explicit	Complainant: Parent
Action: Collaboration with Florida Library Association's Intellectual Freedom Committee. Jamie LaRue wrote a letter to the superintendent commending his use of policy and offering any assistance with policy review.	Resolution: Removed from middle school but retained in the high school library collections. www.tampabay.com/blogs/gradebook/pasco-superintendent-will-not-ban-challenged-novel-in-all-schools/2278898

This One Summer by Jillian and Mariko	Henning School District, Minnesota
Reason: Pervasively Vulgar, Obscene	Complainant: Parent (with the agreement of the librarian, principal, and superintendent)
Action: We received a report of the original challenge and talked with the librarian and superintendent. The school district has no policy and doesn't feel the need for one. With permission, OIF posted a blog about the need for policies to prevent censorship based on personal objections. http://www.oif.ala.org/oif/?p=6559	Resolution: Originally removed. School Board voted 4-2 to retain *This One Summer* in the library but the book must be shelved in a separate section and only available to students in grades 10-12 with parental permission. http://www.slj.com/2016/06/censorship/this-one-summer-restored-to-henning-mn-school-district-library-with-restrictions/#_

Looking for Alaska by John Green	Marion County High School; Lebanon, Kentucky
Reason: Use of Profanity, Pornography	Complainant: Parent, supported by many community members
Action: John Green posted about the removal of this book on Twitter. OIF collaborated with NCTE and NCAC. We talked with the English teacher and the public librarians who attended the school board meeting supporting the teacher who had to publicly defend the book. http://www.oif.ala.org/oif/?p=6575 OIF provided a letter from James LaRue to the reconsideration committee, defending the work and the professional judgement of teachers.	Resolution: Reconsideration Committee voted unanimously to retain the book in the classroom. http://www.slj.com/2016/05/censorship/looking-for-alaska-stays-in-curriculum-in-lebanon-kentucky/ Parents appealed the decision to the superintendent. She retained the book but the book can no longer be taught as a whole class assignment. It has to be taught with other books and in small group instruction.

This One Summer by Jillian and Mariko Tamaki	Seminole County Schools, Florida
Reason: Graphic images	Complainant: Parent of a 3rd grader.
Action: After the original complaint, three high schools removed the book. School required students to submit parental permission slips in order to read the restricted book. OIF wrote a letter expressing concern about "soft censorship".	Resolution: Reinstated http://cbldf.org/2016/03/victory-in-florida-this-one- summer-unrestricted-in-seminole-county-high-schools/

Stranger by the Lake (DVD)	Colorado
Reason: Graphic images	Complainant: Patron
Action: Jamie LaRue wrote a letter and offered support to the library director after it was decided to remove the DVD.	Resolution: Reinstated
Bluest Eye by Toni Morrison	Northville Public Schools, Michigan
Reason: "Possibility of deviant behavior occurring after reading Morrison's text" and "District's "ghettoization" of African Americans."	Complainant: Organized Parents – Northville MI Parents for Educational Excellence
Action: OIF wrote a letter to the school board.	Resolution: Retained http://www.detroitnews.com/story/news/local/wayne- county/2016/04/12/northville-schools-challenge- morrisons-bluest-eye/82959610/

Art Exhibit in a Public Library	New Jersey
Reason: Religious Images	Complainant: Library Board Member
Action: OIF provided resources and counselled on obtaining support from the art and religious community.	Resolution: Removed by Library Board

Online Learning

The Office for Intellectual Freedom presented the following online learning opportunities since the 2016 Midwinter Meeting:

Title	Date	Speakers	Subject
Intellectual Freedom for All: Safeguard Against Censorship of GLBT Books	6/15/2016	Peter Coyl, Gayle Pitman, Susan Kornemann	Observance of GLBT Book Month and defending challenges to GLBT books initiated by librarians themselves.
Intellectual Freedom and Minors	5/26/2016	Theresa Chmara, Chris Crutcher	An overview of minors' First Amendment rights and suggestions on protecting and respecting those rights of parents, teachers, and library staff who are concerned about age-appropriate materials.
Dear Representative	4/22/2016	Lisa Lindle, Deborah Caldwell-tone	Discussion about working with federal and state legislators to advocate for libraries and intellectual freedom issues
Raising Privacy Awareness in Your Library and In Your Community	3/24/2016	Erin Berman, Michael Zimmer, Jamie LaRue	Programming and planning suggestions for libraries observing Choose Privacy Week
Finding Intellectual Freedom Friends	3/7/2016	Charles Brownstein, Emily Brock	Discussion about how to find and recruit allies to support libraries, librarians, and educators addressing book challenges and other IF controversies

Privacy Subcommittee

The IFC Privacy Subcommittee submitted five new privacy guidelines for approval by the Intellectual Freedom Committee. These include:

- Privacy Guidelines for Students in K-12 Schools
- Privacy Guidelines for Library Management Systems;
- Privacy Guidelines for Library Websites, OPACs, and Discovery Services;

- Privacy Guidelines for Public Access Computers and Networks; and
- Privacy Guidelines for Data Exchange Between Networked Devices and Services.

The new guidelines are intended to provide guidance to library and information technology professionals on best practices and policies for protecting user privacy in libraries. The Intellectual Freedom Committee approved all five guidelines. They are attached as information items 19.4 – 19.8.

At this meeting, the Privacy Subcommittee agreed to work on two additional privacy guidelines that will address the privacy issues raised by libraries' use of mobile applications and the privacy needs of library patrons who employ assistive devices and technology to access library resources. The subcommittee also decided to prepare additional materials and programs to assist libraries putting the guidelines into practice, including how-to's, checklists, scorecards, model RPF/contract language, and sample policies. The subcommittee also plans to work with the LITA Patron Privacy Interest Group to offer webinars and to investigate the possibility of sponsoring a privacy pre-conference at next year's Annual Conference.

The subcommittee also intends to investigate the possibility of partnering with the National Information Standards Organization (NISO) to host a privacy summit for librarians and vendors that will focus on how both groups can advance the implementation of the IFC Privacy Guidelines and the NISO Consensus Principles on Users' Digital Privacy in Library, Publisher, and Software-Provider Systems.

Lastly, the subcommittee set the theme for the 2017 observance of Choose Privacy Week. Next year's Choose Privacy Week will focus on "Pretty Good Privacy Practice" in libraries.

PROJECTS

Banned Books Week

SAGE, the Office for Intellectual Freedom, and the Gay, Lesbian, Bisexual, and Transgender Round Table invited ALA Annual Conference attendees to join them at the **Banned Books Readout Booth** to read a passage from a banned or challenged work of GLBT literature to stand in solidarity with Orlando's GLBT community and to show our support for the Orlando shooting victims and their families. All were welcome to speak from the heart about why the book matters. Readings were professionally video recorded and will be featured on the Banned Books Week YouTube channel during Banned Books Week, September 25-October 1, 2016. Check www.youtube.com/bannedbooksweek during the week to view the videos.

Choose Privacy Week

Choose Privacy Week, the American Library Association's annual event that promotes the importance of individual privacy rights and celebrates libraries and librarians' special role in protecting privacy in the library and in society as a whole, was held May 1 – 7, 2016.

This year's Choose Privacy Week events kicked off with a March 24 webinar for librarians and library workers that offered guidance and ideas for developing Choose Privacy Week programming for their libraries. The webinar featured Erin Berman of the San Jose Public Library discussing the SJPL's Virtual Privacy Lab and how it can help libraries and patrons build personalized toolkits for optimizing online privacy; Michael Zimmer of the University of Wisconsin – Milwaukee discussing how to use films and documentaries to increase patron awareness about privacy and surveillance; and OIF director Jamie LaRue discussed his perspective on privacy and libraries and provided a scan of the most pressing privacy issues confronting libraries today.

During Choose Privacy Week, the IFC Privacy Subcommittee hosted a week-long online forum at chooseprivacyweek.org that featured commentaries by educators, librarians and law and privacy experts on respecting and defending students' and minors' privacy. Bloggers included Michael Robinson, Magee Kloepfler, Carolyn Caywood, Dorothea Salo, Michael Zimmer, Galen Charlton, Neil Richards, Debbie and Rigele Abilock, Anna Lauren Hoffmann, Annalisa Keuler, Connie Williams, and Kyle Jones. The website also introduced two new resources during Choose Privacy Week: a page dedicated to student privacy issues and a page dedicated to privacy programming resources for libraries.

<u>New Voices Initiative</u>

OIF has established the New Voices Initiative, coordinated by Shumeca Pickett. It responds to several factors:

- For the past two years, the majority of our top ten most-challenged titles have been written by diverse authors, or featured diverse content.
- The Lee and Low report (http://blog.leeandlow.com/2016/01/26/where-is-the-diversity-in-publishing-the-2015-diversity-baseline-survey-results/) showed that mainstream publishing continues to be dominated by non-diverse decision-makers and content.
- The ethnic composition of the US population changing. According to the US Census, in 2014 there were more than 20 million children under five years old living in the US, and 50.2 percent of them were "minorities" - something other than non-Hispanic white.
- A surge of new content, primarily coming from independent authors and presses, often *does* feature diverse voices and characters. This new content now outnumbers mainstream publications, particularly those of the Big Five.
- Nonetheless, most of this new content does not find its way to library collections.

Using Chicago as a laboratory, OIF will form a New Voices Advisory Council, comprising representatives of both the traditional and emerging publishing ecosystems. The intent of this group is to better connect and inform librarians and local representatives of small, independent, and self-publishers. It is OIF's hope that it will, over the next year or two, develop a template for

the identification, examination, and selection of New Voices in our communities that are not only more diverse than current mainstream offerings but also demonstrate significant quality and value. OIF also hopes to define some new models and paths to distribute this content more easily to libraries.

Advocacy/Intellectual Freedom Boot camps

OIF Director Jamie LaRue and Marci Merola of the Office for Library Advocacy are planning a series of jointly delivered Advocacy and Intellectual Freedom boot camps to recruit and train up a new cadre of leadership in order to respond to the growing generational turnover in the profession. OIF has already begun to advertise these workshops for chapter conferences as a full day pre-conferences, a half day pre-conference, or two shorter sessions during the regular sessions. The first workshop will be in Minnesota this September.

A New Challenges Database

The Office for Intellectual Freedom is refreshing its tools to track and manage the workflow around challenges. The previous database was a single-user and single-purpose database. OIF has purchased, installed, and will shortly begin training and implementation of a shared office product, CaseMap, from LexisNexis that allows OIF to quickly generate and distribute database reports, connect to a core library of policies, procedures, letters, and archive emails, news web pages, and correspondence.

ACTION ITEM

The Intellectual Freedom Committee moves the adoption of the following action item:

CD # 19.9, Religion in American Libraries: An Interpretation of the Library Bill of Rights

Report: Council Resolution Pertaining to Gun Violence Research

Council referred the Resolution on Gun Violence Affecting Libraries, Library Workers, and Library Patrons (2016 ALA MM#45) to the Committee on Legislation and Intellectual Freedom Committee charging them to work in cooperation with the Task Force on Equity, Diversity, and Inclusion ("EDI Task Force") to develop, if possible, a consensus as to the language of a Resolution addressing the matters identified in the Resolution. COL discussed the Resolution and broader issues it raised extensively, ultimately voting to endorse an amended version of the Resolution revised by an informal working group of members discussed in depth in Council Forum. The Committee's actions were presented to an informal joint meeting of representatives of COL, IFC and the EDI Task Force conducted on Monday evening. That group unanimously determined that this Resolution, and the profound and important issues it raises, would benefit from further discussion and revision after the Annual Conference concludes to be reported upon at the 2017 Midwinter meeting in Atlanta.

In closing, the Intellectual Freedom Committee thanks the division and chapter intellectual freedom committees, the Intellectual Freedom Round Table, the unit liaisons, and the OIF staff for their commitment, assistance, and hard work.

Respectfully Submitted,
ALA Intellectual Freedom Committee
Pam Klipsch (Chair)
Doug Archer
Danita Barber-Owusu
Teresa Doherty
Tiffany Arielle Duck
Clem Guthro
Charles Kratz
Jean McFarren
Dale McNeill
Michael Wright
Hannah Buckland (intern)
Johanna Orellana (intern)

Library Privacy Guidelines for Students in K-12 Schools
Introduction

Libraries face a number of challenges in protecting the privacy of users, especially students in elementary, middle, and high schools. School libraries offer print, media, and online content to meet students' educational and research needs as well as to nurture their intellectual curiosity and development. Students' use of library resources is also incorporated into classroom activities, learning outcomes, and assessment.

School libraries typically are integrated into their district's administrative and technology infrastructures. Depending on district administration and outside cooperative technology or vendor agreements, school libraries have greater or lesser degrees of autonomy. A lack of autonomy may make it difficult for librarians to implement policies and procedures to protect student privacy in regard to the use of library systems, applications, and collections. In addition, state and federal laws regarding library records, educational records (e.g., the Family Educational Rights and Privacy Act (FERPA), and the online activities of minors (e.g., the Child Online Privacy Protection Act (COPPA) have both positive and negative impacts on the privacy rights of students. For example, FERPA defines explicit rights to privacy for students and minors but at the same time grants schools and parents access to, and oversight over, student records that weakens these privacy rights.

ALA issues these guidelines to provide school libraries with information about appropriate data management and security practices in respect to student use of library collections and resources in order to strengthen student privacy protections.

Why Privacy Is Important

Protecting user privacy and confidentiality has long been an integral part of the intellectual freedom mission of libraries. The right to free inquiry as assured by the First Amendment depends upon the ability to read and access information free from scrutiny by the government or other third parties. In their provision of services to library users, librarians have an ethical obligation, expressed in the ALA Code of Ethics, to preserve users' right to privacy. Librarians and libraries may also have a statutory or regulatory obligation to protect library users' personally identifiable information and data from unauthorized disclosure and use.

Students' and minors' First Amendment rights to free inquiry and privacy must be balanced against both the educational needs of the school and the rights of the parents. As students and minors mature, it is increasingly important that they are provided with opportunities to exercise their curiosity and develop their intellect free from the chilling effects of surveillance by educators, peers, parents, or commercial interests. As students begin to participate more fully in the online world, they must develop an appreciation for their own privacy and a corresponding respect for the privacy of others.

Clear Privacy Policies
It is important for libraries to develop privacy policies for student use of library resources that are adopted by both the library and the school's policy-making body. Students should be notified about library privacy policies when borrowing materials or accessing resources for the first time and as appropriate when there is a change in services, policies, or access. Library privacy policies should be made easily available and understandable to students in an age-appropriate manner. Safeguarding user privacy requires that staff keep all in-library use and reference questions confidential and assure that there is no monitoring by staff or peers of what students are reading, viewing, or researching while in the library.

Audit
School librarians should conduct privacy audits to determine the current threats to student privacy and what protections are already in place. The audit should cover the library management system; computer and network use in the library; eBooks and other online content; interactive Web tools; social media; and other technologies such as scanners/photocopiers and surveillance cameras. The results of the audit can be used to help create or revise privacy policies.

Collection and Retention of User Data
Libraries should limit the amount of personal information collected about students. Libraries should collect the minimum amount of personal information required to provide a service or meet a specific operational need. Libraries should not build services or resources using sensitive personally identifiable information that, if leaked or accessed by an unauthorized party, could prove detrimental to the user's privacy.
Personally identifiable information should not be retained in perpetuity. The library should establish record retention policies specifying how long to retain different types of data and specifying methods for securely destroying data that is no longer needed. Retention policies should also cover archival copies and backups.

Encryption
The use of data encryption helps enhance privacy protection. All online transactions between client applications (staff desktop clients, web browsers, mobile apps, etc.) and server applications should be encrypted. Client applications that do not support encryption (such as staff desktop clients) should employ virtual private network (VPN) technologies. In addition, any personally identifiable information and student data housed by the library or school off-site (cloud-based infrastructure, tape backups, etc.) should use encrypted storage.

Data Sharing
Library privacy policies should define when school library records can be shared (and under what conditions) with parents or guardians, school staff and teachers, and third-parties such as online service providers.
Federal laws such as FERPA and COPPA as well as state laws concerning the confidentiality of library and student records may impact if and how data is shared. Because of the broad leeway FERPA gives schools in using student data for internal educational purposes, librarians need to clearly distinguish among library records, educational records, and administrative records in order to provide explicit privacy rights in accordance with professional ethical obligations.
Agreements between school libraries and online service providers should address appropriate restrictions on the use, aggregation, retention, and dissemination of students' personally identifiable information. Agreements between libraries and service providers should also specify that libraries retain ownership of all data and that the service providers agree to observe the library's privacy policies, data retention policy, and security policies. In the event of a data breach, users whose data was compromised should be informed promptly (in the case of minors, the parents or guardians should be informed).

Many service providers have signed the Student Privacy Pledge which indicates a commitment to work in an ongoing fashion to meet and exceed all federal requirements to protect student data. Librarians should make participation in the Student Privacy Pledge a criterion when making purchasing decisions.

In addition, many states are passing legislation that restricts the collection and use of students' data by service providers (e.g. California's Student Online Personal Information Protection Act – SOPIPA). Librarians should only contract with service providers that comply with applicable state laws.

Educational Technology Systems
Primary and secondary schools are adopting learning management systems and other technologies that enable educators to monitor student reading habits (e.g. did the student access/read the assigned eBook or online text?) As a result, school districts are co-opting librarians into surveillance regimes by adopting these types of technologies. Librarians need to advocate for protecting student library use in an age of ubiquitous data logging and surveillance technologies, including learning management systems.

Digital Literacy & Advocacy
School librarians have a responsibility to teach students about their privacy rights, practices they can use to protect themselves, ethical behavior online, and respect for the privacy of others. In addition to educating students, school librarians should become advocates for protecting student privacy and intellectual freedom in the larger school environment. Often school librarians are focused only on user privacy within the library to the detriment of larger privacy issues in their school and district context. Because of their professional training and ethical commitment, librarians are well-equipped to be privacy advocates outside of the school library.

Additional Resources
Privacy Technical Assistance Center
U.S. Department of Education
Privacy Toolkit
Intellectual Freedom Committee of the American Library Association
Spying on Students: School-Issued Devices and Student Privacy
Electronic Frontier Foundation
Student Data Principles
Data Quality Campaign and the Consortium for School Networking
Student Privacy Bill of Rights
Electronic Privacy Information Center
Student Privacy Pledge
Future of Privacy Forum (FPF) and The Software & Information Industry Association (SIIA)
Students' and Minors' Privacy Resources
Choose Privacy Week, American Library Association

Privacy Guidelines for Library Management Systems

Introduction

Library management systems (LMS), also known as integrated library systems, are used by libraries to inventory collections and manage user records. The LMS stores personal information collected from patrons for a variety of reasons and maintains records of what items patrons borrow, the holds they place, and fines or fees they may incur. In addition, the LMS may share data with or provides services to other systems employed by the library, for example to provide authentication for online resources.

Libraries must work to ensure that their procedures and practices for managing the LMS reflect library ethics, policies, and legal obligations concerning user privacy and confidentiality. Agreements between libraries and vendors should specify that libraries retain ownership of all data; that the vendor agrees to observe the library's privacy, data retention, and security policies; and that the vendor agrees to bind any third parties it uses in delivering services to these policies as well.

These guidelines are issued by ALA to provide libraries using LMS with information about appropriate data management and security practices in respect to library patrons' personally identifiable information and data about their reading habits and use of library resources.

Why Privacy Is Important

Protecting user privacy and confidentiality has long been an integral part of the intellectual freedom mission of libraries. The right to free inquiry as assured by the First Amendment depends upon the ability to read and access information free from scrutiny by the government or other third parties. In their provision of services to library users, librarians have an ethical obligation, expressed in the ALA Code of Ethics, to preserve users' right to privacy. Librarians and libraries may also have a legal obligation to protect library users' personally identifiable information and data from unauthorized disclosure and use.

Clear Privacy Policies

Users should be notified about library privacy policies when registering for a library card or borrowing materials for the first time. Library privacy policies should be made easily available and understandable to users in an accessible format. Safeguarding user privacy requires that individuals know what personally identifiable information is gathered about them, how long it is stored, who has access to it and under what conditions, and how it is used. A proactive process should be created to notify ongoing users of any changes to the library's privacy policies.

User Consent

The library should give users of the LMS options as to how much personally identifiable information is collected from them and how it may be used. Users should have a choice about whether or not to opt-in to features and services that require the collection of personal information. Users should also have the ability to opt-out if they later change their minds and have the data collected during the opt-in phase be destroyed when possible. For example, if the LMS offers the ability to save the checkout history, this should be an opt-in feature not turned on as a default.

Access to Personal Data

Users should have the right to access their own personal information and evaluate its accuracy. Verifying accuracy helps ensure that library services that rely on personally identifiable information can function properly. Guidance on how the user can access their personal data held in the LMS should be clear and easy to find.

Access to personal information should be restricted to the user or appropriate library staff and conform to the applicable state laws addressing the confidentiality of library records as well as other applicable local, state, and federal law. In addition, state and federal laws may give parents, guardians, and educators access to the library records of minors (see *Library Privacy Guidelines for Students in K-12 Schools* in the Additional Resources section below).

Collection & Retention of User Data

Libraries should limit the amount of personal information collected by the LMS about patrons. In general, the library should collect the minimum amount of personal information required to provide a service or meet a specific operational need. Library policies developed around the collection of personal information should also cover the use of any free-text note fields associated with the patron's record.

Personally identifiable information should not be retained in perpetuity. The library should establish policies for how long to retain different types of data and methods for securely destroying data that is no longer needed. For example, accounts that are expired or inactive for a certain amount of time should be purged. Retention policies should also cover archival copies and backups.

Encryption

All online transactions between client applications (staff desktop clients, web browsers, mobile apps, etc.) and server applications should be encrypted using modern, up-to-date security protocols for SSL/HTTPS. Client applications that do not support encryption (such as staff desktop clients) should employ virtual private network (VPN) technologies.

In addition, any personally identifiable information and user data housed by the library off-site (cloud-based infrastructure, tape backups, etc.) should use encrypted storage.

PINs & Passwords

User personal identification numbers (PINs) and passwords stored in the LMS should be encrypted so that only the user has access to them, i.e. library staff cannot view them. This encryption should use up-to-date best practices. Currently, this means that passwords should be salted and hashed with a SHA-2 hash function, but library personnel responsible for password security should stay current on best practices. In addition, the LMS should provide users with the ability to set their PIN or password themselves without having to reveal it to library staff.

Notifications & Reports

User notifications for holds, overdue items, and fines should contain minimal personal information especially if sent through insecure communication (e.g. email, text message, postcards). Users could be encouraged to login to a secure account for more details. If the LMS provides the ability to include notification history as part of the patron record, this should be offered as an opt-in feature for patrons and not turned on by default.

Access to LMS reports that contain personally identifiable information should be restricted to appropriate library staff. Reports intended for wider distribution should be anonymized by removing or encrypting personally identifiable information.

Libraries that combine patron information from the LMS with external demographic information for analytics should take measures to protect reader privacy. Aggregation and anonymization should be employed to help prevent the identification of reading habits and library usage with specific individuals. Because of the growing threat of reidentification techniques, access to anonymized data sets should still be restricted to appropriate users.

Data Sharing

It has become common practice for organizations to share data including personally identifiable information with third-parties. However, most state statutes on the confidentiality of library records do not permit release of library patrons' personally identifiable information or data about their use of library resources and services without user consent or a court order, although some state library confidentiality statutes permit sharing this data with parents or guardians of minors. In addition, ALA policy forbids sharing of library patron information with third parties without user consent or a court order.

Government Requests

The library should develop and implement procedures for dealing with government and law enforcement requests for library patrons' personally identifiable information and use data held

within the LMS. The library should consider a government or law enforcement request only if it is issued by a court of competent jurisdiction that shows good cause and is in proper form. The library should also inform users through its privacy policies about the legal conditions under which it might be required to release personally identifiable information.

The library could consider publishing a warrant canary notice to inform users that they have not been served with a secret government subpoena or national security letter. If a canary notice is not updated or it is removed, users can assume that a subpoena or national security letter has been served (see *Canary Warrants Frequently Asked Questions* in the Additional Resources section below).

Privacy Awareness

Library staff who have access to patron data in the LMS should receive training on the library's privacy policies and best practices for safeguarding patron privacy.

Libraries should establish and maintain effective mechanisms to enforce their privacy policies. They should conduct regular privacy audits to ensure that all operations and services comply with these policies. A library that suffers a violation in its privacy policies through inadvertent dissemination or data theft must notify the affected users about this urgent matter as soon as the library is aware of the data breach and describe what steps are being taken to remedy the situation or mitigate the possible damage.

Additional Resources

Canary Warrants Frequently Asked Questions, Electronic Frontier Foundation, https://www.eff.org/deeplinks/2014/04/warrant-canary-faq

Library Privacy Guidelines for Students in K-12 Schools, Intellectual Freedom Committee of the American Library Association, http://www.ala.org/advocacy/library-privacy-guidelines-students-k-12-schools

NISO Consensus Principles on User's Digital Privacy in Library, Publisher, and Software-Provider Systems, National Information Standards Organization, http://www.niso.org/apps/group_public/download.php/15863/NISO%20Consensus%20Principles%20on%20Users%92%20Digital%20Privacy.pdf

Privacy Toolkit, Intellectual Freedom Committee of the American Library Association, http://www.ala.org/advocacy/privacyconfidentiality/toolkitsprivacy/privacy

Privacy Guidelines for Library Websites, OPACs, and Discovery Services

Introduction

Libraries publish information and provide services through websites, online public access catalogs (OPACs), and discovery services. The OPAC, often known simply as the library catalog, allows patrons to search the library's collections using a web-based user interface. A discovery service provides a single web-based user interface to search across multiple resources such as library catalogs, periodical databases, institutional repositories, and digital collections.

Library websites, OPACs, and discovery services may collect personal information about patrons for a variety of reasons including authentication, personalization, and user analytics. In addition, personal information is sometimes shared with third parties that provide content or other functionality for the website or service.

The hardware, applications, and data that comprise a website or service may be managed directly by the library; by a parent organization such as a local government, school, or consortium; by a vendor or service provider; or by some hybrid of shared responsibilities among multiple parties. Regardless of the management model, libraries must work to ensure that the websites, OPACs, and discovery services they offer reflect library ethics, policies, and legal obligations concerning user privacy and confidentiality.

These guidelines are issued to provide libraries with information about appropriate data management and security practices in respect to library patrons' personally identifiable information and data about their reading habits and use of library resources.

Why Privacy Is Important

Protecting user privacy and confidentiality has long been an integral part of the intellectual freedom mission of libraries. The right to free inquiry as assured by the First Amendment depends upon the ability to read and access information free from scrutiny by the government or other third parties. In their provision of services to library users, librarians have an ethical responsibility, expressed in the ALA Code of Ethics, to preserve users' right to privacy. Librarians and libraries may also have a legal obligation to protect library users' personally identifiable information and data from unauthorized disclosure and use.

Clear Privacy Policies

Users should be notified about library privacy policies when using a library website, OPAC, or discovery service. Library privacy policies should be made easily available and understandable to users in an accessible format. Safeguarding user privacy requires that

individuals know what personally identifiable information is gathered about them, how long it is stored, who has access to it and under what conditions, and how it is used. A proactive process should be created to notify ongoing users of any changes to the library's privacy policies.

Personalization & User Consent

The library should give users options as to how much information is collected from them and how it may be used. Users should have a choice about whether or not to opt-in to features and services that require the collection of personal information. Users should also have the ability to opt-out if they later change their minds and have the data collected during the opt-in phase be destroyed when possible. For example if the discovery service offers the ability to save their search history, this should be an opt-in feature not turned on as a default.

Access to Personal Data

Users should have the right to access their own personal information and evaluate its accuracy. Verifying accuracy helps ensure that library services that rely on personally identifiable information can function properly. Guidance on how the user can access their personal data should be clear and easy to find.

Access to personal information should be restricted to the user or appropriate library staff and conform to the applicable state laws addressing the confidentiality of library records as well as other applicable local, state, and federal law.

Encryption

All online transactions between client applications (web browsers, ebook readers, mobile apps, etc.) and server applications should be encrypted using modern, up-to-date security protocols for SSL/HTTPS. Communications between server applications and third-party service providers should be encrypted. User passwords should be stored using up-to-date best practices for encryption. In addition, any personally identifiable information and user data housed off site (cloud-based infrastructure, tape backups, etc.) should use encrypted storage.

Data Sharing

It has become common practice for organizations to share data including personally identifiable information with third-parties, often unintentionally. Scripts and embedded content from a third-party that are placed on websites (sharing buttons, photo streams, videos, etc.) may allow that third party to track user behavior and share that data with other parties. However, most state statutes on the confidentiality of library records do not permit release of library patrons' personally identifiable information or data about their use of library resources and services without user consent or a court order. In addition, ALA policy forbids sharing of library patron information with third parties without user consent or a court order.

Libraries should carefully evaluate the impact on user privacy of all third-party scripts and

embedded content that is included in their website, OPAC, or discovery service.

User Generated Content

Library websites, OPACs, and discovery services often allow patrons to create publicly shared content such as comments, ratings, recommendations, etc. The library will need to weigh the costs and benefits of requiring authentication (privacy implications if real identity is used) versus anonymous access (more difficult to prevent spam and other unacceptable use) in order to create shared content. In addition, tools that allow the creation of content may rely on third parties which may collect user data and share it with other parties.

Activity Data & Web Analytics

Libraries should limit the amount of personal information collected about users. Websites, OPACs, and discovery services collect and record data about user activity. Even for anonymous users (I.e. those that do not login to access personalization features) the activity data may include personally identifiable information. In general, the library should collect the minimum personal information required to provide a service or meet a specific operational need.

Access to reports that contain personally identifiable information should be restricted to appropriate library staff. Reports and web analytics intended for wider distribution should be anonymized by removing or encrypting personally identifiable information.

Careful consideration should be given before using a third party to collect web analytics (e.g. Google Analytics) since the terms of service often allow the third party to harvest user activity data for their own purposes.

User activity data with personally identifiable information should not be retained in perpetuity. The library should establish policies for how long to retain different types of data and methods for securely destroying data that is no longer needed. Retention policies should also cover archival copies and backups.

Privacy Awareness

Library staff who manage the library's websites and services should receive training on the library's privacy policies and best practices for safeguarding patron privacy. Library staff that negotiate contracts with vendors that provide websites and services should also receive privacy training.

Libraries should establish and maintain effective mechanisms to enforce their privacy policies. They should conduct regular privacy audits to ensure that all operations and services comply with these policies. A library that suffers a violation in its privacy policies through inadvertent dissemination or data theft must notify the affected users about this urgent matter

as soon as the library is aware of the data breach and describe what steps are being taken to remedy the situation or mitigate the possible damage.

Additional Resources

Let's Encrypt, Internet Security Research Group, https://letsencrypt.org/

NISO Consensus Principles on User's Digital Privacy in Library, Publisher, and Software-Provider Systems, National Information Standards Organization, http://www.niso.org/apps/group_public/download.php/15863/NISO%20Consensus%20Principles%20on%20Users%92%20Digital%20Privacy.pdf

Privacy: An Interpretation of the Library Bill of Rights, American Library Association, http://www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy

Privacy Toolkit, Intellectual Freedom Committee of the American Library Association, http://www.ala.org/advocacy/privacyconfidentiality/toolkitsprivacy/privacy

Library Privacy Guidelines for Public Access Computers and Networks

Introduction

Libraries provide patrons with opportunities to use computers and other devices (e.g. laptops, tablets, ebook readers, etc.) to access online resources such as library catalogs, research databases, ebooks, other digital content, and the Internet. Patrons use library computers to create content including word processing documents, multimedia projects, email messages, and posts to social media and other websites. In addition, libraries often provide wired and wireless public networks that allow patrons to connect using a personal device.

Use of any computer or network may create records of users' activities that can jeopardize their privacy. In addition libraries may collect personal information from users for a variety of reasons such as reserving a computer or checking out a device. Libraries must work to ensure that their procedures and practices for managing public access computers and devices reflect library ethics, policies, and legal obligations involving user privacy and confidentiality.

These guidelines are issued to provide libraries with information about appropriate data management and security practices with respect to library patrons' personally identifiable information and data about their use of public access computers and networks.

Why Privacy Is Important

Protecting user privacy and confidentiality has long been an integral part of the intellectual freedom mission of libraries. The right to free inquiry as assured by the First Amendment depends upon the ability to read and access information free from scrutiny by the government or other third parties. In their provision of services to library users, librarians have an ethical responsibility, expressed in the ALA Code of Ethics, to preserve users' right to privacy. Librarians and libraries may also have a legal obligation to protect library users' personally identifiable information and data from unauthorized disclosure and use.

Clear Privacy Policies

Users should be notified about library privacy policies when accessing a computer or a public network in the library. The privacy policies should be made easily available and understandable to users. Safeguarding user privacy requires that individuals know what personally identifiable information is gathered about them, how long it is stored, who has access to it and under what conditions, and how it is used. A proactive process should be created to notify ongoing users of any changes to the library's privacy policies.

Access Control & Device Checkout
Libraries can use a variety of methods to manage access to computers and networks. These methods range from a clipboard with a sign-up sheet to sophisticated access control software that can include user authentication, reservations, time limits, and management of Internet content filters. The integrated library system may be used to checkout laptops and other devices. In addition, libraries may require users to authenticate in order to access the network when using their personal device.

Whatever methods are employed, libraries should develop appropriate policies and procedures to protect the privacy of patrons and their computer and network activity in the library. Transactional logs generated by access control software and network authentication should be anonymized or destroyed when no longer needed. Sign-up sheets should be redacted or shredded. Checkout records should be purged or anonymized when the device is returned and any overdue fines paid.

Display Screens
Computer display screens are often easily visible to nearby people. Libraries should make privacy screens or recessed displays available to patrons who desire to use them while recognizing no screen will render a user's display completely invisible to other people. In addition, many people dislike privacy screens or recessed displays and therefore should not be forced to use them.

Browser Activity
Many websites track user behavior and share data with third parties via cookies and other technologies. The library should provide browsers and plugins that offer privacy protections when surfing the Web. In addition, browsers should be configured to clear all data (cache, history, cookies, passwords) upon exit.

Routine Maintenance
Public computers should be routinely maintained to ensure they are operating properly, and that the software on the computer designed to protect the user's privacy is activated and effective. A security audit of the computer could be routinely performed to attempt to locate deficiencies in the security of the computer. A physical inspection should also include the identification of unknown devices attached to the computer designed to steal personal information such as keyloggers.

Personal Data on Computer or Device
Use of any computer or device may create records of the user's activities that can jeopardize their privacy. Documents, emails, and other files that may contain private information could be left

on the device. The library should use restoration software or other technological means to remove traces of individual use on public access computers and other devices provided by the library.

Malware

Malware can be a serious threat to personal privacy and security when using a computer. If the malware captures login information and passwords, the user's online accounts maybe compromised. Libraries should take appropriate steps to ensure that malware or other unauthorized software does not reside on the computer or device. These steps could include security protection (anti-malware, anti-spam, anti-virus programs) as well as restoration software to remove all software installed without authorization.

Computer Monitoring & Usage Tracking

Monitoring software can be installed to record activities or remotely view what a user is doing on a device. It is often used for technical support or for compliance with an organization's computer use policy. To protect users' privacy, libraries should avoid using monitoring software on public access computers or other devices provided by the library. If monitoring is employed, users should be informed of its purpose and scope in the library's privacy policies.

Many applications and operating systems are configured by default to automatically share activity data with the software publisher to identify errors, enhance usability, or provide personalization. When possible, the library should disable such usage tracking on public access computers or other devices provided by the library.

Privacy Guidelines for Data Exchange Between Networked Devices and Services

Introduction

Machine-to-machine communications of data allow libraries to offer services such as self-checkout stations and patron account features in library catalogs. A typical scenario might be an application installed on a library management system that allows a client application to access patron data and perform transactions or perform information searches on behalf of a patron. Examples of protocols and APIs supported by many library management systems include SIP2, NCIP, Z39.50, SRU and SRW, and other Web services (see Glossary of Terms at the end of this document). Libraries must work to ensure that their procedures and practices for managing programmatic data communications reflect library ethics, policies, and legal obligations concerning user privacy and confidentiality.

These guidelines are issued to provide libraries with information about appropriate data management and security practices in respect to library patrons' personally identifiable information and data about their reading habits and use of library resources.

Why Privacy Is Important

Protecting user privacy and confidentiality has long been an integral part of the intellectual freedom mission of libraries. The right to free inquiry as assured by the First Amendment depends upon the ability to read and access information free from scrutiny by the government or other third parties. In their provision of services to library users, librarians have an ethical obligation, expressed in the ALA Code of Ethics, to preserve users' right to privacy. Librarians and libraries may also have a legal obligation to protect library users' personally identifiable information and data from unauthorized disclosure and use.

Encryption

The use of data encryption helps enhance privacy protection. Data communications between client applications and server applications that may include patron information should be encrypted. Client-server applications that do not support encryption (such as SIP2) should be deployed over transports that perform encryption, such as virtual private networks (VPNs) or TLS or SSH tunnels. If a particular service or protocol is available over either encrypted or unencrypted connections (e.g., as can be the case with NCIP), the library should mandate the use of the encrypted configuration option.

Access Control

Server applications that allow programmatic data communications should limit access to authorized client applications. The library should monitor server applications to insure no

unauthorized client applications have access to patron information as a standard part of data security measures.

Minimum Disclosure
Server applications that allow programmatic data communications should supply only the minimum of patron information required to fulfill the specific purpose for which that information is being made available to an authorized client application. For example, if a client application needs to verify that a set of credentials correspond to those of a patron who has privileges at the library, that application may not need to be sent any contact or demographic information about that patron. The library should take advantage of available configuration options to enforce the principle of minimum disclosure.

The library should work with service and system providers to perform an audit which identifies what data is currently being transmitted, kept, and under what circumstances in order to ensure minimum disclosure in the future.

Retention of User Data
Server applications that provide programmatic data communications may create log files that contain patron information. The library should establish policies for how long to retain log files and methods for securely destroying data that is no longer needed. Retention policies should also cover archival copies and backups.

Standards Development
Librarians and library technologists who participate in the design of new standards or application profiles for machine-to-machine communication protocols should advocate for standards that follow these guidelines.

Glossary of Terms

API - application programming interface is a set of routine definitions, protocols, and tools for building software and applications.
https://en.wikipedia.org/wiki/Application_programming_interface

Client - a piece of computer hardware or software that accesses a service made available by a server. The server is often (but not always) on another computer system, in which case the client accesses the service by way of a network.
https://en.wikipedia.org/wiki/Client_%28computing%29

NCIP - National Information Standards Organization Circulation Interchange Protocol is a protocol that is limited to the exchange of messages between and among computer-based applications to enable them to perform functions necessary to lend and borrow items, to provide

controlled access to electronic resources, and to facilitate cooperative management of these functions.
https://en.wikipedia.org/wiki/National_Information_Standards_Organization_Circulation_Interchange_Protocol

SIP2 - Standard Interchange Protocol 2 is a proprietary standard for communication between library computer systems and self-service circulation terminals.
https://en.wikipedia.org/wiki/Standard_Interchange_Protocol

SRU - Search/Retrieve via URL is a standard search protocol for Internet search queries, utilizing Contextual Query Language (CQL), a standard query syntax for representing queries.
https://en.wikipedia.org/wiki/Search/Retrieve_via_URL

SRW - Search/Retrieve Web service is a web service for search and retrieval.
https://en.wikipedia.org/wiki/Search/Retrieve_Web_Service

SSH tunnel - an encrypted tunnel created through an SSH protocol connection. Users may set up SSH tunnels to transfer unencrypted traffic over a network through an encrypted channel.
https://en.wikipedia.org/wiki/Tunneling_protocol#Secure_Shell_tunnelin

Religion in American Libraries: An Interpretation of the Library Bill of Rights

The courts have consistently held that for the freedom of the press and speech guaranteed by the First Amendment to the United States Constitution to be fully meaningful, people must also have the right to receive information: that is, to read, view, hear or access what they choose. In addition, the First Amendment guarantees the right of individuals to believe and practice their religion or practice no religion at all (the "free exercise" clause) and prohibits government from establishing or endorsing a religion or religions (the "establishment" clause). Thus the freedom of, for and from religion, are similarly guaranteed.

In most cases involving religion and libraries, these latter freedoms of, for and from religion are not at issue. Rather, the constitutional principles at stake are usually freedom of expression and the corollary freedom to access the expression of others. For instance, most challenges to materials with religious content potentially infringe on the rights of other persons to access constitutionally protected speech rather than limiting the challenger's own beliefs or the practice of his or her own religion.

For the purpose of this interpretation "religion" refers to all that touches on the infinite, a supreme deity or deities or one's understanding of the ultimate meaning or purposes of life. It includes formal organized systems of belief and practice and informal individual spiritualties. It also refers to adherents of older religions, newer religions, and no religion. While this interpretation is most clearly applicable to public libraries, it should in most cases also be appropriate for school and academic libraries. Private libraries, especially those associated with religious institutions, should apply these guidelines as appropriate in relation to their institutional mission.

Librarians have a professional responsibility to be inclusive rather than exclusive in collection development. Libraries serve all members of their communities and within their budgetary constraints should address all information concerns of all members—including their religious information needs. Collections should reflect those needs by providing access to diverse religious thought without becoming a proponent of any of them. Articles I and II of the Library Bill of Rights are clearly inclusive regarding audience ("all people of the community the library serves") and materials ("all points of view on current and historical issues"). This includes both fiction and non-fiction materials regardless of format.

Collection development and materials selection should be done according to standards set forth in library policy that incorporates professional standards established in the Library Bill of Rights and Code of Ethics of the American Library Association and that are tailored to the community that the library serves. These may include but are not limited to contemporary significance or permanent value, community interest and/or demand, artistic and literary excellence, cost and format. The policy may include a reference to the role of the library as a limited public forum providing access to the marketplace of ideas. For example, it may state that the library provides

unfettered access to different points of views and ideas. Above all, collection development should be content-neutral, assuring that the library reflects a diversity of ideas including controversial or unorthodox points of view.

The selection, shelving and labeling (especially the use of religious symbols in labeling) of religious fiction are particularly sensitive. Nevertheless, excluding religious fiction would be a violation of the Library Bill of Rights: “Materials should not be excluded because of origin, background, or views of those contributing to their creation." Librarians should distinguish between providing access to religious fiction and the appearance of supporting or endorsing a particular religious point of view. Religious content is no more or less protected than any other type of speech. While libraries and librarians should respect the diverse religious traditions of their communities, libraries exist to serve the information needs of all users in their communities.

Library policy should be applied equally to shelving of religious books, to storage or display of religious objects, or to access to religious Web sites as they would be to any other shelving, storage, display, or Web access. Privileging one religious tradition over others could violate the establishment clause of the First Amendment. Placing specific materials according to religious point of view or status within a given faith community rather than according to the cataloging system used in the library can make it difficult for users to locate such materials. It could be a violation of the Library Bill of Rights to give special treatment to a specific sacred text or object or to limit access to such a text or object. On the other hand, it is appropriate to add additional titles or versions of a text or objects to the collection to meet community needs or interest but not to remove or sequester them. The scriptures or religious materials of all religions should be treated respectfully and equitably.

If a library sets aside tables or shelves for specialized materials or purposes such as atlases, directories, college guides, dictionaries or local history, it would be appropriate to set aside shelving for scripture, as long as all scriptures are treated equally, including texts that occupy a similar status among other groups (e.g., *The Humanist Manifesto II*).

Regarding meeting rooms, courts have consistently held that libraries may not exclude religious groups from their meeting rooms solely because the group is religious in character or because the meeting may include religious activities. Many precedents exist for the use of public facilities (e.g., school auditoriums or park pavilions) by all types of community groups, including religious groups. Courts that have considered the question have consistently held that libraries are limited public forums for the receipt of information. In turn libraries may designate areas within their facilities as limited public forums for use by the community for the exchange of information and may create rules for their use. No court has ever ruled that a library must exclude religious groups. The safest course of action is to provide the same access and apply the same rules of use to all community groups. As with collections, these rules should be content-neutral and address only behavioral restrictions (time, place and manner). Consistency is crucial: all groups should be treated the same and subject to the same rules, such as rental fees, frequency restrictions, noise policies or food bans.

With regard to displays, libraries are not required to open display or exhibit space to community groups. If libraries choose to open their exhibit and display space to community groups, space

should be provided on an equitable basis to all groups that request it, regardless of the beliefs or affiliations of individuals or groups requesting their use. A library may wish to consider the amount of such space and its location when deciding whether to open it to community groups. Article II of the Library Bill of Rights states, "Materials should not be excluded because of the origin, background, or views of those contributing to their creation" and "Materials should not be proscribed or removed because of partisan or doctrinal disapproval." For additional details, see "Exhibit Spaces and Bulletin Boards: An Interpretation of the Library Bill of Rights."

If a library provides space for community groups to distribute literature to the public, religious groups should be allowed to do so on an equitable basis with all groups that use the distribution space, regardless of the beliefs or affiliations of individuals or groups distributing such literature. Policies covering the number of individual items of literature, the size and definition of such items and the length of time that items will be left out for distribution should be considered.

The religious views that patrons and employees bring with them into the library are more community relations and employment issues rather than intellectual freedom issues and are addressed in the Intellectual Freedom Committee's "Religion in American Libraries: Questions and Answers."
http://www.ala.org/advocacy/intfreedom/librarybill/interpretations/meetingrooms/religion-q-a

Precisely because religion is such a sensitive and sometimes controversial concern of library users, it should be accorded the full protections promised to its myriad forms by the First Amendment of the United States Constitution and the American Library Association's Library Bill of Rights.