ALA Intellectual Freedom Committee
Report to Council
2017 ALA Midwinter
Atlanta, GA
Tuesday, January 24, 2017

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

INFORMATION

Revamped Challenge Reporting Form and Updated Challenge Support Pages

The Office for Intellectual Freedom unveiled its redesigned reporting form and updated Challenge Support pages on the ALA website on Dec. 20. The new, simplified form reduces the number of questions by more than 60 percent and includes an entry to allow for the reporting of hate crime in libraries.

The Challenge Support pages on the ALA website, which include policy guidelines, FAQs and Library Bill of Rights interpretations, have been migrated from the Banned Books Week microsite to its own section in ALA's Professional Tools. OIF's goal in rolling out these new challenge reporting tools is to encourage educators to report censorship (an informal 2011 survey confirmed that only about 20% of challenges were reported to ALA) and offer a navigable resource where librarians can easily find support when responding to challenges and hate crimes.

Online Learning

This fall, OIF offered three engaging and successful webinars. Academics Emily Knox, Joyce Latham and Candace Morgan reviewed the origins and evolution of censorship in "History of Intellectual Freedom and Censorship," a webinar co-sponsored by OIF and the Freedom to Read Foundation. The next month, notable ACLU leader Emilio De Torre spoke on the complexities of student activism in the OIF webinar "Students Rights, Protests and Free Speech." Finally, the office hosted a free webinar in January that introduced the new challenge reporting resources, walking participants through reporting forms, office resources and real-world censorship examples. This webinar received nearly 100 registrations.

Journal of Intellectual Freedom and Privacy

Michael Zimmer, associate professor at the School of Information Studies at the University of Wisconsin–Milwaukee and director of the Center for Information Policy Research, has been appointed editor of the *Journal of Intellectual Freedom and Privacy* (JIFP) through the fall of 2018. Shannon Oltmann, assistant professor at the School of Information Science, College of Communication & Information at the University of Kentucky will serve as associate editor, working with Zimmer on content and editorial guidelines for the journal. Martin Garnar, dean of

the Kraemer Family Library at the University of Colorado in Colorado Springs, has agreed to serve as production editor, managing article submissions.

The new issue of the *Journal of Intellectual Freedom and Privacy* is now available at journals.ala.org/jifp. It features Garnar's article "Professional Principles and Ethics in LIS Graduate Curricula," and includes additional features, book reviews, and opinion pieces in addition to the latest news on censorship challenges, court decisions, legal controversies and success stories.

OIF's 50th Anniversary Focuses on the Library Bill of Rights

The Office for Intellectual Freedom and the Intellectual Freedom Committee are both charged with upholding the Library Bill of Rights, their core document and the foundation for all their work. In honor of OIF's 50th anniversary, the office offered free pocket-sized, downloadable Library Bill of Rights and Freedom to Read Statements on its website. It also gifted packets of 50 to those who filled out an online request form.

In December, the office also unveiled an ALA- and OIF-branded Library Bill of Rights poster, now available at the ALA Store. First drafted in 1938 and adopted by ALA in 1939, the Library Bill of Rights was written to speak out against the "growing intolerance, suppression of free speech and censorship affecting the rights of minorities and individuals." It's the only Library Bill of Rights-themed product on the ALA Store.

Privacy Subcommittee and Choose Privacy Week

This fall, the IFC's Privacy Subcommittee partnered with the LITA Patron Privacy Interest Group to create seven checklists to provide libraries with practical guidance on implementing the Library Privacy Guidelines published by the Intellectual Freedom Committee in 2016. These include:

1. Library Privacy Checklist Overview
2. Library Privacy Checklist for Library Websites, OPACs, and Discovery Services
3. Library Privacy Checklist for Students in K-12 Schools
4. Library Privacy Checklist for Public Access Computers and Networks
5. Library Privacy Checklist for E-book Lending and Digital Content Vendors
6. Library Privacy Checklist for Data Exchange Between Networked Devices and Services
7. Library Privacy Checklist for Library Management Systems / Integrated Library Systems

The subcommittee submitted the checklists to the IFC, which approved all seven documents. They are attached as information items 19.1 – 19.7.

The Privacy Subcommittee has planned both a webinar and a series of blog posts to observe this year's Choose Privacy Week, which takes place May 1-7, 2017. The theme for this year's Choose Privacy Week is "Pretty Darn Good Privacy." As part of its preparations, the subcommittee is revamping and redesigning the Choose Privacy Week website to serve as a hub for privacy education and guidance for libraries and librarians seeking information on implementing best privacy practices.

The subcommittee will begin work on additional privacy guidelines and checklists to address a number of emerging privacy issues for libraries. These include assistive devices, the use of biometric identifiers, mobile applications, and the use of patron data for marketing. The subcommittee also plans to revise the existing document, "RFID in Libraries: Privacy and Confidentiality Guidelines" which was last revised in 2006.

ISSUES

Hate crimes and challenges to library materials

Since 1990 – when ALA began formally documenting censorship – OIF has received an average of one challenge per day. Since November 2017, OIF began to observe an uptick in the number of hate crimes in libraries, prompting the office to begin documenting such incidents for the challenge database. Working with the Office for Diversity, Literacy and Outreach Services, OIF may be able to develop additional support for the field.

All reports submitted to the Office for Intellectual Freedom are kept confidential unless the challenge is reported in the media or if the person reporting the challenge has given permission to share information about the challenge. The following are public reports.

Material Challenges

The following are a few notable cases of the public challenges OIF has documented since Sept. 1, 2016:

Accomack County Public Schools (VA) received a formal complaint from a parent against the use of *To Kill a Mockingbird* and *The Adventures of Huckleberry Finn* due to their racial slurs. The books were retained.

Issaquah High School (WA) library received a formal complaint from a parent whose 14-year-old son brought home the comic book *Mangaman* by Barry Lyga. The book contains a sexual scene between two characters. The book was retained.

The Perks of Being a Wallflower by Stephen Chbosky was challenged for "supporting illegal and immoral behavior" at Hempstead High School (IA). It was retained.

I Know Why the Caged Bird Sings and *The God of Small Things* were withdrawn from Lemont High School (IL) after a parent submitted a complaint.

When an excerpt of *Wolf Boys: Two American Teenagers and Mexico's Most Dangerous Drug Cartel* by Dan Slater circulated in Texas Monthly, the Texas Department of Criminal Justice (TDCJ) Directors Review Committee read the book and decided to ban it because it contained "material on the setting up and operation of criminal schemes or how to avoid detection of criminal schemes by lawful authorities charged with the responsibility of detecting such illegal activity." Gabriel Cardona and Rosalio Reta, the subjects of *Wolf Boys*, are current inmates of TDCJ.

Author Disinvitations

At Northumberland County School District (VA), author Steve Watkins was asked by a principal to read from another book at a middle school assembly because of his book's profanity. In a high school English class, the same principal interrupted Watkins' discussion to escort him from the building.

Hate Crimes

Since November, OIF has documented nine hate crimes. These public reports include a patron threatening a library worker at the Salt Lake County Library's Columbus Branch, swastika vandalism at the Kansas City Public Library (MO) and Cottage Grove Public Library (OR), and vandalism at the Casa Guadalupe Literacy Center (WI) and Everett Public Library (WA).

Intellectual Freedom Q&As and Guidelines

The Intellectual Freedom Committee approved "Q&A: Makerspaces, Media Labs and Other Forums for Content Creation in Libraries." The Q&A addresses uses, eligibility, liability and policies of content creation in libraries. It has undergone numerous legal reviews, including a vetting by FTRF general counsel Theresa Chmara. The document is attached as information item 19.8.

The Intellectual Freedom Committee also approved "Guidelines to Minimize the Negative Effects of Internet Content Filters on Intellectual Freedom." The document is attached as information item 19.9. The IFC will continue elaborating on the guidelines with a Q&A, tools and practical examples supplement.

PROJECTS

Banned Books Week

The 2016 Banned Books Week (Sept. 25 - Oct. 1) theme was "Stand Up for Your Right to Read," featuring graphics centering on superhero icons and highlighting diverse authors and themes. For the ALA-led initiative, ALA collaborated with SAGE Publishing to host "Battling Bannings," a webinar on censorship from an author's perspective that included author Herthel, co-author of "I Am Jazz." OIF Assistant Director Kristin Pekoll also led a "50 Shades of Banned Books Week" webinar, outlining program and display ideas.

The Public Affairs Office tracked more than 1,176 articles/mentions of Banned Books Week, resulting in a circulation rate of more than 2.8 billion. Coverage highlights included Publishers Weekly, TIME, The Guardian (UK), TIME for Kids, National Geographic, CNN.com, Quartz, Bloomberg News, Washington Post, Houston Public Radio, Atlanta Public Radio, Voice of America Radio, and the New York Times.

The OIF blog published opinion pieces from several notable authors during Banned Books Week, including Chris Crutcher and Alex Gino. That week, the blog saw a 58% increase in views compared to the previous week. OIF's Thunderclap — a platform that releases an advocacy message on participants' social media accounts on the same day — reached an audience of 1.6 million people, prompting the hashtag #BannedBooksWeek to trend on Twitter Sept. 26.

ALA collaborated with the U.K. for the first Banned Book Week across the pond. London's Islington Library and Heritage Services partnered with the British Library and Free Word to host two speaker programs. According to Islington Library and Heritage Services, the organization was inspired by ALA to raise awareness about censorship.

Our Voices

Our Voices – a Chicago initiative of OIF and ALA Office for Diversity, Literacy, and Outreach Services to promote the growth of diverse, quality content in library collections – established an

Advisory Council, comprised of leaders from the publishing, bookselling and library communities. The Advisory Council made an appearance at the Chicago Book Expo on Nov. 8, where the panelists discussed independent publishing and diversity in literature trends. Our Voices is currently working with the Independent Publishers Group to set up an online submission form for writers to submit their work. The next steps are to recruit librarians to review the submissions for quality.

Intellectual Freedom Advocacy Bootcamp

The Office for Library Advocacy (OLA) and OIF launched Advocacy Bootcamp, a new advocacy training geared for state chapter conferences. It focuses on the mentoring of new advocates, building an advocacy plan for individual libraries and creating consistent messaging for all types of libraries. Building on the momentum and resources of ALA's new public awareness and advocacy campaign, Libraries Transform, the bootcamp emphasizes four key messages:

- Libraries transform lives.
- Libraries transform communities.
- Librarians are passionate advocates for lifelong learning.
- Libraries are a smart investment.

OIF Director James LaRue and OLA Director Marci Merola have hosted two bootcamps and have seven more scheduled.

Resolution on Gun Violence

The Intellectual Freedom Committee approved the substitute Resolution on Gun Violence Affecting Libraries, Library Workers, and Library Patrons, prepared by the Joint COL/IFC Working Group.

Resolution on Access To Accurate Information

In 2005, Council adopted the resolution on Disinformation, Media Manipulation & the Destruction of Public Information, which presciently recognized the growing problem of disinformation and its impact on access to public information and civic discourse. Because of a growing trend over the past several years of not only information disappearing from the public domain, but also actual disinformation propagated across multiple media platforms, the committee felt this resolution should be reaffirmed and updated to reflect the current media environment.

ACTION ITEM

The Intellectual Freedom Committee moves the adoption of the following action item:
CD # 19.10, Resolution on Access to Accurate Information.

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)
Helen Adams

Doug Archer

Danita Barber-Owusu

Hannah Buckland

Teresa Doherty

John Mack Freeman

Clem Guthro

Jean McFarren

Jo Rolfe

Keila Zayas-Ruiz

Melissa Butler (intern)

Johana Orellana (intern)

Library Privacy Checklist
Overview

This is checklist is intended to help libraries of all capacities take practical steps to implement the principles that are laid out in the Library Privacy Guidelines. It is an overview checklist that highlights general actions that are applicable across multiple guidelines. There are also **specific checklists** that libraries can consult for each guideline.

Priority 1 are actions that hopefully all libraries can take to improve privacy practices. Priority 2 and Priority 3 actions may be more difficult for libraries to implement depending on their technical expertise, available resources, and organizational structure.

Priority 1 Actions

1. Create a policy that addresses the collection of patron information. Such a policy should specify that the library is not collecting more patron information than what it needs and that it is not keeping the personally identifiable information of patrons longer than what is necessary.
    a. Create a privacy policy that is understandable by a layperson.
    b. Make sure the privacy policy is posted in the library where the public can see it.
    c. Ensure that the privacy policy includes information about what information the library is tracking, why, and for how long the data is kept.
    d. Ensure that the privacy policy includes when patron information can be shared and under what conditions.
2. Destroy all paper records with user data, such as computer sign-in sheets.
3. Ensure all existing security certificates for HTTPS/SSL are valid and create a procedure for revalidating them annually.
4. Designate a Library Privacy Officer to handle requests for personally identifiable information of patrons from law enforcement officials and other third parties.

Priority 2 Actions

1. Ensure there is a formal process in place to address breaches of patron data directly under library control or maintained by third parties. The library should notify affected users when they become aware of a breach.
2. Encrypt all user data with secure algorithms in all network and application communications.
3. Purge search history records regularly, ideally when the individual computer session ends.
4. Purge circulation and interlibrary loan records when they are no longer needed for library operations. Any patron data that is kept for analysis should be anonymized or de- identified and have access restricted to authorized staff.
5. Utilize HTTPS wherever possible.
6. Ensure that the privacy policy is updated often and schedule regular times for its review.

Priority 3 Actions

1. Publish and distribute flyers and/or web content for patrons that includes information on how to protect personally identifiable information and other data.
2. Publish and distribute flyers and/or web content for patrons about available software and alternative browsers and plugins to protect their privacy online and can be used in the library.
3. Publish and distribute flyers and/or web content about VPN services and/or Tor and patrons' ability to use these systems on the library network.
4. Test compliance with these standards through a trusted third party service or individual.

Resources

1. ALA's Guidelines for Developing a Library Privacy Policy: http://www.ala.org/advocacy/privacyconfidentiality/guidelines-developing-library-privacy- policy
2. How to Geek's 5 Alternative Search Engine's That Respect Your Privacy: http://www.howtogeek.com/113513/5-alternative-search-engines-that-respect-your- privacy/
3. ALA's Library Bill of Rights: http://www.ala.org/advocacy/intfreedom/librarybill
4. ALA's Privacy Toolkit: http://www.ala.org/advocacy/privacyconfidentiality/toolkitsprivacy/privacy
5. EFF Surveillance Self Defence - Choosing the VPN That's Right for You: https://ssd.eff.org/en/module/choosing-vpn-thats-right-you
6. EFF Surveillance Self Defence - Introduction to Threat Modeling: https://ssd.eff.org/en/module/introduction-threat-modeling
7. EFF Surveillance Self Defence - Keeping your Data Safe: https://ssd.eff.org/en/module/keeping-your-data-safe
8. EFF Surveillance Self Defence - Seven Steps to Digital Security: https://ssd.eff.org/en/module/seven-steps-digital-security
9. NIST'S Policy on Hash Functions http://csrc.nist.gov/groups/ST/hash/policy.html

2016-2017 ALA CD #19.2
2017 ALA Midwinter Meeting

Library Privacy Checklist for Library Websites, OPACs, and Discovery Services

This checklist is intended to help libraries of all capacities take practical steps to implement the principles that are laid out in the Library Privacy Guidelines for Library Websites, OPACs, and Discovery Services.

Priority 1 are actions that hopefully all libraries can take to improve privacy practices. Priority 2 and Priority 3 actions may be more difficult for libraries to implement depending on their technical expertise, available resources, and organizational structure.

Priority 1 Actions

1. Establish a library privacy policy which includes data privacy and security policies based on legal regulations and professional/industry standards.
    a. Ensure that the privacy policy is readily available in easy-to-understand language to users of a library website, social media site, OPAC or discovery service.
    b. Provide links to third party privacy and terms of service pages for users when appropriate.
2. Limit the amount of personal information collected about users. In general, the library or service provider should collect the minimum personal information required to provide a service or meet a specific operational need.
3. Provide users with 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 such as borrower history, reading lists, or favorite books.
    a. Configure services directly under library control to use the opt-in method whenever possible for features that involve the collection of personal information.
    b. Work with providers to configure external services to use the opt-in method whenever possible for features that involve the collection of personal information. This ability to opt-in should be an important criteria when the library decides to select or renew a service.
    c. 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.

4. Establish procedures that restrict access to personal information 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. Ideally these procedures are supported by technical measures such as role-based permissions for staff account.
5. Provide training to library staff who manage the library's websites, OPACs, and discovery services on the library's privacy policy and best practices for safeguarding patron privacy. Library staff that negotiate contracts with vendors that provide websites and services should also receive privacy training.

Priority 2 Actions

1. Create a proactive process to notify ongoing users of any changes to the library's privacy policy or any violations in user privacy through inadvertent dissemination or data theft.
    a. In the event of a data breach libraries should describe what steps are being taken to remedy the situation or mitigate the possible damage, and what steps patrons should take to protect themselves.
    b. Consider enacting canary warnings to notify patrons when information may have been subpoenaed through a court order.
2. Evaluate the impact on user privacy of all third-party scripts and embedded content (e.g. cover images, ratings, reviews, etc.) that are included in a library website, OPAC, or discovery service.
    a. Limit use of Javascripts from third-parties on library sites.
    b. Avoid Flash-based plugins.
    c. Review any terms of service for scripts and embedded content, as they often allow the third party to harvest user activity data for their own purposes.
    d. Consider alternative solutions that better respect user privacy. For example, use Piwik for web analytics instead of Google Analytics.
3. Do not retain in perpetuity any user activity data with personally identifiable information.
    a. Establish policies for how long to retain different types of data and methods for securely destroying data that is no longer needed.
    b. Retention policies should also cover archival copies and backups.
    c. Anonymize or de-identify user data stored for assessment or metrics. Anonymization provides better protection than de-identification.
    d. Anonymize reports and web analytics intended for wider distribution by removing or encrypting personally identifiable information.
4. Provide users the ability to access their own personal information and evaluate its accuracy. Guidance on how the user can access their personal data and offer corrections if needed should be clear and easy to find.

5. Ensure that all services directly under library control are secure.
    a. Stay aware of and remediate known exploits.
    b. Keep software and applications up-to-date.
    c. Monitor logs for intrusions and perform regular security audits.
    d. Perform regular backups and have a disaster recovery plan. Note that backups should be subject to your policy on data retention.
6. Work with service providers to review contracts/licenses and if needed revise them so that they are in compliance with relevant legal regulations and library policy.
    a. Create an addendum to contracts regarding liability for data breaches that affect user privacy.

Priority 3 Actions

1. Establish and maintain effective mechanisms to enforce library privacy policies. Conduct regular privacy audits to ensure that all operations and services comply with these policies.
2. Encrypt all online transactions between client applications (web browsers, e-book readers, mobile apps, etc.) and server applications using modern, up-to-date security protocols for SSL/HTTPS. Communications between server applications and third-party service providers should be encrypted.
3. Store user passwords using up-to-date best practices for encryption with a cryptographically secure hash.
4. Ensure that any personally identifiable information and user data housed off site (cloud-based infrastructure, tape backups, etc.) uses encrypted storage.
5. Explore the possibility of two-factor authentication and implement if possible.

Resources

1. Example Privacy Policy from NYPL
2. Personally Identifiable Information
3. HTTPS Everywhere
4. Let's Encrypt
5. How to Check if your Library is Leaking Catalog Searches to Amazon
6. Warrant Canary
7. A Visual Guide to Practical Data De-Identification
8. NISTIR 8053: De-Identification of Personal Information
9. Password Storage Cheatsheet

2016-2017 ALA CD #19.3
2017 ALA Midwinter Meeting

Library Privacy Checklist for Students in K-12 Schools

This checklist is intended to help libraries of all capacities take practical steps to implement the principles that are laid out in the Library Privacy Guidelines for Students in K-12 Schools.

Priority 1 are actions that hopefully all libraries can take to improve privacy practices. Priority 2 and Priority 3 actions may be more difficult for libraries to implement depending on their technical expertise, available resources, and organizational structure.

Priority 1 Actions

1. Create internal library procedures to protect student privacy based on:
    a. school policies related to privacy and confidentiality of student data, especially student circulation records and the use of library resources in all formats.
    b. federal laws such as the Family Educational Rights and Privacy Act (FERPA), Children's Online Privacy Protection Act (COPPA), and state privacy laws regarding library records.
    c. ALA and AASL policy statements, online tool kits and Q&As, guidelines, and other resources provided by national and state library associations.
2. Collect the minimum amount of information necessary about students to conduct library business.
3. Configure circulation software to delete students' borrowing history and retain only necessary records.
4. Ensure any paper records with sensitive information are stored in a secure area and shredded when no longer needed.
5. Train library staff and volunteers to respect students' privacy and the confidentiality of their library records.

Priority 2 Actions

1. Educate administrators, faculty, and support staff about students' library privacy and the confidentiality of student data using a variety of communication methods.
    a. Initiate conversations with the principal, teachers, students, and parents about the need for an official library privacy policy.
2. Add privacy-related resources to the library collection including items related to personal privacy, minors' privacy rights, and privacy as a national and international issue.
    a. Consider creating a privacy information section on the school library web page

or a privacy-themed pathfinder (e.g. LibGuide) with privacy resources.

3. Integrate online privacy into library instruction and programming. For example:
    a. Introduce students to online privacy information such as secure passwords and web tracking during library orientations and other brief presentations.
    b. Celebrate Choose Privacy Week and other privacy-related observances (Data Privacy Day, Teen Tech Week, etc.) with the school community.
    c. Create privacy-related displays and set up videos in the library to educate parents during parent-teacher conferences and other evening school and community events
    d. Offer presentations to parents about students' privacy online and other topics of interest to families.
4. Advocate within the school or district for protecting students' privacy rights in learning management systems or other technologies that enable educators to monitor student reading and research habits. Assessment should not include monitoring how students use specific library materials and online resources as part of free inquiry and research.
5. Volunteer to serve on the school's data governance committee. If one does not exist, advocate for its creation.

Priority 3 Actions

1. Work with other stakeholders in the school or district to create an official library privacy policy in regards to student circulation records and the use of library resources.
    a. The privacy policy should be approved by the school's governing body (e.g. school board, school committee, etc.)
    b. Post the policy in the library and on the library's section of the school website.
    c. Promote the library's privacy policy within the school community.
2. Work through school lines of authority to write or adapt a K-12 privacy curriculum and have it formally approved and taught. Collaboratively teach privacy units with teachers using the iKEEPSAFE and/or other privacy curricula.
3. Work with school officials to incorporate privacy protections into RFP's and resulting contracts. Discuss privacy concerns with digital resource and technology vendors, especially in regards to the school's/library's contracts with these vendors.
4. Ensure that all online transactions between client applications and server applications are encrypted.
5. Ensure that storage of personally identifiable student information is housed using encrypted storage.

Resources

ALA/AASL Policy Statements

- ALA/AASL Policy Statements Position Statement on the Confidentiality of Library Records. http://www.ala.org/aasl/advocacy/resources/statements/library-records
- ALA. 2008. Code of Ethics. http://www.ala.org/advocacy/proethics/codeofethics/codeethics
- ALA. 2014. Privacy: An Interpretation of the Library Bill of Rights. http://www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy

Legislation

- American Library Association. State Privacy Laws Regarding Library Records. http://www.ala.org/advocacy/privacyconfidentiality/privacy/stateprivacy
- Federal Trade Commission. Children's Online Protection Act (COPPA) Rule. https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule
- U.S. Department of Education. Laws and Guidance: Family Educational Rights and Privacy Act (FERPA). http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html
- U.S. Department of Education. Laws and Guidance: Family Policy Compliance Office. http://www2.ed.gov/policy/gen/guid/fpco/index.html

Learning Resources

- ALA. Choose Privacy Week. Students and Minors' Privacy- Selected Resources. https://chooseprivacyweek.org/students-and-minors-privacy/
- ALA. Intellectual Freedom News. Note: Subscribe to future issues of Intellectual Freedom News, a free biweekly compilation of news delivered via email by the ALA Office for Intellectual Freedom. Web form URL: http://ala.informz.net/ala/profile.asp?fid=3430
- ALA. 2014. Privacy Tool Kit. http://www.ala.org/advocacy/privacyconfidentiality/toolkitsprivacy/privacy
- ALA. 2014. Questions and Answers on Privacy and Confidentiality. http://www.ala.org/advocacy/intfreedom/librarybill/interpretations/qa-privacy
- Christine Eldred. Colchester High School (VT) Intellectual Freedom LibGuide. (with Choose Privacy Week tab) http://chs.csdvt.libguides.com/intellectualfreedom
- Common Sense Media. Privacy and Internet Safety [Information aimed at parents]. https://www.commonsensemedia.org/privacy-and-internet-safety#
- Consortium for School Networking. Protecting Privacy in a Connected World. http://cosn.org/focus-areas/leadership-vision/protecting-privacy
- Library Freedom Project. "Teen Privacy Guide." https://libraryfreedomproject.org/teenprivacyguide/

- National Cyber Security Alliance. “Privacy Library.” https://staysafeonline.org
- YALSA. Teen Tech Week. http://teentechweek.ning.com/page/faq
- U.S. Department of Education. Privacy Technical Assistance Center. http://ptac.ed.gov/

Teaching Tools

- ALA. Choose Privacy Week Programming Guide and Activities. 2010 http://chooseprivacyweek.org/wp-content/uploads/2013/04/CPWResourceGuideProgram.pdf
- iKEEPSAFE. K-12 Curriculum Matrix. November 2015. http://ikeepsafe.org/privacy-k-12-curriculum-matrix/
- San Jose Public Library. Virtual Privacy Lab. (modules in English, Spanish, and Vietnamese)https://www.sjpl.org/privacy
- Digital Defenders (free, CC-licensed kids' booklet about privacy) https://edri.org/files/privacy4kids_booklet_web.pdf

Advocacy

- Data Quality Campaign and Consortium for School Networking. Student Data Principles. http://studentdataprinciples.org/the-principles/
- Electronic Privacy Information Center. Student Privacy Bill of Rights. https://epic.org/privacy/student/bill-of-rights.html
- Future of Privacy Forum (FPF) and the Software and Information Industry Association (SIIA). Student Privacy Pledge. https://studentprivacypledge.org/privacy-pledge/

2016-2017 ALA CD #19.4
2017 ALA Midwinter Meeting

Library Privacy Checklist
Public Access Computers and Networks

This checklist is intended to help libraries of all capacities take practical steps to implement the principles that are laid out in the Library Privacy Guidelines for Public Access Computers and Networks.

Priority 1 are actions that hopefully all libraries can take to improve privacy practices. Priority 2 and Priority 3 actions may be more difficult for libraries to implement depending on their technical expertise, available resources, and organizational structure.

Priority 1 Actions

1. Use analog signage and/or splash screens to explain the library's network and Wi-Fi access policies, including any privacy-related information.
    a. Make a policy decision about the level of privacy versus convenience that the library will offer its Wi-Fi users and adequately warn users of potentials for traffic interception and other risks of an insecure network.
2. Set up public computers to purge downloads, saved files, browsing history, and other data from individual user sessions. This can be accomplished
    a. on logout via the computer reservation system if the library uses such a system;
    b. by using restoration software such as CleanSlate or Deep Freeze;
    c. by configuring browsers to clear all history and other usage data upon exit.
3. Ensure that paper sign-up sheets for public computers, devices, or classes are destroyed when no longer needed.
4. Offer classes and other educational materials to users about best practices for privacy and security when using the library's public computers.
5. Offer privacy screens to patrons who desire to use them.

Priority 2 Actions

1. Use antivirus software on all public computers. Ensure that antivirus software that is installed has the ability to block spyware and keylogging software.
2. Ensure that any computer reservation management system records, print management records, or ILS records in regards to computer use are anonymized or destroyed when no longer needed.
3. Configure any content filters to not collect or store browsing data.
4. Anonymize or destroy transactional logs for network activity when no longer needed.

5. Perform regular security audits on all public computers, including digital inspection of security risks and flaws and physical inspection for unknown devices.

Priority 3 Actions

1. Install plugins on public computers to limit third party tracking, enable private browsing modes, and force HTTPS connections.
    a. HTTPS Everywhere: https://www.eff.org/https-everywhere
    b. Privacy Badger: https://www.eff.org/privacybadger
    c. See guides about Firefox security options, e.g. https://securityinabox.org/en/guide/firefox/windows
2. Install the Tor browser on public computers as a privacy option for patrons.
3. Offer the privacy-oriented Tails OS on bootable USB or CDROM for use on public computers or patron devices.
4. Install malware-blocking, ad blocking, and anti-spam features on firewalls.
5. Segment the network to isolate staff computers, public computers, and wireless users into their own subnets.
6. Ensure that any applications and operating systems on public computers are disabled from automatically sharing activity data with software publishers (e.g. error reporting).

Resources:

https://securityinabox.org/en/guide/basic-security/windows

https://libraryfreedomproject.org/resources/privacytoolkit/

http://www.dataprivacyproject.org/mapping-data-flows/

https://www.consumer.ftc.gov/media/video-0080-public-wi-fi-networks

https://www.sjpl.org/privacy/security-how-internet-works

https://www.f-secure.com/en/web/labs_global/threat-descriptions

http://www.howtogeek.com/221929/how-to-choose-the-best-vpn-service-for-your-needs/

http://www.niso.org/apps/group_public/download.php/16064/NISO%20Privacy%20Principles.pdf

https://www.amazon.com/Protecting-Patron-Privacy-Practices-Computers/dp/1610699963

2016-2017 ALA CD #19.5
2017 ALA Midwinter Meeting

Library Privacy Checklist
For E-book Lending and Digital Content Vendors

This checklist is intended to help libraries of all capacities take practical steps to implement the principles that are laid out in the Library Privacy Guidelines for E-book Lending and Digital Content Vendors.

Priority 1 are actions that hopefully all libraries can take to improve privacy practices. Priority 2 and Priority 3 actions may be more difficult for libraries to implement depending on their technical expertise, available resources, and organizational structure.

Priority 1 Actions

1. Provide links to vendor privacy policies and terms of service pages for users when appropriate, e.g. from the library's own privacy policy page or from a library web page about the vendor's product or service.
2. Work with vendors to configure services to use the opt-in method whenever possible for features that involve the collection of personal information.
3. Develop a strategy to assist patrons in managing their privacy when using vendor products and services. The strategy could include in-person reference, handouts, web guides, classes, or other programming. Topics covered could include:
    a. Settings for personal accounts on vendor websites.
    b. Vendor applications on personal devices including any privacy settings and how to remove the application and any associated stored data.
4. Notify staff and patrons of any data breaches and assist patrons in mitigating the impact (changing passwords, uninstalling applications, etc.).

Priority 2 Actions

1. Add privacy considerations to the library's selection criteria for new purchases or the renewal of existing purchases. These considerations should include the vendor:
    a. Notifying users of their privacy policies at the point of access and restricting the collection of patron data to clearly stated operational purposes.
    b. Seeking patron consent for data collection by using the opt-in method whenever possible for features that involve the collection of personal information.
    c. Providing a method for patrons to access, review, correct and delete their personal data.
    d. Encrypting connections using SSL/HTTPS to provide secure access to digital content.
    e. Allowing users to uninstall vendor applications and delete associated stored data from personal devices.
2. Review all new license agreements regarding the use, aggregation, retention, security,

and dissemination of patron data. Before purchasing a new product or service the library should ensure that the license agreement:

a. Complies with all applicable local, state, and federal laws regarding the confidentiality of library records.
b. Conforms to the library's privacy, data retention, and data security policies.
c. Stipulates that the library retains ownership of all patron data.
d. Includes a protocol for responding to government and law enforcement requests for patron data.
e. States the vendor's responsibilities to notify the library and affected patrons in the event of a data breach.

Priority 3 Actions

1. Review existing license agreements using the privacy concerns outlined above for new agreements.
    a. Work with vendors to change language of license agreements when possible to address concerns.
    b. Consider not renewing contracts with vendors that are unable to provide these assurances in the license agreement.
2. Review vendors' data governance plan that addresses patron consent, data security, encryption, anonymization, retention, dissemination/data sharing, and destruction. If the vendor does not have a plan, ask them to create one.
3. Request that vendors conduct regular privacy audits and make audit results available to the library for review. Make the results of the review one of the criteria for renewal.

Resources

ALA. "Encryption and Patron Privacy." *American Library Association*, 2016, www.ala.org/advocacy/encryption-and-patron-privacy

Cavoukian, Ann. "Privacy by Design: The 7 Foundational Principles; Implementation and Mapping of Fair Information Practices." *Internet Architecture Board*, 2011, https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf

Department of Computer Engineering, Boğaziçi University. "Guide to Data Protection Auditing." *Data Protection*, http://www.cmpe.boun.edu.tr/~ozturan/etm555/dataaudit/html/refer/checks/index.htm

Hoffman-Andrews, Jacob. "What Every Librarian Needs To Know About HTTPS." *Electronic Frontier Foundation*, 6 May 2015, https://www.eff.org/deeplinks/2015/05/what-every-librarian- needs-know-about-https

International Association of Privacy Professionals. "Security Breach Response Plan Toolkit." *IAPP Resource Center*, 2016, https://iapp.org/resources/article/security-breach-response-plan-toolkit/

Internet Security Research Group. *Let's Encrypt* [https certificate registry], https://letsencrypt.org/

Perera, Charith, McCormick, Ciaran, Bandara, Arosha K., Price, Blaine A., and Bashar Nuseibeh. "Privacy-By-Design Framework for Assessing Internet of Things Applications and Platforms." *IoT 2016, 7-9 Nov. 2016, Stuttgart, Germany*, https://arxiv.org/pdf/1609.04060v1.pdf
Riffat, Muzamil. "Privacy Audit - Methodology and Related Considerations." *ISACA Journal*, vol. 1, 2014, http://www.isaca.org/Journal/archives/2014/Volume-1/Pages/Privacy-Audit- Methodology-and-Related-Considerations.aspx
Chmara, T. (2012). Privacy and E-Books. Knowledge Quest, 40(3), 62-65.

Additional Questions to Consider

- What are the local statutes regarding patron/user information use?
- Does the vendor's privacy policy jive with the library's privacy policy?
- Is the vendor's privacy policy explicit on the product portal?
- Can the vendor's privacy policy be shared with the library to publicize for its users?
- User's browsing, borrowing, downloads, notations, group affiliations shall not be shared with any other parties without the specific written consent of the individual user.
- Does the language in the policy/contract/license specifically address other devices and do the terms extend to other devices as well (smartphone apps, tablet, etc.)?
- What is the retention policy of the institution/library, including proxy server collection of IP address access, and what is the retention policy of the vendor?
- Is the language of the policy consistent with the age of the product's intended audience, can the minor user for instance understand the policy?
- Does the language of the policy/contract/license specify that harvested user data should be destroyed and not retained in perpetuity by the vendor?
- In case of data breach, does the language specify that the vendor inform the library as soon as it is aware of the breach?
- How should the library respond in terms of user privacy when a data breach is identified?
- Vendor must give libraries advance notice of any changes to the user privacy policies, at least 30 days to respond.
- Agreements and contracts should be reviewed annually per their individual renewal/ purchase date.

2016-2017 ALA CD #19.6
2017 ALA Midwinter Meeting

Library Privacy Checklist for Data Exchange Between Networked Devices and Services

This checklist is intended to help libraries of all capacities take practical steps to implement the principles that are laid out in the Library Privacy Guidelines for Data Exchange Between Networked Devices and Services.

Priority 1 are actions that hopefully all libraries can take to improve privacy practices. Priority 2 and Priority 3 actions may be more difficult for libraries to implement depending on their technical expertise, available resources, and organizational structure.

Priority 1 Actions

1. Establish minimum security practices for devices and services.
    a. Change any default passwords.
    b. Disable remote access to the superuser account (i.e. root or administrator).
    c. Keep all software up-to-date using a secure and verified source.
2. Require authentication for all client connections to services that allow access to patron information.
    a. Limit clients to only the access they need, i.e. the least privilege model.
    b. Enable mutual authentication of server and client if supported.
    c. Use a secure authentication standard such as oauth when feasible.
3. Implement a logging policy for devices and services that covers rotation and retention, types of data collected, and the implications on patron privacy.

Priority 2 Actions

1. Harden security on devices and services.
    a. Disable any extraneous services that are running on devices.
    b. Limit administrative privileges to authorized individuals through user access controls or the sudo program.
    c. Require a unique password for each instance of a service.
    d. Implement and enforce a strong password policy that specifies password length, formation, and duration. Consider using randomly generated passwords.
2. Encrypt data communications between client applications and server applications that may include patron information.
    a. Configure services when possible to require encryption by default, i.e. do not allow unencrypted connections.
    b. If services do not support encryption (e.g. SIP2), use an encrypted transport

such as SSH tunnel or a VPN.

3. Encrypt sensitive data at rest (i.e. data warehouses, archives, tapes, offsite backups, etc.).
4. Store passwords in applications using up-to-date best practices for encryption (i.e. hashed and salted).

Priority 3 Actions

1. All remote access (including SSH) should be through secure keys not passwords.
    a. Keys should be no less than 2048 bit, 4096 bit is preferable.
    b. Do not allow deprecated or insecure ciphers.
    c. Ensure private keys are secure (use subkeys and keep master keys very safe).
    d. Rotate keys regularly and be ready to revoke them in case of compromise.
2. Review the protocols employed by devices and services. Protocols should:
    a. Be standard, established, and open.
    b. Not be deprecated due to security concerns.
    c. Support data integrity including origin authentication, non-repudiation of origin, non-repudiation of receipt, and verification of payload using cryptographic signature or a hash.
3. Verify security of devices and services by using penetration testing tools.

Resources

Passwords: CPNI

Burr, W. E., Dodson, D. F., & Elaine, M. (2011). Newton, Ray A. Perlner, W. Timothy Polk, Sarbari Gupta, and Emad A. Nabbus. Electronic authentication guideline. *NIST Special Publication*, 800-63.

Chandramouli, R., Iorga, M., & Chokhani, S. (2014). Cryptographic key management issues and challenges in cloud services. In *Secure Cloud Computing* (pp. 1-30). Springer New York.

Hoeper, K. & Chen, L. (2009). *Recommendation for EAP Methods Used in Wireless Network Access Authentication*. Retrieved from: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-120.pdf

Jakimoski, K. (2016). Security Techniques for Data Protection in Cloud Computing. *International Journal of Grid and Distributed Computing*, *9*(1), 49-56.

Jansen, W., & Grance, T. (2011). Guidelines on security and privacy in public cloud computing. *NIST special publication*, *800*(144), 10-11.

National Center for Education Statistics (Ed.). (n.d.). Chapter 6: Maintaining a Secure Environment, Weaving a Secure Web around Education: A Guide to Technology Standards and Security. Retrieved from https://nces.ed.gov/pubs2003/secureweb/ch_6.asp

Peng, C., Kesarinath, G., Brinks, T., Young, J., & Groves, D. (2009). Assuring the Privacy and Security of Transmitting Sensitive Electronic Health Information. *AMIA Annual Symposium Proceedings*, *2009*, 516–520.

Singhal, A., Winograd, T., & Scarfone, K. (2007). Guide to secure web services. *NIST Special Publication*, *800*(95), 4.

Tysowski, P. (2016). OAuth Standard for User Authorization of Cloud Services. *Encyclopedia of Cloud Computing*, 406-416

2016-2017 ALA CD #19.7
2017 ALA Midwinter Meeting

Library Privacy Checklist for Library Management Systems / Integrated Library Systems

This checklist is intended to help libraries of all capacities take practical steps to implement the principles that are laid out in the Library Privacy Guidelines for Library Management Systems. Library Management Systems (LMS) are also known as Integrated Library Systems (ILS).

Priority 1 are actions that hopefully all libraries can take to improve privacy practices. Priority 2 and Priority 3 actions may be more difficult for libraries to implement depending on their technical expertise, available resources, and organizational structure.

Priority 1 Actions

1. Develop a privacy policy about patron information in the LMS and publish it on the library's website in a place that is easy to find.
2. Request and store only the personal information about patrons necessary for library operations. Periodically remove data that is no longer necessary for library operations (e.g. purchase-request data).
    a. If the LMS supports it, use "fuzz" demographic information wherever possible (e.g. use a "minor/not a minor" classification instead of recording full birth date).
3. Aggregate or anonymize reports to remove personally identifiable information. Reports should be periodically reviewed to ensure they are not revealing this type of information.
4. Configure the LMS by default to remove transactional data between patrons and materials they borrow / access when it is no longer needed for library operations.
    a. Allow patrons the ability to opt-in to personalization features like keeping their checkout history or a list of favorite titles.
    b. Allow patrons to later opt-out of features if they change their mind. Ensure that data previously retained for these features is deleted when patrons opt out.
5. Develop procedures for library staff on how to handle law enforcement and government requests for patron records.

Priority 2 Actions

1. Restrict access to patron records in the LMS to staff members with a demonstrated need for it. For example, circulation staff need access but shelvers do not.
2. Configure library notifications for holds, overdues, etc. to send a minimal amount of personal information.

3. Develop policies and procedures regarding the extraction, storage, and sharing of patron data from the LMS for in-house or contracted third-party use.
    a. Restrict access to the extracts to appropriate staff.
    b. The policy should include disposal/deletion of extracts.
4. Encrypt offline data backups to prevent access by unauthorized personnel.
5. Keep LMS applications and underlying server software up-to-date to mitigate the impact of security vulnerabilities.

Priority 3 Actions

1. Store all passwords (patron and staff) in a secure fashion using a proper cryptographic hash function. At this time bcrypt or better are good standards.
2. Encrypt all traffic between the LMS server and any client connections outside a secure LAN. For example, use a VPN to encrypt the connection over the Internet of a checkout station at a branch library to the LMS server at the main library.
3. Conduct regular audits of the network and LMS servers to make sure reasonable security measures are in place to prevent unauthorized access.
4. Create procedures to handle data breaches to unauthorized parties and mitigate their impact on patrons.

Resources

Marshall Breeding's article from the January 2015 *Smart Libraries Newsletter*
"Privacy and Security of Automation and Discovery Products"
https://librarytechnology.org/repository/item.pl?id=20425
Electronic Privacy Information Center (EPIC)
The Code of Fair Information Practices
https://epic.org/privacy/consumer/code_fair_info.html
Marshall Breeding - "Privacy and Security for Library Systems"
Library Technology Reports [May/June 2016]
https://librarytechnology.org/repository/item.pl?id=21672

2016-2017 ALA CD #19.8
2017 ALA Midwinter Meeting

Q&A: Makerspaces, Media Labs and Other Forums for Content Creation in Libraries

Statement of Purpose: This Q&A can be used as a guide by libraries as they create policies for makerspaces or other content creation forums within their facilities. It is not intended to be a template for such policies but rather a source for answers to questions that are likely to be asked as libraries formulate content creation policies. This document should not be construed as legal advice but may serve as insight as to when a library may need to seek legal advice.

Is a library really an appropriate space for hands on creative activities?

Historically libraries have often included in their functions the creation, as well as the preservation and dissemination, of content in many different formats. Libraries have supported and encouraged scholars, writers, inventors, artists and artisans, and provided study rooms, carrels, meeting, exhibit and performance spaces, as well as tools and equipment for individual and group use.

Providing 3D printers and other tools and technology in makerspaces, tech labs, STEM (Science, Technology, Engineering, and Math) or STEAM (Science, Technology, Engineering, Arts, and Math) labs, media labs, exhibit and performance venues, as well as other physical and virtual spaces for creative endeavors, is only the latest manifestation of the library's natural role in encouraging and facilitating the creativity and ingenuity of its community of users.

How does the public forum concept under the First Amendment apply to makerspaces, media labs and virtual spaces in libraries?

Case law has established that public libraries are designated public forums where the right of library users to access information and ideas in multiple formats is protected by the First Amendment. Public libraries may also provide physical spaces in their buildings, such as meeting rooms and/or display cases, as spaces where members of the community may exercise their First Amendment rights to gather and share information as well as ideas in various ways. When the library opens such spaces for public use, they become designated public forums. An academic and school library would generally be considered a non-public forum.

However if an academic or school library opened a meeting room or other space to public use, then it would be a designated or limited public forum as to that use and as defined by the entity. These libraries exercise greater control over access consistent with their missions. They may limit access to the library to the class of user intended to benefit from the library — *e.g.*, students, faculty, staff, and alumni. However, decisions about access to resources and the removal of materials remain subject to the First Amendment.

Technological innovation has expanded the ability of public, academic and school libraries to provide both physical and virtual spaces where library users have access to technology that allows them to create their own original content in many different formats and to gather to share, discuss and disseminate their original content on many different platforms.

Libraries may establish and equip such physical and virtual spaces as designated sites and platforms for creating, sharing and disseminating original content. Some current examples of such sites and platforms are makerspaces, media labs, social media sites, and print-on-demand services. Such sites and platforms may be limited to library-sponsored or library-related programs; or may be opened for access to events, exhibits, programs and performances sponsored by community groups and organizations; or opened for independent individual access and use. When a publicly funded library opens such sites and platforms for general public use, they will be considered a designated or limited public forum.

Are there any libraries to which this does not apply?
The First Amendment applies to federal, state and local governments and their agents, but not to private entities. Public libraries and public schools are considered governmental agents, so they are subject to the First Amendment restrictions on uses of public and limited public forums discussed above. However, private libraries—such as a private school library—are not.

What determines who is eligible to use such spaces in the library?
Every person who uses the library should have an equal opportunity to use all of the library's services. Access to designated forums for creative content should not be abridged or denied because of origin, age, background or views of the user. A library may give a higher priority to a defined community of library users. A publicly funded library may prioritize users who are taxpayers or cardholding members of the library or even limit or exclude users not meeting those criteria. Academic and school libraries may limit eligible users to persons who are students, faculty and staff of the college, university, or school.

Can a library set any kinds of limits on how a public forum it provides is used? Can it penalize misuse of the forum?
A library may set reasonable content-neutral time, place and manner restrictions on the use of the designated public forums for content creation. In a designated public forum, any content-based restrictions on access must meet a strict-scrutiny standard to be deemed constitutional. In other words, the restriction must serve a compelling government interest and be narrowly drawn to achieve that interest.

A library, such as a school or academic library, which is considered a nonpublic forum, may set content-based restrictions on the use of the forum if the restriction is reasonable in light of the mission of the institution and the uses for which it has been designated.
A user who violates the library's policy defining acceptable use of the forum may face consequences on the violations as stated in the policy, including suspending or terminating the right to use the forum (so long as the policy provides this possibility).

What should be addressed in an acceptable use policy?
Any use that violates federal, state, or local law, or library policy or guidelines, constitutes an unacceptable use of the content creation forum. Examples of issues to address in an acceptable use policy include, but are not limited to, the following:

- Damaging or otherwise misusing physical or virtual library resources

- Behaving in a manner that disrupts the orderly conduct of the physical or virtual forum, prevents other patrons from using library resources, or interferes with library employees performing their duties

- Creating or sharing content that is legally defined as obscene or child pornography, or knowingly sharing with minors content that is harmful to minors.

- Creating or sharing content that constitutes physical or virtual harassment of others as long as the library has consulted with legal counsel to be sure that a behavior policy including harassment offers clear guidance to patrons on what the term means and that legal counsel advises that the harassment definition meets constitutional tests.

- Transmitting or reproducing copyrighted or patented content without permission from the copyright or patent holder

- Hacking, misappropriating, tampering with or damaging the work-in-progress or shared content of other forum users, or redistributing their content without authorization

- Intentionally engaging in the distribution of malware or similar malicious software or hardware

- Using false identification to mislead others

- Using another individual's personally identifiable information without his/her explicit permission

The library's acceptable use policy should clearly state the consequences of violating the policy, including whether their library privileges may be denied or suspended and the procedure for doing so (including notification, penalties, reinstatement, and appeals).

What about costs? Who pays for materials consumed or damaged?
If a library charges cost-recovery fees for consumable materials used by participants in library-sponsored activities, provision should be made to cover fees for those who otherwise could not afford to participate. If a library's policy preclude waiving cost-recovery fees efforts should be made to find a sponsor — such as a "Friends of the Library" organization — to pay the fees. If a library charges cost-recovery fees for loss or damage to library property or resources, these fees need to be clearly stated in the policy, and the library should consider offering alternatives — such as volunteer service — to those who cannot afford the fees.

Who is responsible for preventing misuse and illegal activities?
Each user is personally responsible for appropriate and legal use of library spaces, equipment, hardware and software, Internet access, Web sites, social media and other resources. Generally, a library is not responsible for the actions of individual users as long as the library conspicuously posts an acceptable use policy that clearly states user responsibilities. In some cases, existing policies that serve as a measure of protection for the library, such as those addressing use of

copiers and printers may be broadly enough worded that they include new technology: if not, it may be possible to expand those policies rather than create new ones.

Can a user make items like a gun or sexually explicit images or toys?
While it is possible to create a gun using a 3-D printer, the software required to do so is complex and may be proprietary. Even if a user had access to the software to create parts of a gun, other parts required for it to function could not be created on the printer.

If a library's policy prohibits gun possession in the library then the creation of a gun or gun parts would violate that policy if that policy is in line with state law of gun possession. If state law allows possession of a gun in a library then the library would need to work with its legal counsel to determine if a legal prohibition against creating a gun can be fashioned within state law.

The same is true of creating sexually explicit images or toys. If a library policy prohibits sexually explicit material in the library then creation of sexual explicit images or toys also violate the rule but the library would need to work with its legal counsel to determine if the prohibition against sexually explicit materials has adequate definition that follows state law as well as constitutional tests.

Does a library's risk of liability increase with makerspaces? What about the librarian's?
Makerspaces may include technology such as laser cutters or sewing machines that present danger of physical harm to patrons and library workers and bring new risks of liability to a library and/or individual library employees and volunteers. The institution should employ a full legal and insurance review before it begins using such technology. That review should include all the risks new technology brings including copyright and patent infringement, defects in the technology and, defects or misuse of content created with that technology.

Does a library have a responsibility to vet or approve what is created in a forum it has provided?
Libraries are not responsible for monitoring the legality content creators' use of intellectual property or accuracy of content created and/or shared in designated public forums. However, if the library becomes aware that a user is engaging in illegal activity, it may have a legal and/or ethical duty to intervene. In addition, the Library Bill of Rights states: "Materials should not be proscribed or removed because of partisan or doctrinal disapproval." Just so, when libraries provide their users with technology and forums to create and share their own content, the provision of these resources does not constitute an endorsement of the content or the views expressed by the creators, any more than the inclusion of content in the library's collection constitutes an endorsement of the content or the views of its creators.

What rights do users have in what they create?
All users have the right to create constitutionally protected content, so long as it does not violate the rights of others. The ALA Code of Professional Ethics states: "We respect intellectual property rights and advocate balance between the interests of information users and rights holders." Users have the right to maintain the integrity of the content they have created and to be acknowledged as the creator of their content. Libraries should provide content creators with information on how to protect their creations with copyright patent, trademark or areas of law.

What other issues should the library consider before creating makerspaces?
The library should carefully review all licenses it signs for new technology. Remember, once signed, the license controls. The library should also review existing licenses to determine if there are any impacts from the implementation of new technology or processes. The library should also review any existing partnership agreements to determine what, if any, impact new technology may have. The library should also be aware that local building codes may limit makerspace creation or uses. Disability compliance laws should be considered when installing new technology or creating makerspaces.

2016-2017 ALA CD #19.9
2017 ALA Midwinter Meeting

Guidelines to Minimize the Negative Effects of Internet Content Filters on Intellectual Freedom

Introduction

For a variety of reasons, many public libraries and schools install content filters on the Internet access they provide to their patrons and students. A library may decide to filter in response to community standards or to comply with state filtering legislation in order to receive funding. A governing authority such as a school district or local government may also require a library under its jurisdiction to filter. Libraries that receive federal E-rate funds for Internet access or in-building network enhancements must also comply with the filtering and other requirements of the Children's Internet Protection Act (CIPA).

Whatever the reasons, many libraries must deal with the well-documented negative effects of content filters on intellectual freedom. Filters often block adults and minors from access to a wide range of vital information and forms of expression that are constitutionally protected speech. CIPA requires only a narrow category of speech to be blocked: visual images that are obscene, child pornography, or visual images that are deemed "harmful to minors" under the law. Filtering technology is not sophisticated enough to make such narrow distinctions, and as a result both over filtering and under filtering occurs in the attempt to block images that meet these criteria.

Filters also threaten the privacy of users by monitoring and logging Internet activity. As more websites move to HTTPS to secure communications from eavesdropping, this presents a challenge for filters that employ content inspection techniques. Some filters now include the ability to decrypt HTTPS protocols and can thereby monitor and log user activities on secure websites. Implementation of these capabilities is not required under legislation like CIPA, nor is it consistent with the mission and values of libraries.

These guidelines are issued to provide public and school libraries with information about how to select, configure, manage, and assess content filters to minimize the negative effects on free inquiry and the privacy of library users.

Selection

Library staff, who have an ethical obligation to protect intellectual freedom, and information technology (IT) staff, who typically must install and support the product, should work collaboratively to select filtering software.

The filter selection team should consider standard criteria for purchasing any technology product or service including features, performance, ease of administration, vendor support, cost, user privacy, etc. To minimize the negative effects on intellectual freedom, the following additional

criteria should be considered when selecting a filter:

- Ability to select narrow and specific categories of content to be blocked.
- The technologies and procedures used by the vendor to categorize content.
- Ability to permanently unblock content that is incorrectly blocked.
- Ability to notify users that content is being blocked and their options, if any, for accessing the content.
- Options to easily disable the filter upon request by library staff or directly by the users.
- Ability to run reports or analytics on what is being blocked and how frequently it is blocked.

Configuration

Deciding what categories of content to filter is a law and policy decision that should be made by library and school administration and ultimately approved by their respective boards. Filter settings should not be selected solely by IT staff who likely do not have a background in the importance of intellectual freedom in libraries.

Filters often come pre-configured with many categories and types of content blocked by default. These settings should be carefully reviewed by library staff, school administrators, and educators. Only the minimal number of categories (e.g. only illegal categories of sexually explicit images, if the concern is CIPA compliance) should be blocked. Ideally a technology team (consisting of library staff, IT staff, administrators, educators, etc.) will test filter configurations by running sample searches before implementation to ensure that the chosen settings over-block and under-block as little as possible.

Avoid blocking content based on viewpoint or because the topic is controversial. Avoid blocking entire types of content (e.g. videos or social media) or protocols (i.e. music streaming). Some libraries may restrict these services not because of the nature of their content but because of the bandwidth they consume. However, bandwidth concerns can be managed without blocking protected speech by using other technologies and techniques that focus on the amount of network activity, rather than the type of content.

Limitations in filtering technology cause over filtering, a situation that occurs when content is blocked because it is incorrectly categorized. Schools and libraries should establish procedures that allow adults and minors to request content which is incorrectly categorized to be unblocked in a timely manner. Schools and libraries should also establish procedures to notify users about what is being filtered and what their options are to access incorrectly blocked content.

Many filters provide the ability to decrypt secure (HTTPS) transactions using a so-called "man-in-the-middle" method. This allows the filter to scan the content of web pages and URLs that would normally be secure. Without decryption, a filter can only block an entire HTTPS domain (e.g., ala.org), and it is unable to block individual web pages or sections of a website. The effects of decryption on the privacy of patrons can be profound if they use the library for web activities that require secure communications. For example, the security of usernames,

passwords, and sensitive personal information, including commercial, educational, financial, legal, and medical information may be compromised. Because of this, decryption should not be enabled on library computers.

By default, most filters and routers generate logs of user activity data. Library staff have an ethical and often a legal obligation to protect the privacy of this information and thus access to these logs should be restricted to authorized staff. The library should configure the device to log the minimum amount of data and develop procedures to regularly delete the logfiles.

Management

The ability to easily disable filters is crucial to mitigating their negative effects on free inquiry. The Supreme Court affirmed in its decision to uphold CIPA that adults and minors 17 or older have the right to have content unblocked or the filter disabled for research or any lawful purpose. Public and school libraries need to establish a set of procedures that allow the disabling of filters for adults and minors 17 and older quickly and easily with as little staff intervention as possible. Libraries of all types should be prepared to unblock incorrectly categorized or incorrectly blocked websites for users of all ages.

Here are some possible disabling scenarios to accommodate libraries of different sizes and technical capabilities.

- A library could make some computers available with a browser extension that allows the user to disable the filter by enabling a web proxy.[1] The library would need to have procedures in place to make sure only adults and minors 17 and older used the computers with the proxy extension.

- A library could provide staff with the ability to disable the filter at the request of an adult. If the filter does not support disabling by staff on-the-fly, the computers could be configured with a second account with unfiltered access that requires staff login. The disadvantage of this scenario is that making users ask library staff for unfiltered access presents a barrier that may have a chilling effect on such requests.

- A library with computer sign in software that includes user authentication could allow adults and minors 17 and older to choose their own filtering level, e.g. none, minimal or strict. If the sign in software does not support the ability of adult users to select their filtering level when logging in, the browser could be configured with an extension that allows the user to quickly and easily disable the filter by using a web proxy.

[1] A web proxy is a service that makes requests on behalf of a client browser to websites. Web proxies are often used to avoid content filtering and censorship. There are a number of browser extensions that allow users to enable a pre-defined proxy. A library could run their own proxy using free software like Squid or point to one of the many public proxies. Note that making some computers available that are unfiltered would not be CIPA compliant because of specific language in the legislation that mandates that filters must be installed on all computers.

- A library or school could set up procedures to allow users to request that specific web pages or websites become unblocked by library staff either temporarily for a specific activity (e.g. student assignment) or permanently. The procedures to permanently unblock a resource should include a request form that allows the user to explain why the resource should be unblocked, a review process by library staff or educators, and a way to notify the requester about the outcome of the review.

In addition if CIPA compliance is the concern, filters only have to be applied to devices provided by the library for use in the library or school. User-owned devices connecting to a library's wireless or wired network do not need to be filtered. Laptops and other devices checked out for use outside the library or school do not need to be filtered.

Assessment

All types of libraries should establish procedures to continually assess the impact of the filter on library users. The assessment should include:

- Tests by library staff on common research topics to determine extent of over filtering and under filtering.
- Regular reports on what is being blocked, recategorizations, disabling requests, etc.
- Survey of library and classroom users on the effect of the filter on their Internet activities.

The results of the assessment should be used to make continual improvements to the filter (i.e. to reduce the negative impacts on free inquiry and privacy). These improvements may involve changes to the filtering software's configuration, changes to library and school procedures, or the selection of different filtering software.

Additional Resources

Bandwidth Management (TechSoup for Libraries)

Children's Internet Protection Act (CIPA) Guidance for Libraries (Universal Service Administrative Company, July 2016)

Fencing Out Knowledge: Impacts of the Children's Internet Protection Act 10 Years Later (American Library Association, Office of Information Technology Policy OITP & Office for Intellectual Freedom Policy Brief No. 5, June 2014)

Filtering and the First Amendment (American Libraries, April 2013)

How to: Circumvent Online Censorship (Surveillance Self-Defense, Electronic Frontier Foundation)

Internet Filtering: An Interpretation of the Library Bill of Rights (American Library Association)

Issue Brief: The Time has Come to Move to HTTPS! (Center for Democracy & Technology, October 2016)

Libraries and the Internet Toolkit: Legal Issues: CIPA and Filtering (American Library Association)

SSL Filtering Whitepaper (Smoothwall)

The Man in the Middle: E-rate, Filtering and CyberSecurity (Knowledge Quest Blog Post by James LaRue: Journal of the American Association of School Librarians, September 28th 2016)

2016-2017 ALA CD 19.10
2017 ALA Midwinter Meeting

On Tuesday, January 24, 2017, the ALA Council adopted this resolution as amended.

RESOLUTION ON ACCESS TO ACCURATE INFORMATION

Whereas the American Library Association recognizes the contribution of librarianship in informing and educating the general public on critical problems facing society (Policy, A.1.1);

Whereas the mission of ALA is to provide leadership for the development, promotion, and improvement of library and information services and the profession of librarianship in order to enhance learning and ensure access to information for all (Policy A.1.2);

Whereas ALA has as one of its officially stated goals that it is the leading advocate for the public's right to a free and open information society (Policy A.1.3);

Whereas ALA opposes any use of governmental power to suppress the free and open exchange of knowledge and information (Policy B.8.5.1);

Whereas in 2005 ALA adopted a Resolution on Disinformation, Media Manipulation and the Destruction of Public Information (2004-2005 ALA CD #64);

Whereas inaccurate information, distortions of truth, deliberate deceptions, excessive limitations on access and the removal or destruction of information in the public domain are anathema to the ethics of librarianship and to the functioning of a healthy democracy;

Whereas some governments, organizations, and individuals use disinformation in pursuit of political or economic advantage to thwart the development of an informed citizenry;

Whereas the exponential growth in the use of disinformation and media manipulation constitutes a critical problem facing our society and includes:

- the distribution of fake news via websites, social media, and traditional media under the guise of independent journalism;
- the increased potency of disinformation due to the confirmation bias effect of personalized newsfeeds, social media sharing, and web search algorithms (i.e. the filter bubble);
- propaganda campaigns and cyberwarfare operations conducted by governments and non-state actors to influence or disrupt the domestic affairs of adversaries;
- the use of paid political partisans as commentators and analysts on news networks and publications; the rise of branded content that are advertisements masquerading under the guise of legitimate reporting in many publications;
- the suppression or removal of scientific studies and data that disagree with possible policy positions, for example, the human effects on climate change;

RESOLUTION ON ACCESS TO ACCURATE INFORMATION/2

- the removal of public information from U.S. depository libraries and the libraries of government agencies;
- the unreasonable delay or denial of public records and Freedom of Information Act (FOIA) requests and heightened assaults on constitutional rights under the guise of national security;
- attacks on the reputation of news organizations and intimidation of journalists; and

Whereas freedom of the press and freedom of speech is protected by the First Amendment of the United States Constitution and affirmed by the United Nations' Universal Declaration of Human Rights;

Whereas access to accurate information, not censorship, is the best way to counter disinformation and media manipulation; now, therefore, be it

Resolved, the American Library Association, on behalf of its members:

1. reaffirms the resolution on Disinformation, Media Manipulation and the Destruction of Public Information approved in 2005 (2005 ALA CD #64).

2. opposes the use of disinformation, media manipulation, and other tactics that undermine access to accurate information;

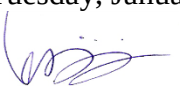
3. encourages its members to help raise public consciousness regarding the many ways in which disinformation and media manipulation are used to mislead the public;

4. urges librarians and library workers to actively seek and provide sources of accurate information that counter disinformation;

5. supports the critical role of librarians and library workers in all types of libraries in teaching information literacy skills that enable users to locate information and evaluate its accuracy;

6. will pursue partnerships with news organizations, journalism institutions, and other allies to promote access to accurate information and defend the role of journalists and the free press in American society.

Adopted by the Council of the American Library Association
Tuesday, January 24, 2017, in Atlanta, Georgia



Keith Michael Fiels
Executive Director and Secretary of the ALA Council