2 $ / & ' ±
$ / $ $ Q Q & X R D Q O H U H Q F H

TO: ALA Council

DATE: June 3, 2022

RE: (select one)
ACTION REQUESTED
INFORMATION
X REPORT

ACTION REQUESTED: [illegible]

Rhonda Evans and members of the subgroup have also organized a program for ALA Annual that will provide information to aid in understanding of what Critical Race Theory actually is and how the concept is being adopted by different advocacy groups as a means to ban books, materials, and programs that address the history of systemic racism in America. The program will also discuss the current ongoing challenges and legislation and how library workers can respond to these threats to intellectual freedom.

JOINT PROFESSIONAL VALUES PROGRAMMING SUBGROUP

The Joint Professional Values Programming Subgroup formed after the 2021 ALA Annual Conference ,(c)6(y,Pbg(l)-2war)3.02 -k /P <</on1aCID 0 50/MCID 4 >>B(r)3(3ups)-1(3)(v)[4(a3(ra4

UNITE AGAINST BOOK BANS

To advance the proposed course of action, member leaders and OIF and staff began to collaborate with consultants and subject-matter experts to research and launch an initiative to disrupt and defeat the ongoing, national censorship campaign and the effort to utilize law, policy, and politics locally and in the states to censor library materials.

On April 4, during National Library Week, ALA launched the Unite Against Book Bans, a national non-partisan, grassroots advocacy campaign intended to empower readers everywhere to stand together in the fight against censorship. Relying on in-depth polling that confirms that large majorities of voters and parents oppose book bans in public and school libraries and have overwhelmingly favorable opinions of public and school libraries, the campaign will amplify the voices of individuals opposed to book censorship and expand the reach of national organizations representing librarians; educators; authors; publishers, civil liberties and equality organizations in the fight against censorship.

Over 30 national partners have joined the campaign, including members of the National Associations of Librarians of Color, the American Federation of Teachers, the American Booksellers for Free Expression, the Authors' Guild, the National Book Foundation, the National Coalition Against Censorship, and several publishers, including Penguin Random Houseyvengu0uS(a

2021-2022 ALA CD#19.3
2022 ALA Annual Conference

May 12, 2022

A Community Approach to User Privacy: An Invitation to Participate

The rapid evolution of technology in the last decade prompted substantial changes across libraries as well as the vendors that serve the library community. From digital resources and online services to the software and hardware used for critical library infrastructure, libraries increasingly rely on library vendors to provide products, resources, and services to serve their users.

This increased reliance on third parties has also introduced and perpetuated legitimate concerns about surveillance of user identities and activities, which have at times been exacerbated by conditions including:

1.

- As a library worker, how can I identify privacy red flags and make informed licensing decisions? How can I add my voice and position to this discourse?
- As a service or content provider, what are the most critical priorities of my community? How can I learn where improvements are desired, without opening the door to unconstructive, public critique?

…segued into questions that require all our input, such as *how might we create an open, shared community of practice that fosters a mindset of continual improvement around library user privacy?*

This last question is rooted in the current reality that as the use of third-party technology products and services continues (and even increases more over time), concerns about surveillance and user privacy will persist. It also acknowledges that data can be valuable, when anonymized and in the aggregate - for decision making for libraries, and product improvement for vendors - but that responsible data practices are important to agree upon.

At ALA Annual 2022 on June 24 2022, from 10:30-11:30 AM, the Vendor Privacy Resolution Working Group plans to kick off its transition into a community of practice. Motivations for growing to a community of practice include providing a forum where past and existing efforts can be socialized, and to foster a community-wide culture of iterative improvement.

Importantly, these goals are dependent upon stakeholders across the community getting involved - service and content providers, in addition to libraries. Involvement could include attendance at the initial kick-off but also engagement with ongoing work and discussions.

Pragmatically, a shared community of practice is an opportunity to address concerns specific to each of our roles as well as those that are shared.

- As a library worker, I need to be a good steward of institutional resources. This includes minimizing the risks our users take when using electronic resources we license. I need to advocate for their right to pursue their own intellectual paths.
- As a service provider to libraries, I need to clearly understand the community's expectations around privacy practices and policies to ensure I’m investing in the right improvements, and balance that work against my organization’s existing objectives and initiatives. I need to iterate over time, and want to be more transparent about timelines, limitations, and my need for more feedback from my community.

To help shape and grow this initiative, please join us at our first convening at the ALA Annual Convention in Washington, D.C. this June. We will also be launching an online space for discussion and announc Jaan oulb.6(n)1cn4a4.

7. Aggregation: Aggregate personal data in reports to the greatest extent possible. Periodically review reports to check that they are not revealing personal data.
8. Borrowing History: Disable the borrowing history function by default. In other words, set the LMS to remove transactional data between users and the materials they borrow or access. The data should be removed when it is no longer needed for library operations. For example, a user borrows an item. The library keeps that record until the user returns the item. That borrowing history can then be removed.
    - Allow users the ability to opt in to personalization features. Examples include keeping their checkout history or a list of favorite titles.
    - Allow users to later opt out of features if they change their mind. Delete the data previously retained for these features when users opt out.
9. Resetting Passwords and PINs: Develop procedures for when staff assist users in creating and resetting their passwords, including:
    - Staff can show users how to use the password or Personal Identification Number (PIN). However, staff should not know the new password or PIN.
    - Users, not staff, should set their password and PIN.
    - Do not announce the password in a public space, such as the circulation or help desk.
    - Encourage users not to share passwords with others, including library staff.
    - Do not send the password via unencrypted email or chat.
10. Law Enforcement Requests: Develop procedures for library staff on how to handle law enforcement and government requests for user records. Refer to the ALA Laws & Law Enforcement Inquiries for suggested guidelines. These resources can help develop the policies and procedures.

PRIORITY 2 ACTIONS

1. Notifications: Configure library notifications to send a minimal amount of personal data. Examples include notifications for holds and overdues.
2. Third Parties: Limit and audit the collection, use, storage, retention, and sharing of personal data from the LMS by third parties, such as:
    - Departments and offices in the larger organization
    - Vendors
    - Third party integrations and applications, such as Application Program Interfaces (APIs) and data analytics products
3. Data Backups: Encrypt data backups to prevent unauthorized access to personal data.
4. Security Updates: Keep LMS applications and underlying server software up to date to mitigate the impact of security vulnerabilities:
    - Install security patches and updates to local servers, desktop clients, and other locally hosted LMS applications.

- Coordinate security patches and updates with third-party hosting any cloud LMS applications and systems.

5. Laws: Check vendor licenses for compliance to relevant library privacy and data privacy regulations, such as:
   - European Union General Data Protection Regulation (GDPR)
   - California Consumer Privacy Act (CCPA)
   - Family Educational Rights & Privacy Act (FERPA)
   - Children's Online Privacy Protection Act (COPPA)
   - Relevant state library privacy regulations

PRIORITY 3 ACTIONS

1. Password Encryption: Encrypt all LMS passwords in storage and in transit using current encryption best practices and standards.
2. Encrypting Traffic: Encrypt all traffic between the LMS and any application connections. For example, use a Virtual Private Network (VPN) to encrypt the connection between a checkout station at a branch library to the LMS server at the main library.
3. Security Audits: Conduct regular audits of the network and LMS servers. Audits help verify that necessary security measures are in place to prevent unauthorized access. Refer to the Privacy Audits Field Guide for developing policies and procedures.
4. Data Breaches: Create procedures to respond to data breaches and mitigate their impact on users.

Approved January 21, 2017 by the Intellectual Freedom Committee; revised January 26, 2020 and April 2022.