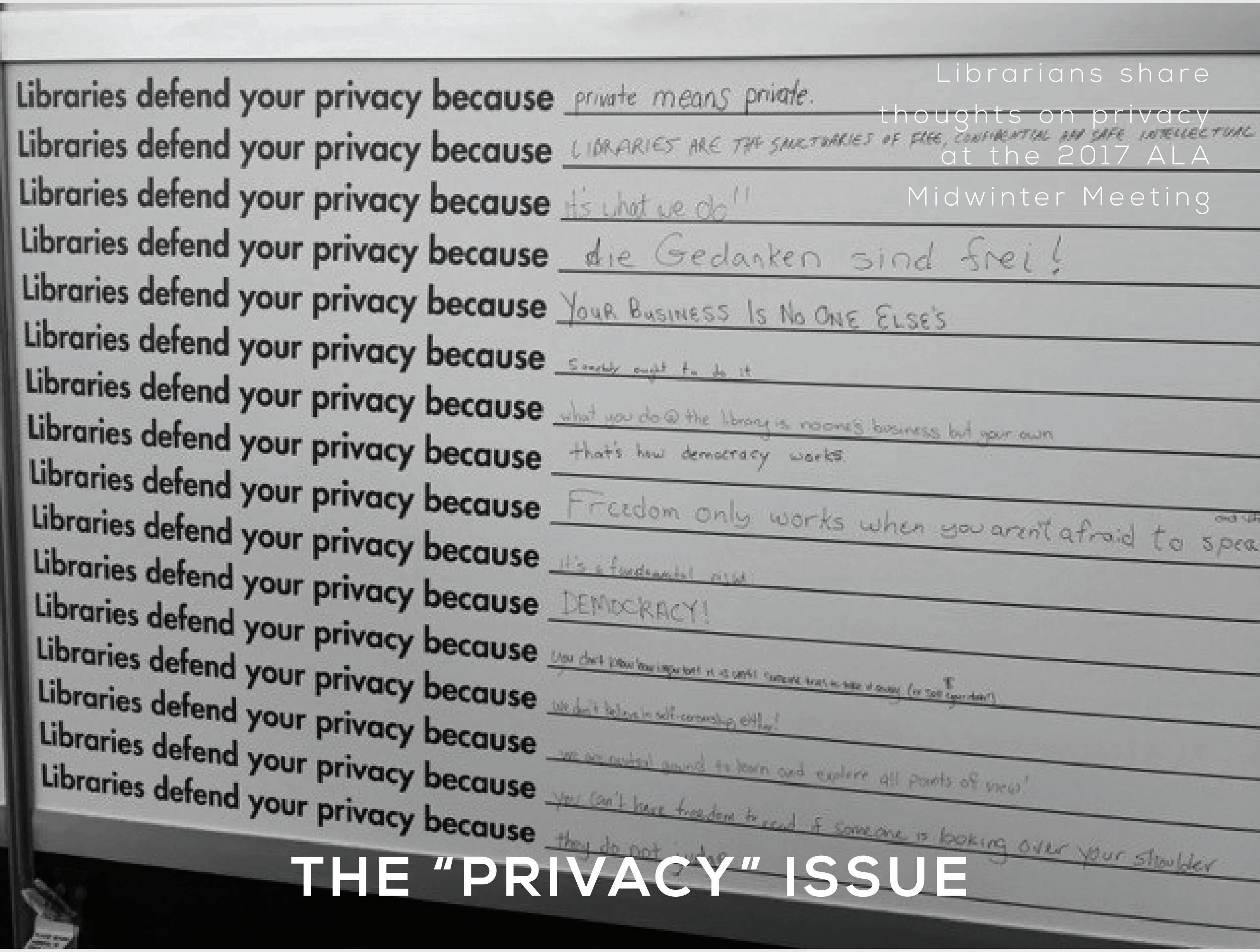
JOURNAL OF
INTELLECTUAL FREEDOM & PRIVACY
Office for Intellectual Freedom, an Office of the American Library Association


Libraries defend your privacy because private means private.
Libraries defend your privacy because LIBRARIES ARE THE SANCTUARIES OF FREE, CONFIDENTIAL AND SAFE INTELLECTUAL
Libraries defend your privacy because it's what we do!!
Libraries defend your privacy because die Gedanken sind frei!
Libraries defend your privacy because YOUR BUSINESS IS NO ONE ELSE'S
Libraries defend your privacy because Somebody ought to do it
Libraries defend your privacy because what you do @ the library is noone's business but your own
Libraries defend your privacy because that's how democracy works.
Libraries defend your privacy because Freedom only works when you aren't afraid to spea
Libraries defend your privacy because it's a fundamental right
Libraries defend your privacy because DEMOCRACY!
Libraries defend your privacy because You don't know how important it is until someone tries to take it away (or sell your data!)
Libraries defend your privacy because We don't believe in self-censorship either!
Libraries defend your privacy because we are neutral ground to learn and explore all points of view!
Libraries defend your privacy because you can't have freedom to read if someone is looking over your shoulder
Libraries defend your privacy because they do not judge

Librarians share thoughts on privacy at the 2017 ALA Midwinter Meeting

THE "PRIVACY" ISSUE

INSIDE
SPRING 2017
VOL. 2 _ NO. 1
ISSN 2474-7459

CONTENTS _ SPRING 2017

EDITORIAL

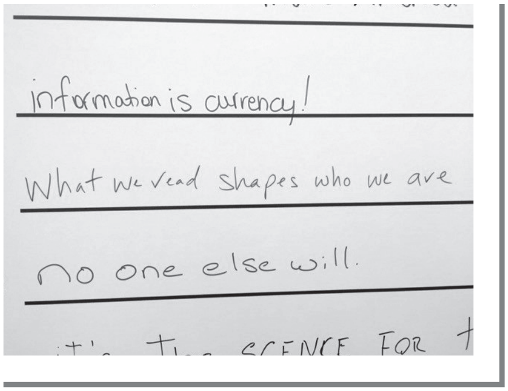
COMMENTARIES

FEATURES

REVIEW

> "PRIVACY IS ESSENTIAL TO THE EXERCISE OF FREE SPEECH, FREE THOUGHT, AND FREE ASSOCIATION. . . . THE POSSIBILITY OF SURVEILLANCE, WHETHER DIRECT OR THROUGH ACCESS TO RECORDS OF SPEECH, RESEARCH AND EXPLORATION, UNDERMINES A DEMOCRATIC SOCIETY.
>
> Privacy: An Interpretation of the Library Bill of Rights

SPRING 2017 _ ABOUT THE COVER



_ Many librarians and information professionals have struggled since waking up November 9, 2016, and realizing that Donald Trump would be the 46th President of the United States of America. Concerns quickly arose about how the Trump administration would value privacy, intellectual freedom, information literacy, and other core aspects of the librarian ethic.

It came as a shock for many when, soon after the election, the American Library Association issued a release indicating the association's willingness to "work with President-elect Trump, his transition team, incoming administration and members of Congress to bring more economic opportunity to all Americans and advance other goals we have in common." This was followed by another release (apparently mistakenly posted in draft form) describing how libraries can work to support various policy priorities of the new administration.

For many librarians, there was little common ground to be found between their professional values and the rhetoric that marked Trump's campaign. After considerable backlash, the ALA retracted their initial statement and affirmed its commitment to supporting efforts to abolish intolerance and to promote cultural understanding and inclusiveness.

These events colored much of ALA Midwinter 2018, held a few months later in Atlanta. In response to membership's concerns about the ALA's post-election stance regarding the Trump administration, the ALA Executive Board convened a town hall meeting on "Library Advocacy and Core Values in Uncertain Times." The ensuing discussion focused on issues of power, resistance, and advocacy.

Upon leaving the town hall, I stumbled upon the white boards depicted on the cover of this special issue. Prominently displayed in the registration area, Midwinter attendees were encouraged to share why they feel it is essential for libraries to play an active role in defending privacy.

Reading these diverse expressions of how libraries fight to protect privacy served as a sober reminder of the critical role librarians play in preserving American values in the face of adversity. Library advocacy has never been more important.

Journal of Intellectual Freedom and Privacy (ISSN 2474-7459)
vol. 2, no. 1 _ Spring 2017

Editor
Michael Zimmer, University of Wisconsin-Milwaukee

News Editor
Henry Reichman, California State University,
East Bay, Oakland, CA

Associate Editor
Shannon Oltman, University of Kentucky, Lexington, KY

Production Editor
Martin Garnar, University of Colorado, Colorado Springs, CO

Editorial Board
John T. F. Burgess, University of Alabama, Tuscaloosa, AL

Roseanne Cordell, Northern Illinois University, DeKalb, IL

Mack Freeman, West Georgia Regional Library, Carrollton, GA

Martin Garnar, University of Colorado, Colorado Springs, CO

Clem Guthro California State University, Fullerton, CA

Emily Knox, University of Illinois at Urbana-Champaign, IL

Shannon Oltmann, University of Kentucky, Lexington, KY

Michael Wright, Dubuque County Library, Asbury, IA

Publisher
James LaRue, Director, Office for Intellectual Freedom

Managing Editor
Deborah Caldwell-Stone, Deputy Director,
Office for Intellectual Freedom

Production
ALA Production Services: Chris Keech, Tim Clifford,
Lauren Ehle, and Hannah Gribetz

Journal of Intellectual Freedom and Privacy is published quarterly (Spring, Summer, Fall, Winter) by the Office for Intellectual Freedom, an office of the American Library Association, 50 E Huron St., Chicago, IL 60611.

Introduction: The "Privacy" Special Issue of the *Journal of Intellectual Freedom & Privacy*

Michael Zimmer (zimmerm@uwm.edu), Editor, *Journal of Intellectual Freedom & Privacy*

As editor of the *Journal of Intellectual Freedom & Privacy*, I'm excited to present the journal's first special-themed issue on **Privacy**.

Within libraries, a patron's intellectual activities are protected by decades of established norms and practices intended to preserve patron privacy and confidentiality, most stemming from the American Library Association's Library Bill of Rights and related interpretations. As a matter of professional ethics, most librarians protect patron privacy by engaging in limited tracking of user activities, instituting short-term data retention policies, and generally enabling the anonymous browsing of materials. These are the existing privacy norms within the library context, and the cornerstone of what makes up the "librarian ethic."

However, these norms are being increasingly challenged from numerous fronts: law enforcement and government agencies continuously pressure libraries to turn over data on patron activities; Library 2.0 and related cloud-based tools and services promise to improve the delivery of library services and enhance patron activities, yet require the tracking, collecting, and retaining of data about patron activities; and given the dominance of social media—where individuals increasingly share personal information on platforms with porous and shifting boundaries—librarians and other information professions are confronted with possible shifts in the social norms about privacy.

With valuable insights from library practitioners, information technology professionals, compliance officers, and academic researchers, the work gathered in this special issue engages head on with this growing challenge to long-standing privacy norms within libraries.

The special issue includes two feature articles exploring the privacy implications of the growing practice of leveraging patron data to enhance library services. In **"Balancing Privacy and Strategic Planning Needs: A Case Study in De-Identification of Patron Data,"** Becky Yoose, library applications and systems manager at Seattle Public Library, discusses how libraries increasingly seek information about specific patron demographic groups to provide effective targeted programs and services while recognizing that such collection and use of patron data might jeopardize patron privacy. Using the recent planning and implementation of a data warehouse and de-identification plan at Seattle Public Library as an example, Yoose details how libraries can both be "data-informed" and remain protectors of patron privacy through the use of de-identified patron data within their data warehouses.

In **"Privacy Policies and Practices with Cloud-Based Services in Public Libraries: An Exploratory Case of BiblioCommons,"** Katie Chamberlain Kritikos and I, from the University of Wisconsin-Milwaukee Center for Information Policy Research, report on the results of a pilot research study investigating how libraries are implementing third-party cloud computing services, how these implementations might affect patron privacy, and how libraries are responding to these concerns. After examining policies and records from thirty-four public libraries that use the cloud-based BiblioCommons discovery layer, we provide recommendations for tailoring privacy policies, practices, and patron communication for other libraries seeking to leverage cloud-based patron services.

Complementing these two feature articles, this special issue includes four short commentaries that provide helpful insights on various privacy-related issues for librarians and information professionals. First, in **"The Path to Creating a New Privacy Policy: NYPL's Story,"** Bill Marden, director of data privacy and compliance at New York Public Library, gives us an insider's view of the process—and the philosophy—the drove NYPL's recent update to its patron privacy policy. Second, Jessica Garner, a librarian at Georgia Southern University, provides additional advice for libraries seeking to communicate better with patrons—as well as the public—regarding the importance of privacy in her commentary, **"We Can't All Be Rock Stars: Reaching a Mass Audience with the Message of Library Privacy."** Next, Mike Robinson from the Consortium Library at University of Alaska Anchorage, shares pragmatic guidance in **"How to Get Free HTTPS Certificates from Let's Encrypt,"** detailing his experiences moving his library's servers and services to Let's Encrypt to provide more security and privacy for their systems and patrons. The fourth commentary, **"Libraries and the Right to be Forgotten: A Conflict in the Making?,"** by Eli Edwards, summarizes the challenges libraries will inevitably face in the wake of recent European court rulings that suggest personal information that is irrelevant, outdated, or inaccurate should not be readily accessible to the general public.

The special issue closes with Rudy Leon's thoughtful review of the new book *Protecting Patron Privacy: A LITA Guide*, co-edited by Bobbi Newman and Bonnie Tijerina, and published through the Library Information Technology Association.

COMMENTARY

The Path to Creating a New Privacy Policy

NYPL's Story

Bill Marden (williammarden@nypl.org), Director of Data Privacy and Compliance, New York Public Library

Every library has (or should have) one. Ironically, in an institution devoted to reading and intellectual inquiry, it is probably the most seldom-read document in its collections. I am referring to library privacy policies, which have become increasingly important in an era when the broad gathering of information and data is exponentially increasing.

The New York Public Library (NYPL) has aimed to change that with its new privacy policy, publicly released in November 2016. The journey to revise the Library's privacy had begun before I arrived in November 2015 and became the first full-time director of privacy and compliance at NYPL; and, though I am not an attorney, my position is situated in the Library's legal department which, as a group, is responsible for the review, if not the actual writing, of most of the NYPL's legal policies and notices.

As with any almost institution going through a policy-writing process, we began with what we already had. In its 120-year history, NYPL has evolved its data-collection practices from the age of paper call slips to complex digital circulation systems. In the normal course of its operations, NYPL checks out books and materials to patrons (23 million per year), provides classes and programs to both adults and children, and—in the age of the internet—provides access to online information and databases that span the globe.

NYPL's board of trustees, which has a committee devoted to reviewing the Library's policies and programs, has consistently expressed the need for library operations to (a) know what information and data we were collecting from patrons; (b) know what we were doing with that information once collected (including who could access it and where); (c) articulate how patrons could opt in and out of our the data that they provide in the course of using the Library; and (d) determine how we respond to legal requests for information (such as subpoenas, warrants, etc.).

Discovery

Answering the first question—what do we collect—involved a thorough inventory of the Library's systems, databases, and paper-based information gathering. For instance, besides using our main integrated library system (ILS) to track the borrowing of materials in the branch libraries, we also use an age-old call-slip method in our four major research collections. The attempt to track the myriad data-collection methods began before I arrived and concluded shortly after I started. Finding the sources of data streams, be it analog or digital, involved speaking with every department in the Library to better understand (a) their reasons for collecting the data, (b) where they kept it and for how long, (c) if and when they shared it within or outside the Library and with whom, and (d) how they ultimately disposed of it when it was no longer needed.

These became the key elements of determining NYPL's current state and how to move forward.

Similar institutions

While the inventory was happening, we also talked to other nonprofit institutions to learn how they had developed and maintained their privacy policies. Among the models we reviewed were those from San Francisco Public Library (partly because California's library privacy statutes are among the strictest in the nation), the American Civil Liberties Union, as well as our fellow New York City library systems at Brooklyn Public Library and Queens Library. The Smithsonian Institution, another organization that recently had hired a full-time privacy officer, was also a great source of information about best practices for both privacy policies and their underlying practices.

Principles

The American Library Assocation (ALA), of course, has long been a bedrock of advocacy for library patron privacy and user rights. For our purposes, the most valuable tools were the ALA's Intellectual Freedom Committee's guidelines, including its "Privacy Toolkit," which outlines the five "Standard Privacy Principles," which are based on the Electronic Privacy Information Center's *Fair Information Practice Principles*. These five principles are

1. There must be no personal data record-keeping systems whose very existence is secret.
2. There must be a way for a person to find out what information about the person is in a record and how it is used.
3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.
4. There must be a way for a person to correct or amend a record of identifiable information about the person.
5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.

In short, these can be defined as the rights of "notice," "choice," "access," "security," and "enforcement," and were at the heart of both our internal discussions as well as the drafting of NYPL's new privacy policy

Internal discussions

During the spring and summer of 2016, we held discussions with management throughout NYPL, ensuring that we gathered input and feedback from such departments as library services, research, digital, legal, marketing/communications, IT, facilities, and security. Each group has a stake in our privacy policy to the extent that they are engaged in at least some part of the data lifecycle (i.e., collection, storage, use, transmission, etc.). Additionally, we engaged a subgroup of our board of trustees who reviewed the early stages of the drafts and gave their valuable input.

The legal department was at the center of this process, in particular our associate general counsel, who wrote each draft as well as the final document, and NYPL's general counsel, who was a key player in the shepherding of the new policy from inception through completion.

After four months of solid drafting, the new policy was ready for presentation to the NYPL board of trustees' Program and Policy (P&P) Committee. The discussion centered on such topics as how long we retain data (minimally), how we respond to subpoenas and warrants (we are creating internal procedures), how to further strengthen public awareness and education about our practices, and how patrons can opt in and out of information gathering.

The newly revised policy approved by the P&P Committee at its September 2016 meeting now provided the public with clear explanations of the following:

- what information NYPL collects from is users
- how NYPL uses that information

- how users can manage the information NYPL collects about them (including methods of opting in and out of that collection)
- when NYPL shares information with third parties

Rollout

With official approval of the policy now complete, we had the further work of ensuring that it was adequately rolled out and publicized, both internally and externally. To that end, I worked with our human resources department to create a five-minute online training video that we required all NYPL employees to view. In the video, our general counsel and I explained what changes were represented in the new privacy policy as well as how to answer potential questions from patrons. This was all accomplished in the three weeks before the "go live" date of November 30.

On the morning of November 30, 2016, we launched three simultaneous events to ensure the new policy received maximum attention:

- The new policy was uploaded to the same location as the previous policy (via a link from our homepage) and labeled with a "last updated" date of November 30, 2016.
- Visitors to our website (nypl.org) saw a large yellow banner announcing the new policy at the top of all our webpages. The banner ran for two weeks.
- Our marketing and advertising department sent a single e-mail announcing the new policy to more than 1 million patrons, donors, and those who had signed up for library events. The e-mail provided a link that gave further information about the reasons for the policy revision and what key elements to look for.

Shortly after the rollout, we used a professional translating service to create versions of the full privacy policy in Spanish, Chinese, and Russian (the three most common non-English languages spoken by New York City residents). These non-English language versions are prominently linked to from the main English-language privacy policy page on NYPL's website.

In the months and years ahead, we plan to further educate both our staff and the public on best practices for understanding and protecting privacy and information security. One key way to accomplish that is with an internal group that I created early in 2016. The NYPL Privacy Advisory Committee brings together representatives from every division of the Library to get updates on privacy initiatives and news as well as work to work on specific projects. Additionally, we expect the policy will evolve to keep pace with the ever-changing world of technology.

Come visit NYPL's new privacy policy today at https://www.nypl.org/help/about-nypl/legal-notices/privacy-policy.

We Can't All Be Rock Stars

Reaching a Mass Audience with the Message of Library Privacy

Jessica C. Garner (jgarner@georgiasouthern.edu), Interlibrary Loan Librarian, Zach S. Henderson Library, Georgia Southern University

The dust had scarcely settled on the ruins of the World Trade Center and at the Pentagon when US legislators, in what can be charitably called an overabundance of caution, passed the USA PATRIOT Act, a sweeping and often controversial series of powers designed overtly to aid security officials in detecting and thwarting any additional attacks by terrorists on American targets. Nestled in among the tangle of legal language was Section 215, immediately dubbed "the library records provision." Under Section 215, federal officials—specifically, the FBI—could request almost any document or record from a library with no need to provide probable cause and a strict prohibition against any librarian discussing such requests. Librarians, predictably, found Section 215 onerous. President George W. Bush's attorney general at the time, John Ashcroft, called the concerns of librarians "baseless hysteria" in 2003. The library community found its villain that day.

Two years later, it found heroes, too. In 2005, George Christian, a Connecticut library executive, was served with papers from the FBI "demanding that he surrender 'all subscriber information, billing information and access logs of any person' who had used one computer at one of the libraries he managed" (Z. Carpenter 2015, 14). Christian balked at the request and went to court alongside three other library officials. Collectively, the group became known as "The Connecticut Four," and their case opened the door to bombshell reporting by the *Washington Post*, which documented government use National Security Letters (NSLs) for overreach. After the FBI abandoned both its request for information and the associated gag order, the quartet of folk heroes earned the admiration of the library community (15). But the events took place before the first iPhone was ever produced, before Facebook had expanded beyond college campuses, and when encountering something viral still meant a trip to the doctor. Outside of the library bubble, the tale of the Connecticut Four's dedication to patron privacy is still relatively unknown.

This is all a very winding road to an extremely important question: since the greatest heroes of the modern library privacy movement exist almost entirely in obscurity, do libraries need a high-profile advocate?

Section 215 of the USA PATRIOT Act quietly died on the table in May of 2015 when reauthorization of the statute failed (Kelly 2015). Before librarians could properly sit back and enjoy being out from under the shadow of the legislation, the 2016 elections flipped politics on its head and reacquainted the everyday American vernacular with terms like "hacking" and "authoritarianism" as well as introducing new doozies like "fake news" and "alternative facts." To be fair, at the time of this writing (March 2017), the policies of the Trump administration are still nebulous, but the new president put forward Mike Pompeo as his pick to lead the CIA, and Pompeo was confirmed 66–32 late in January. Pompeo's ascension to the CIA seat has rubbed civil liberties groups the wrong way in part because of Pompeo's continued "support for the National Security Agency's now-defunct bulk communications metadata collection and other surveillance programs" (Landay 2016). Librarians had likely already latched on to particular campaign rhetoric from the president focused on promises of domestic security and "law and order." Even before Republicans consolidated power by winning both houses of Congress and the White House, the Connecticut Four penned an op-ed for the *Hartford Courant* warning against moves in Congress to again empower federal officials with the authority to request information and mute any discussion of those requests. "The senators could try again at any time," the quartet warned (Chase et al. 2016).

With all due respect to the *Courant* and great admiration for the Connecticut Four, the most well-known voices in the public sphere are not librarians. Celebrities of all stripes—actors, authors, internet personalities, whatever the Kardashians are—bring a virtual army with them to nearly anything they call attention to, from the plight of refugees to marijuana legalization. Unfortunately, a basic Google search of "celebrity library advocates" turns up nothing especially noteworthy or viral-ready. Emma Watson, who plays noted bibliophile Belle in the upcoming Disney live-action adaptation of *Beauty and the Beast*, has already taken up a full dossier of causes. Author Neil Gaiman is famous, but mostly to people who already have a strong relationship with books and libraries.

Pining for a celebrity advocate to speak up at the next awards show on behalf of libraries may be a bit reductive; a naive belief in the power of the celebrity megaphone to push an important issue to the forefront of public discussion. But if privacy issues swell to the forefront as they did beginning in 2001, some expansive and memorable plea to American citizens is in order. Initiatives like NISO (National Informational Standards Organization) are already helping guide the Library Freedom Project (T. Carpenter 2016, 29), but there is not a public face or coordinated, singular campaign to remind the American public about the value and sanctity of libraries. In fact, both NISO and the Library Freedom Project are hardly known outside library circles despite their work to codify and enact best practices for all libraries to protect patron privacy.

It is hardly the place of this author to pretend to the expertise necessary to design and implement a nationwide campaign to raise awareness of the library privacy issue in the vein of the American Library Association's successful "Read" poster campaign. But I do have some idea what such an effort would look like. It would make the diminishing number of private spaces an issue average Americans would relate to without being alarmist. It would stress the long history of libraries as spaces where intellectual freedom was defended. To be a successful public relations campaign, it would juxtapose unpopular ideas with popular breakthroughs—perhaps a student studying volatile combustible materials to develop a new form of jet fuel. And, in my opinion, the campaign very well might have one famous face and voice to serve as the campaign's "guide."

Perhaps such a campaign isn't needed at all. With some luck, the next iteration of the Connecticut Four will thrive in the exploding Information Age. But it is worth courting the idea that the commitment to the privacy of our patrons should be brought to the attention of the widest audience possible. It is worth considering how a voice with a virtual bullhorn might draw a spotlight to the cause of patron privacy. It shouldn't take a new law like Section 215 or an unartful comment by Pompeo or Trump to give libraries and their supporters a rallying point.

If there's a way to call in the "big guns," sooner might be a better time than later.

References

Carpenter, Todd. 2016. "Respecting Privacy: Consensus Is Reached on NISO Privacy Principles." *Computers in Libraries* 36, no. 5: 26-29.

Carpenter, Zoe. 2015. "Librarians vs. the NSA." *Nation* 300, no. 21: 12-15.

Chase, Peter, Barbara Bailey, Jan Nocek, and George Christian. 2016. "Librarians Stand Again Against FBI Overreach." *Hartford Courant* (Hartford, CT), September 28, 2016.

Kelly, Erin. 2015. "Patriot Act Provisions Expire as Senate Compromise Comes Late." *USA Today*. Last modified June 1. http://www.usatoday.com/story/news/nation/2015/05/31/nsa-cia-data-collection/28259481/.

Landay, Jonathan. 2016. "Trump's CIA Pick Supports Domestic Surveillance, Opposes Iran Deal." *Rueters*. Last modified November 18. http://www.reuters.com/article/us-usa-trump-pompeo-newsmaker-idUSKBN13D2HM.

How to Get Free HTTPS Certificates from Let's Encrypt

Mike Robinson (mcrobinson@limxr.org), Chair of the ALA's Intellectual Freedom Privacy Subcommittee and Head of Systems at the Consortium Library at the University of Alaska Anchorage

There has been a push by many organizations in recent years to move all websites from nonsecure HTTP to the more secure HTTPS protocol. HTTP is vulnerable to eavesdropping and content hijacking. HTTPS helps protect against these problems by establishing an encrypted connection between your browser and the website. There are a number of initiatives promoting the move to HTTPS:

- Federal government websites are now required to be HTTPS.
- Google now gives a ranking boost to HTTPS sites in search results.
- Firefox and Chrome now warn users that HTTP sites are insecure.
- The Freedom of the Press Foundation started the Secure the News project to track and promote the adoption of HTTPS by major news sites.
- The Electronic Frontier Foundation launched an Encrypting the Web campaign.
- The Library Digital Privacy Pledge encourages libraries and their content providers to adopt HTTPS.

Perhaps one of the most successful initiatives has been Let's Encrypt, a new certificate authority that provides both free HTTPS certificates and tools to easily install them. Let's Encrypt has a number of sponsors including the Electronic Frontier Foundation, Mozilla, Chrome, Facebook, and the American Library Association (ALA). That's right, ALA is a sponsor of this important initiative to help libraries move to HTTPS. The free tools and certificates from Let's Encrypt became available in a beta version November 2015 and moved out of beta status in April 2016. Adoption has been rapid (Aas 2017). In January 2016, they supported 240,000 active certificates, which grew to more than 28 million by January 2017, making it one of the largest certificate authorities in the world. Approximately half of the web is now on HTTPS.

Most libraries have never had HTTPS (Breeding 2016), and its time for that to change. Let's Encrypt can be used to install HTTPS on a variety of library websites and services. I have written a series of blog posts that provide step-by-step recipes of how we moved our library servers to HTTPS (Robinson 2016) last year using Let's Encrypt, including the following server types:

- Apache Web Server on CentOS 6
- IIS Web Server on Windows 2008
- Standalone EZproxy Server on CentOS 6
- Library OPAC Server—SirsiDynix Enterprise on Tomcat CentOS 5
- API Server—SirsiDynix Web Services on Tomcat CentOS 6

These recipes are for servers under the library's direct control. It was simple and straightforward for the system administrator to install the Let's Encrypt client and obtain the certificate on a variety of servers with one exception—it was tricky to install the Let's Encrypt client on the server running the aging CentOS 5 operating system because of out-of-date dependencies. Another possible issue is libraries that use EZproxy to access content from a large number of HTTPS websites. The recommended way to do this is through a wildcard HTTPS certificate, which Let's Encrypt does not yet support. Let's Encrypt does support up to one hundred domain names on a single certificate, so it can work fine for libraries with a moderate number of HTTPS resources to proxy.

Good documentation and community support exists for those that want to integrate Let's Encrypt into their products and services. More than a hundred web hosting platforms (Let's Encrypt 2015) have integrated Let's Encrypt so that certificates can be installed by customers from their control panel with just the click of a button. Vendors and content providers in the library world should begin integrating support for Let's Encrypt into their products and services.

References

Aas, Josh. 2017. "Let's Encrypt 2016 In Review." *Let's Encrypt Blog*, January 6. https://letsencrypt.org/2017/01/06/le-2016-in-review.html.

Breeding, Marshall. 2016. "Protecting Patron Privacy: Libraries are failing to use HTTPS." *American Libraries Magazine,* May 31. https://americanlibrariesmagazine.org/2016/05/31/protecting-patron-privacy/.

Let's Encrypt. 2015. "Web Hosting who support Lets Encrypt." December. https://community.letsencrypt.org/t/web-hosting-who-support-lets-encrypt/6920.

Robinson, Mike. 2016. "Let's Encrypt Cookbook for Library Servers." *Mike Robinson: UAA/APU Consortium Library* (blog), June 13. https://consortiumlibrary.org/blogs/mcrobinson/blog/2016/06/13/lets-encrypt-cookbook/.

COMMENTARY

Libraries and the Right to be Forgotten

A Conflict in the Making?

Eli Edwards (misseli@mac.com)

The right to be forgotten (RTBF), an concept in European privacy law, is based on the notion that personal information that is irrelevant, outdated, or inaccurate should not be readily accessible to the public. The right was codified in the European Union's 1995 Data Protection Directive (European Commission 2012).

In 2014, the Court of Justice for the European Union (CJEU) was petitioned on the question of whether the RTBF applied to digital information held by search engines. To the surprise of many, the Court ruled that search engines, even those whose data was held largely outside of Europe, were subject to the Directive. To comply, search engines that began delisting certain search results when requested by European citizens; this applies across all domains, but only to viewers within Europe (Carter 2016). This application of RTBF so far occurs only at the search-engine level—the primary content is not taken offline ("Weak Spots" 2016).

Google's process is a case-by-case staff determination of each request ("Google Transparency Report: Frequently Asked Questions" n.d.). As of mid-January 2017, Google has received 671,463 requests from European citizens to remove links, and it has evaluated for removal 1,852,776 URLs; 43.2 percent of the URLs processed were removed from search results ("Google Transparency Report: European Privacy Requests for Search Removals" n.d.). A 2016 study found that removal requests clustered around criminal and/or sexual issues (Xue et al., 2016). The study also explained a technical flaw that would allow third parties to find delisted articles and identify removal requesters. Eighty professors in Europe and the United States signed a letter requesting that Google provide more details in its transparency report of delisting requests (Goodman 2015).

In 2016, the European Parliament passed legislation replacing the 1995 Data Protection Directive, effective mid-2018. The new directive includes a right of erasure of personal data if it's "no longer necessary in relation to the purposes for which [it was] collected." There are explicit exceptions for freedom of expression and archiving for scientific or historical purposes (Regulation (EU) 2016/679 2016).

Supporters have praised the decision and implementation as reasonable restraints against the reputation harm suffered from the the persistency of online information (Rotenberg 2014). Critics worry RTBF will create "memory holes" in the historical record that impede access to knowledge and accountability of public figures (Palmer 2016). Some archives and researchers have pointed out that they already have protocols for the removal of certain information, if petitioned, and the Google case does not change those protocols (British Library 2014; Jones 2012).

Library organizations have shown concern over RTBF and long-term information access. Deborah Caldwell-Stone, deputy director of the American Library Association's Office for Intellectual Freedom, has pointed out "the possibility of losing the ability to find information and preserve the historical record" (Lynch 2016). In 2016, the International Federation of Library Associations and Institutions (IFLA) released a statement focused on balancing freedom of expression and preserving information with protecting individual privacy (IFLA 2016).

American librarians have taken on the role of privacy advocates with alacrity, especially around privacy for accessing information, on and offline. Librarians also consider access and preservation of information to be an essential duty. We must, as IFLA recommends in its statement on RTBF, continue conversations between stakeholders to support our missions to provide access to information and encourage user privacy.

References

British Library. 2014. "A Right to be Remembered." *UK Web Archive* (blog), July 21. http://britishlibrary.typepad.co.uk/webarchive/2014/07/a-right-to-be-remembered.html.

Carter, Edward L. 2016. "The Right To Be Forgotten," *Oxford Research Encyclopedia of Communication*, November. https://doi.org/10.1093/acrefore/9780190228613.013.189.

European Commission. 2012. "Factsheet on the 'Right to be Forgotten' Ruling (C-131/12)." http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf.

Goodman, Ellen P. 2015. "Open Letter to Google From 80 Internet Scholars—Release RTBF Compliance Data," medium.com, May 14. https://medium.com/@ellgood/open-letter-to-google-from-80-internet-scholars-release-rtbf-compliance-data-cbfc6d59f1bd#.49sy85wan.

"Google Transparency Report: European Privacy Requests for Search Removals." n.d. Google. Accessed January 10, 2017. https://www.google.com/transparencyreport/removals/europeprivacy/.

"Google Transparency Report: Frequently Asked Questions." n.d. Google. Accessed January 10, 2017. https://www.google.com/transparencyreport/removals/europeprivacy/faq.

International Federation of Library Associations and Institutions (IFLA). 2016. "IFLA Statement on the Right to be Forgotten." February 25. http://www.ifla.org/node/10272.

Jones, Meg Leta (Ambrose). 2012. "You are What Google Says You Are: The Right to Be Forgotten and Information Stewardship." *International Review of Information Ethics* 17 (July). Retreived from https://ssrn.com/abstract=2154353.

Lynch, George R. 2016. "Could a Right to be Forgotten Kill Online Libraries?" Bloomberg Law: Privacy & Data Security, Bloomberg BNA, October 17. https://www.bna.com/right-forgotten-online-n57982078697/.

Palmer, Aeryn. 2016. "Wikimedia Foundation Files Petition against Decision to Extend the 'Right to be Forgotten' Globally." Wikimedia Foundation, October 19. https://blog.wikimedia.org/2016/10/19/petition-right-to-be-forgotten/.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). 2016. Official Journal of the European Union. L119/1, May 4. http://eur-lex.europa.eu/eli/reg/2016/679/oj.

Rotenberg, Marc. 2014. "EU Strikes a Blow for Privacy: Opposing View. *USA Today*, May 14. http://www.usatoday.com/story/opinion/2014/05/14/european-union-google-privacy-epic-editorials-debates/9104063/.

"Weak Spots in Europe's 'Right to be Forgotten' Data Privacy Law." 2016. *Science Daily*, June 7. https://www.sciencedaily.com/releases/2016/06/160607120801.htm.

Xue, Minhui, Gabriel Magno, Evandro Cunha, Virgilio Almeida, and Keith W. Ross. 2016. "The Right to be Forgotten in the Media: A Data-Driven Study." *Proceedings on Privacy Enhancing Technologies* 4: 1–14. https://doi.org/10.1515/popets-2016-0046.

Balancing Privacy and Strategic Planning Needs

A Case Study in De-Identification of Patron Data

Becky Yoose (becky.yoose@spl.org), Library Applications and Systems Manager, Seattle Public Library

In their efforts to create and foster an evidence-based practices environment, library administrators often examine outreach efforts and collection management. Library administrators seeking to improve these areas might ask complex questions such as, "We see a gap in library use for certain age groups; for example, we see that teens and parents are active library users, but people in their twenties are not. For patrons who *are* active in their twenties, were they active users in their teens?" or, "Certain language collections see high circulation in certain branches; however, we are not sure if the patrons using those collections are traveling from other parts of the city to use those materials. Is there a way we can determine the percentage of patrons who are checking out those selected language collections outside of their home branch?"

Libraries who are looking for ways to improve outreach into their communities need information about specific patron demographic groups to provide effective targeted programs and services. Collections managers need a certain level of detail in collection data to determine if certain collections are meeting the needs of particular patron groups. Assessment and outcome-based evaluation of library programs and services cannot be effective without a specific level of detailed data. Patron data is vital for libraries to make the best use of limited resources and funding by determining what programs, services, and practices are the most effective and efficient.

The type of data needed in these analyses is also the type of data that libraries usually discard to protect the privacy of their patrons. This kind of data is considered extremely valuable by companies whose operations depend on customer data: Amazon and Facebook are two examples of businesses with various recommendation algorithms and marketing systems that are built on user behavior data. Libraries should—if not *must*—be sanctuaries from this kind of default detailed data collection, yet, because of the importance of data in evaluation and decision processes, libraries need to gain insights into their patron populations to continue to be a vital resource to their communities.

This article explores one way that libraries can be both data-informed and protectors of patron privacy with the use of a data warehouse with de-identified patron data. De-identification allows for a level of granularity that makes it possible for libraries to answer questions like the ones above, while at the same time maintaining appropriate patron privacy. After establishing a baseline understanding of library data privacy regulations, personally identifiable information, and de-identification, the article focuses on the case study of the planning and implementation of a data warehouse and de-identification plan at the Seattle Public Library (SPL). Some considerations follow for libraries investigating the options of a locally developed or vendor-hosted data warehouse solution with some more general comments about the future of data warehouses and de-identification practices in libraries at the end.

Background

Library Patron Data Privacy Regulations

Rules governing library patron data access and privacy falls within two broad areas: varying levels of special legal treatment on federal, state, and local levels and guidelines and policies provided by organizations. In the United States, the USA PATRIOT Act and, more recently, the USA Freedom Act, are the most prominent federal laws pertaining to library patron data. On the state level, each state has a different approach to defining the privacy of library patron data. The state of Washington, for example, does not have laws that explicitly protect patron data; however, state law does call out library records as an exemption from public disclosure under RCW 42.56.310. Other states have stronger patron privacy laws, including laws regarding parental access to their child's account information and when patron data can be disclosed outside of the library.[i] Finally, for libraries tied to local governments, there are additional records management and privacy regulations to follow in addition to the state and federal laws and regulations. While Seattle does not have any specific regulations regarding library patron records, for example, there are more general privacy and record management regulations by which city departments must abide.

Outside of legislation and regulations, various organizations provide guidelines and best practices regarding the privacy of patron data. The American Library Association's (ALA) Library Bill of Rights and interpretations thereof serve as one of the major sources for US libraries to reference for their approach to managing patron data (ALA 1996). In ALA's Policy concerning Confidentiality of Personally Identifiable Information about Library Users, ALA specifies that confidentiality of patron data extends to a variety of different data sets—including database use, use of library services and facilities, and information from reference/research inquiries—and that this information must be protected from unauthorized access by government agents outside of a warrant (ALA 1991). Beyond ALA, the International Federation of Library Associations (IFLA) also provides more general guidance for libraries in terms of how to approach handling patron data (IFLA 2016). IFLA recommends libraries to abstain from the collection of patron data that would compromise the privacy of said patrons, limit the data collected from patrons, and to educate both patrons and staff about how to protect their privacy, be it online or in the physical world.

Personally Identifiable Information

The National Institute of Standards and Technology (NIST) divides Personally Identifiable Information (PII) into two categories. The first category, PII-1, is information that can directly identify a person, including name, birthdate, address, and Social Security Number. The second category, PII-2, pertains to an individual's activities that can be linked back to that individual. NIST lists several examples of such information, including medical, educational, financial, and employment information (United States 2008). In the context of libraries, the second category of PII includes the intellectual pursuits of the patron, including reference interactions, search queries, and circulation history. This kind of data, in sufficient enough quantities, can be used in certain circumstances to reverse engineer an identity. A famous example of re-identification using PII-2 data is the America Online release of search data in 2006. Even though the data was edited to remove some PII, the amount of PII-2 data present in the dataset enabled researchers to identify searchers by specific search patterns and queries (Techcrunch 2006).

De-identification

Since library patron data contains both categories of PII, libraries must consider the various risks regarding what data should be stored and used for operational use, along with the additional risks of having PII stored with third party vendors. If a library wants to have some ability for longitudinal analysis with regards to library collections and services, then they need to construct a way to track unique data points without identifying unique individuals

[i] For a list of state laws regarding library record privacy, please visit http://www.ala.org/advocacy/privacyconfidentiality/privacy/stateprivacy

through PII disclosure (intentional or accidental). Anonymizing the data does not allow for this type of analysis, making it difficult to use the otherwise rich context that historical data would have provided.

Outside of anonymization, another approach to consider for long-term analysis of unique data points is de-identification. The de-identification process focuses on scrubbing particular PII data in a data set while at the same time keeping the data in a state where one can still track unique data points (Garfinkel 2015). With the removal or obfuscation of several PII-1 and PII-2 data points, one's ability to identify a particular individual in a data set is severely hampered, if not made impossible to do.

De-identification is a viable option for protecting the privacy of individuals in particular datasets that are used to track behavior or trends on an individual level. In practice, library patron data de-identification has its unique challenges and considerations. The following case study shows how the SPL approached these challenges with the construction of their data warehouse.

Case Study—The Seattle Public Library

The First Iteration: Targeted Population Market Analysis

The SPL, consisting of twenty-seven physical libraries as well as mobile library services, serves the Seattle community. The Library, as part of its efforts to better serve its community, applied and received a grant in 2013 and 2014 to conduct a marketing research project regarding patrons in the "Millennial" generational age range. The goal of the project was to increase the use of Library services and resources by Millennials over a specific time period. At this time, the only data sets available to conduct this research were from the data sources themselves, primarily from the Library's SirsiDynix Horizon integrated library system (ILS). Because the ILS has both PII-1 and PII-2, the Library was faced with the problem of needing to manipulate the data in a way that would protect patron privacy within policies and regulations but at the same time ensure that the data can provide both the insight desired to gain more traction with the targeted population as well as ways to measure the effectiveness of any actions informed by the analysis. In short, the Library needed a way to track individuals without identifying who they are to get a more granular picture of current Library usage by the target population instead of the more aggregated view that traditionally has been the default in market analysis.

In an attempt to meet the needs of the project, the Library decided to create a separate internal database with exported circulation transactions from the ILS. The transactions had most PII-1 scrubbed or manipulated in a manner to obfuscate identity; for example, the age of the patron at the time of the transaction was entered into the database instead of importing the date of birth attached to the patron record. In the end, the data from the database was used to create a persona for the marketing department to use in developing services and programs for the targeted population. Regular snapshots of circulation transactions from the ILS were imported into the database to help measure the success of the above programs. At the end of the grant-funded project, the data gleamed from this database did play a major role in meeting the goals of the project (increased library usage by the target population by 15 percent over the course of a summer) (Yoose and Halsey 2016).

The Transition to a Data Warehouse

Nevertheless, the analysis could not answer some questions regarding the type of activity being seen in the circulation transactions. The database, while storing individual circulation transactions, was not set up in a way to track circulation transactions by unique individuals. The data was mostly anonymized and the Library could not tell what percentage of the transactions came from particular patrons. For marketing, knowing the type of library usage by patrons can shape outreach and events. Does the usage indicate a core of dedicated library patrons who make extensive use of the library services and resources, or does the usage show a group of patrons who make a couple of transactions, but in greater numbers? Knowing the pattern of use on the individual level gives marketing and outreach a sense as to where to spend resources in their programs and events.

Another consideration for the Library was the ability to use the database for the market study for other projects. The data collected in the database primarily served one purpose—to track individual level circulation transactions of a certain age group. Unfortunately, this focused approach in building the database left little room for other uses of the data by other departments who, for example, might want to see circulation transactions across multiple age groups or branches. The database had a positive, real-world impact, and the desire was to find a way to bring that success into other parts of the Library.

To address the above issues and needs, the Library began work on a data warehouse, the successor to the database used in the grant-funded project above. The data warehouse would incorporate multiple sources of data in a central location, giving different departments in the Library the ability to report on the same data instead of the previous practice of performing multiple exports of raw data from the data sources themselves, which opens up a variety of problems regarding consistency of reporting as well as privacy and security of data containing patron PII. The data warehouse also provides the opportunity for the Library to balance the needs of data analysis and patron privacy through various de-identification techniques and approaches in the warehouse architecture.

Data Warehouse Architecture—Approaches to Security and Privacy

PII-1 AND PII-2

The approach as to what to include in the data warehouse is guided by the NIST definition of PII-1 and PII-2. Between the two categories, PII-1 tends to be clearer in terms of what needs to be excluded from the warehouse: full name, home address, library barcode, patron record number, and so on. There are a few pieces of PII-1, though, that can be obfuscated to keep some level of granularity in the warehouse for data analysis. For example, many people might be familiar with the case of replacing the date of birth with age. For reporting purposes, the age is just as useful as having the date of birth; for privacy purposes, listing the age instead of the date of birth makes it more difficult to re-identify a person through the warehouse data.

Another way to obfuscate individual data while not tying PII-2 data back to individuals is data aggregation. In the case of title usage statistics from a major digital resources vendor, several staff needed the ability to report on title usage by certain demographic characteristics, such as home branch, age, and council district. Instead of having the demographic information all in one table tied to a specific title, multiple tables were created with each one having a different demographic indicator. For example, one table has title information tied to age group, another table has the same title information tied to the borrower type code from the ILS, and so on. Data stored in these tables were also analyzed against the existing data in the data warehouse, resulting in the adjustment of an existing title circulation table for the same vendor to minimize the overlap of data points between the table and the newer aggregated tables.

EXTRACT-TRANSFORM-LOAD

In a data warehouse, the data goes through a three-step process called extract, transform, and load, or ETL. The ETL process is key to ensuring that no raw PII data enters the data warehouse proper. The following example of importing circulation transactions illustrates the general ETL process of importing data into the warehouse:

1. A script exports the non-PII patron data from the patron record and the item record from the ILS and imports the data into a staging database outside of the data warehouse. During this process the script also transforms the full call number into a truncated call number to obfuscate the PII-2 data point.
2. In the staging area, scripts then prepare and pull together the two separate datasets, matching the de-identified patron information with each transaction.
3. A script then loads the transformed data from staging into the appropriate data warehouse table.

By using the ETL process, the Library has more control as to what data to export from various systems and what data is imported into the database and in what state that data is at the point of import. An ETL process reduces the risk of accidental inclusion of unobfuscated PII or other data that could be used to identify an individual.

PATRON DE-IDENTIFICATION

As mentioned above, the Library needed a way to perform longitudinal analysis without identifying specific individuals. To research use of a particular resource or service over a period of time, however, a way to track distinct data points was needed. One approach is to record all of the transactions with the age and home branch of the patron. The problem with this approach, though, is that it restricts the ability to answer questions such as "do people who check out ebooks still use print?" The essential key to answer questions such as the one listed is that we need to know that Person A is Person A and Person B is Person B, and nothing more.

The solution to tracking distinct data points for the data warehouse is a de-identified patron ID, or De-ID. The De-ID consists of the borrower record number from the ILS, plus a few other key pieces of patron information, run through a SHA-256 hashing algorithm.[ii] In addition, we add a salt to the ID for added security.[iii] The creation of the De-ID happens outside of the data warehouse.

[ii] ii. SHA stands for Security Hash Algorithm. SHA-256 refers to a specific set of cryptographic hashing algorithms designed to create strings of text that cannot be reverse engineered back to the original data fed into the algorithm.

[iii] iii. "Salt" refers to random data that is inserted during the hashing process, making it more difficult for potential attackers to reverse engineer the algorithm used to create the hashed value.

ACCESS

Access to the database portion of the data warehouse is tightly controlled. Only the IT staff who maintain the warehouse have full read-write access to the database. Select library staff have a read-only direct connection to the database. This mitigates the risk of unintentional (or intentional) changes to the data in the database.

The reporting portion of the data warehouse includes a section on the staff SharePoint intranet where staff can access "canned" reports created by IT, such as collection usage by collection code or circulation numbers of items by branch. Staff cannot access the full database and all the tables from the site, though staff can access select tables of raw data (again, access provided by IT). The data warehouse as a whole is covered under existing policies and procedures regarding access to patron information. The data in the warehouse is treated like data in the ILS—staff already have strict, clear policies about how, when, and why they can access patron data.

RISK MITIGATION

Data warehouses and de-identification cannot be fully free from risk of re-identification of individuals; nevertheless, the warehouse's structure is as such that said risk of re-identification is low. Some risk mitigation strategies are mentioned above: de-identification, obfuscation of PII data, data aggregation, and controlled access of raw data. Another mitigation is the overall architecture surrounding the warehouse. To identify an individual's transactions in the data warehouse, one has to do the following:

1. Breach the ILS database and locate the patron record.
2. Recreate the hash algorithm used in creating that patron's De-ID, including figuring out the salt and the pieces of information used for the De-ID before they are hashed.
3. Breach the data warehouse database and query the table.

The risk for each step varies, depending on various circumstances surrounding each step. Risk mitigations for breaching the two databases above include following best practices and security standards for server and network security, as well as creating and enforcing appropriate access and permissions for user accounts for each system. Nonetheless, given enough resources and time, a potential attacker could execute a successful breach of either database. Recreating the hash algorithm, on the other hand, would be the most difficult out of the three steps above, provided that those who created the algorithm do not fall victim to a social engineering attack or unintentional release of information, such as revealing what pieces of information are included in the creation of the De-ID.

There are other risks beyond someone breaking into the Library's systems, including government requests and data leaks. The de-identification and PII obfuscation guidelines for the data warehouse only leaves the fact that certain kinds of transactions happened, and no specifics, including specific websites visited, titles borrowed by individuals, and so on.

The Data Warehouse's Effect and Considerations

The data warehouse proved useful early in its inception. In the first iteration of the data warehouse, the Library included usage statistics from the library computer reservation system. The data in the warehouse was obfuscated to only include the date and length of time for each session, tied to a De-ID. Because the data was structured in a way that staff can track unique and repeat computer sessions within a period of time, the Library was able to analyze the existing public computer usage policy and adjust the policy to minimize the misuse of the Express workstations (Yoose and Halsey 2016; Loter 2016).

Currently, the data warehouse has reached a critical milestone in housing several types of circulation data by title, aggregated with obfuscated demographic information, such as age range and Census Tract information. The reporting features of the data warehouse have reached a milestone with the launch of a SharePoint site where staff can run "canned" reports, including circulation by branch in a specific timeframe, off of the database.

The future of the data warehouse at the Library will only see growth in the data it houses and the reporting features for staff. Nonetheless, with the increase in data and reporting, the data warehouse's future will be guided by a governance structure. While the IT department is the business owner for the majority of data that resides in the warehouse, the data warehouse ultimately serves the organization's reporting and statistical needs. For the warehouse to be viable in the long term, the warehouse must reflect the business needs of the organization. Other departments in the organization—including Technical and Collection Services, Public Services, and Administrative Services—therefore have a key stake in the warehouse, particularly what data is stored, establishing the authoritativeness of data stored in the warehouse and how it is reported out to both internal and external audiences. Including the stakeholders in the governance of the data warehouse gives the opportunity for the warehouse to meet organizational needs while it provides the chance for education about the abilities and limitations of current data collection and management practices at the Library with the overarching theme of balancing patron data privacy with reporting needs.

Practical Implications for Libraries

Libraries are asked to provide data for making mission-critical decisions surrounding the allocation of resources. A data warehouse can be a valuable asset for a library in making these decisions without creating major risks in using patron data in the decision-making process. Libraries considering their own data warehouse should consider several factors and risks in deciding to either create their own data warehouse or contract a vendor in creating/hosting a similar product.

> “IT [IS] IMPORTANT THAT LIBRARIES USE THE DATA COLLECTED BY THEIR LOCAL SYSTEMS AS WELL AS REMOTE SERVICES IN A RESPONSIBLE MANNER THAT PROTECTS THE PATRONS BUT AT THE SAME TIME DOES NOT NEGLECT THE ORGANIZATIONAL NEEDS FOR EVALUATION AND INFORMED DECISION MAKING

Service Population Size

One reason why the SPL's data warehouse can be effective is the size of the service population that the Library serves. Smaller library systems would run a greater risk of identification, even with de-identification methods. Smaller library systems run a greater chance of having distinct data points tied to specific individual outliers. For example, if a patron lives in a zip code with a small population and does not belong to the majority demographic groups of that zip code, that patron would become easier to identify in a database even with a De-ID and obfuscated PII-1 information.

Available Resources

The SPL has the resources to build and support an in-house data warehouse, including server space, software, and the technical skills of several staff. Some of these skills include knowledge of database architecture, hashing algorithms, obfuscation and aggregation approaches, ETL procedures, and SQL. If libraries wish to secure the information in a data warehouse, a base level of skills, knowledge, and resources are needed to mitigate risks of unintentional disclosure of PII-1 and PII-2.

Data Ownership and Liability

For libraries who wish to contract with a vendor to create a data warehouse or something similar, it is vital for the library to retain ownership of the data they send to the vendor. On a foundational level, libraries differ from vendors in the sense that vendors do not have a commonly held standard of ethics and principles that libraries hold surrounding patron privacy. While libraries are bound to uphold the ethics and principles held by the profession, vendors are not under any professional obligation to do so. Not owning the data in the vendor system increases risk, including exposure of data in a wider data breach, accidental or intentional data leaks, and so on. In addition, the library puts itself in greater risk if there is no liability clause in the vendor contract in case there is a breach or leak. Finally, if the library decides to leave a vendor and does not own the data in the vendor system, the vendor is under no obligation to delete the data if there is no clause in the contract for deletion upon cancellation of services. One way to mitigate the risks mentioned above is to include a data liability clause in the vendor contract, such as the one developed by the SPL in the appendix.

Security and Privacy

The approach to security and privacy for both locally hosted and vendor hosted data warehouses differ in the level of control a library has over the environment. A locally hosted warehouse offers more control over the level of security and privacy a library can build into the data warehouse; the tradeoff, though, is that there needs to be enough resources and skillsets on hand to implement and maintain the desired level of security and privacy. A vendor should have the resources and skillsets, but then the tradeoff is less control over the security and privacy practices applied to the data warehouse.

Future Considerations

Data warehouses, when combined with de-identification of patron data, can be a valuable tool for libraries needing data for assessment and strategic planning. The level of granularity provided by de-identification enables libraries to conduct longitudinal research and analysis that can lead to more effective distribution of limited library resources. Going back to the questions asked in the introduction of the article, by analyzing the de-identified data, a library can create targeted programs and services focused on retaining active teen patrons when they cross over to the next age group if the data shows that active patrons in their twenties were active in their teens. If the data shows that a sizable number of patrons from one home branch are traveling across the city to use another branch library's language collection, then collection and branch managers can plan ways to grow that language collection's footprint in the home branch in question for easier access.

Not every library can cleanly implement a de-identified data warehouse, partly because of limitations of current de-identification practices (particularly for small data sets) and partly because of resource limitations, be it staff or budget. As de-identification methods evolve, risk of re-identification in small datasets might decrease. There are ways for these libraries to gain similar insights without a full data warehouse implementation, but the risks of potential exposure or identification of unique patrons tied to their activity are still considerable given current practices. In addition, libraries who do reach out to vendor solutions, such as the case of St. Paul Public Library in 2015, face increased scrutiny from other libraries as well as the community that they serve (Gilbert 2015).

Given the rise of evidence-based practices and assessment in libraries in recent years, combined with tying outcomes to future funding and resource allotments, it becomes only more important that libraries use the data collected by their local systems as well as remote services in a responsible manner that protects the patrons but at the same time does not neglect the organizational needs for evaluation and informed decision making. De-identification—and, to a larger extent, anonymization—of data is one of many tools that libraries have at their disposal in conducting responsible data assessment. Unfortunately, this tool is out of reach for some libraries to implement in-house. These libraries, under pressure to produce data for both internal and external audiences (and funding), look outward to vendor products to meet those needs. Libraries have several products to choose from, but the matter of libraries consolidating all patron activity data with a third-party vendor cannot be left unaddressed by the library community. Some of this conversation is already taking place in the form of the ALA Privacy Guidelines and upcoming checklists,[iv] but there is room for the conversation to grow. The community will need to test and to solidify ways to hold both parties—libraries and vendors alike—accountable for protecting patron privacy.

[iv] A current list of the guidelines, as well as the upcoming checklist, can be access through http://www.ala.org/advocacy/privacyconfidentiality.

References

American Library Association (ALA). 1996. "Library Bill of Rights." http://www.ala.org/advocacy/intfreedom/librarybill.

———. 1991. "Policy concerning Confidentiality of Personally Identifiable Information about Library Users." Ammended June 30, 2004. http://www.ala.org/advocacy/intfreedom/statementspols/otherpolicies/policyconcerning.

Garfinkel, Simson L. 2015. "De-identification of Personally Identifiable Information." *NIST*. http://csrc.nist.gov/publications/drafts/nistir-8053/nistir_8053_draft.pdf.

Gilbert, Chris. 2015. "Coming soon to your St. Paul library: Data tracking." *Minnesota Public Radio News*. June 30. Accessed January 12, 2017. http://www.mprnews.org/story/2015/06/30/library-analytics.

International Federation of Library Associations (IFLA). 2016. "IFLA Statement on Privacy in the Library Environment." April 5. http://www.ifla.org/publications/node/10056.

Loter, Jim. 2016. "Gaining Insights and Protecting Privacy: De-identifying Patron Data at The Seattle Public Library." *Alki* 32(1): 11-13. Accessed January 12, 2017. https://wala.memberclicks.net/assets/Alki/alki_mar2016_v32-1-v3.pdf.

TechCrunch. 2006. "AOL: 'This Was a Screw Up'." http://techcrunch.com/2006/08/07/aol-this-was-a-screw-up/.

United States. 2008. *Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information: Report to Congressional Requesters*. Washington, DC: US Govt. Accountability Office. http://purl.access.gpo.gov/GPO/LPS111810.

Yoose, Becky, and Stephen Halsey. 2016. "De-identifying Patron Data to Balance Privacy and Insight." Presented at Public Library Association Conference, Denver, Colorado, April 7. http://2016.placonference.org/program/de-identifying-patron-data-to-balance-privacy-and-insight/.

Appendix. The Seattle Public Library Data Liability Addendum for Vendor Contracts

ADDENDUM

CONFIDENTIALITY OF SEATTLE PUBLIC LIBRARY RECORDS AND DATA

The Seattle Public Library (SPL) collects and manages records and data which require confidentiality under one or more federal or state laws, or under recognized industry standards, including but not limited to, the following:

- Health Insurance Portability and Accountability Act of 1996
- Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009
- Children's Online Privacy Protection Act of 1998 (COPPA)
- The Privacy Act 1974 (as specified in the National Institute of Standards and Technology (NIST) SP 800-122)
- Washington State RCW 42.56.310
- Family Educational Rights and Privacy Act of 1974
- The American Library Association Library Bill of Rights
- United States Constitution, including the first and fourteenth amendment

Specifically, a provider of services to SPL will not reveal or disclose any data or records, either physical or electronic, which are designated as confidential by the Library or which pertain to SPL patrons when such data or records could be used in any manner to identify a Library patron or any references or materials that a specific Library patron accesses.

A provider of services to SPL must treat all the designated or individually identifiable SPL records as confidential and protected. Encryption of such data while in motion or at rest, and restricting access to confidential data, are typical methods of data protection. No SPL records or data shall be released by the provider to any third party without the prior written consent of the SPL.

In the event that the provider violates this addendum, then said provider agrees to indemnify, defend and hold harmless SPL and its employees from and against any losses, costs, expenses, liabilities (including attorney's fees), penalties and sanctions arising out of or relating to such violation. This addendum does not limit the provider's liability as specifically established under law.

The Parties hereto agree that this amendment modifies, changes, amends and has precedence over any contradictory language in the contract between the Parties.

Provider__________ Date___

Seattle Public Library__________ Date___

Privacy Policies and Practices with Cloud-Based Services in Public Libraries

An Exploratory Case of BiblioCommons

Katie Chamberlain Kritikos (kritikos@uwm.edu), PhD Student, UW-Milwaukee School of Information Studies
Michael Zimmer (zimmerm@uwm.edu), Associate Professor, UW-Milwaukee School of Information Studies

Public libraries are increasingly turning to cloud-based and Library 2.0 solutions to provide patrons more user-focused, interactive, and social platforms from which to explore and use library resources. These platforms—such as BiblioCommons—often rely on the collection and aggregation of patron data, and have the potential to disrupt longstanding ethical norms within librarianship dedicated to protecting patron privacy. This article reports on the results of a pilot research study investigating how libraries are implementing third-party cloud computing services, how these implementations might impact patron privacy, and how libraries are responding to these concerns. The results of this research provide insights to guide the development of a set of best practices for future implementations of cloud-based Library 2.0 platforms in public library settings.

Introduction

Public libraries are increasingly turning to cloud-based and Library 2.0 solutions to provide patrons more user-focused, interactive, and social platforms from which to explore and use library resources while taking advantage of new opportunities for cost savings, flexibility, and enhanced data management (Casey and Savastinuk 2007; Courtney 2007; Casey and Savastinuk 2006). These third-party cloud services provide robust solutions to help libraries deliver resources, services, and expertise efficiently while also encouraging patrons to share information and participate in a platform that empowers them to socialize and leverage the power of a large community of users (Breeding 2011; Goldner 2010). Examples of cloud-based Library 2.0 platforms for libraries include OCLC WorldShare, Ex Libris Alma, and BiblioCommons.

Alongside the growth in cloud-based platforms to deliver library services, patrons are increasingly encouraged to participate in their integrated social and Web 2.0 features, ranging from maintaining user profiles, to creating lists of books, to sharing comments with other users, among others. Many such platforms also aggregate patron usage and activity data to fuel algorithmic filtering, provide personalized content and recommendations, and help identify and analyze trends. While librarians have historically engaged in professional practices that limit retention of patron data and protected confidentiality, such as limited tracking of user activities, having short-term data retention policies, and fostering the anonymous browsing of library materials (Morgan 2006; Gorman 2000), many Library 2.0 platforms are largely based on the tracking, collection, and aggregation of user data. Libraries are thus faced with balancing the use of cloud computing in libraries and its potential to disrupt longstanding ethical norms within librarianship dedicated to protecting patron privacy (Zimmer 2013a, 2013b).

This article reports on the results of a pilot research study investigating how libraries are implementing third-party cloud computing services, how these implementations might affect patron privacy, and how libraries are responding to these concerns. Focusing on thirty-three libraries who have implemented the BiblioCommons cloud-based discovery layer to manage their collections, this study assesses whether the participating libraries modified their privacy policies after launching the new Library 2.0 platform and how any potential effects to privacy were communicated to patrons. The results of this research provide insights to guide the development of a set of best practices for future implementations of cloud-based Library 2.0 platforms in public library settings.

Library 2.0: Technology and Privacy in Libraries

Patron Privacy and Librarian Ethics

Privacy is a necessary ingredient for achieving and protecting intellectual freedom because it forms the bedrock for an individual's right to read and to receive ideas and information (Richards 2015, 2013). As former Supreme Court Justice Louis Brandeis found in his dissenting opinion in *Olmstead v. United States*, "The right to be left alone—the most comprehensive of rights, and the right most valued by a free people" (*Olmstead v. U.S.* 1928). Only when an individual is assured that her choice of reading material does not subject her to reprisals or punishment can she fully enjoy the freedom to explore ideas, weigh arguments, and decide for herself what she believes (Richards 2015, 2013; see ALA 2016). Such freedoms are threatened in an atmosphere in which library use is monitored and individual reading and library-use patterns are available to anyone without permission (Zimmer 2013a, 2013b).

To address privacy issues in US libraries, a set of "librarian ethics" has emerged from documents and ethical frameworks that the American Library Association (ALA) has refined and codified over time (see Magi and Garnar 2015). Ensuring the free and unfettered access to information is a cornerstone of the librarian profession enshrined in the ALA's Code of Ethics. Initially adopted at the ALA's midyear meeting in 1939, the Code of Ethics establishes general policies to guide ethical decision making in libraries (ALA Council 2008). The ALA also adopted the Library Bill of Rights in 1939, creating a formal policy statement on intellectual freedom that entitles everyone to free thought and expression and to the free access of library materials (Magi and Garnar 2015). In response to the changing global political environment at that time, the Library Bill of Rights outlined three policy statements to ensure free and open access to public library services: (1) library materials should be selected on the basis of their value and intrinsic interest to the community, not on the authors' race, nationality, political, or religious views; (2) library materials should "fairly and adequately" represent all sides of social issues; and (3) library meeting rooms should have a democratic open-use policy to provide equal access to all community groups (Magi and Garnar 2015).

From the moment that the ALA adopted the Library Bill of Rights, intellectual freedom defined the library's role as a forum for uninhibited intellectual inquiry and debate (Magi and Garnar 2015). Revisions to the policy followed as libraries faced challenges to intellectual freedom during the politically and socially tumultuous years between 1939 to 1969 (Magi and Garnar 2015), culminating in today's strong statement of six policies that express both the rights of library users to intellectual freedom and the expectations that the ALA places on libraries to support their users (ALA Council 1996). Patron privacy and intellectual freedom, however, are perennially challenged, such as through government attempts to gain access to patron records (see Foerstel 2004; Doyle 2003; Foerstel 1991; Kennedy 1989; McFadden 1987). In response, the ALA has continually reaffirmed its commitment to protecting these values, issuing policy statements like *Confidentiality of Personally Identifiable Information about Library Users* (ALA Council 2004) and *Privacy: An Interpretation of the Library Bill of Rights* (ALA Council 2014).

Complementing the ALA's policy responses to intellectual freedom and privacy threats, librarians and libraries often take action to protect patron privacy and confidentiality, including destroying patron reader records, destroying internet access logs daily, posting warning signs, offering patron education on privacy issues, and abandoning plans to use new technology that profiles the reading habits of patrons and informs them when works they may enjoy are published (Murphy 2003; Sanchez 2003). Indeed, librarians have a rich history of protecting patron privacy, fighting to ensure that the democratic ideal of intellectual freedom survives such challenges to the privacy and confidentiality of patrons' information-seeking activities (Zimmer 2013a, 2013b). For example, Louise Robbins, a historian of ALA policy responses to intellectual freedom threats, has argued that the Library Bill of Rights and related ALA policies grant librarians both the responsibility and the tools to defend the right of readers to freedom of inquiry, which established a "zone of autonomy" for librarians to perform their duties (Robbins 1991, 360). Such a zone of autonomy also naturally extends to library patrons, who traditionally count on libraries to provide the freedom to read, inquire, and learn without undue oversight or threats of surveillance. Web 2.0, Library 2.0, and the use of technology in libraries, however, complicate the existing privacy norms and expectations within the library context.

Introducing Web 2.0 and Library 2.0

In general, "Web 2.0" refers to second-generation websites and services whose design and functionality encourage user interactivity, collaboration, and user-generated and -driven content (Rustad 2016; Casey and Savastinuk 2007; Courtney 2007). Examples of Web 2.0 websites that enable "users to work collaboratively" and increase the "scope of synchronous communications" (Rustad 2016, 20) include Wikipedia, YouTube, and Facebook. Web 2.0 transcends technology to capture the zeitgeist of modern ideas, behaviors, and ideals (see Allen 2008). It represents a blurring of the boundaries between web users and producers, consumption and participation, authority and amateurism, play and work, data and the network, and reality and virtuality (Zimmer 2008). In short, Web 2.0 suggests that everyone can and should use new internet technologies to organize and share information and to interact within communities by harnessing the power of collaboration and social networks to celebrate and empower the individual (Zimmer 2008).

Following the democratic trend of social interaction and collaboration, "Library 2.0" brings the ideology of Web 2.0 into the library. Librarian Michael Casey (2005), who originated the term Library 2.0 in 2005, defines the concept as user-centered change that gives library users a participatory role in the design of physical and virtual library services. At the time of Library 2.0's inception, library scholars and practitioners grappled with the exact definition of the phenomenon (see, e.g., Boxen 2008; Evans 2008; Farkas, 2007; Lankes et al. 2007; Murley 2007; Maness 2006; Bingsi and Xiaojing 2006). Even without a standard definition, however, the literature reflects a consensus that the implementation of Library 2.0 technologies and services means bringing interactive, collaborative, user-centered, and web-based technologies to the library (Casey and Savastinuk 2007; Courtney 2007; Casey and Savastinuk 2006).

Examples of Library 2.0 technology related to OPACs and discovery layers include

- creating dynamic and personalized recommendation systems (e.g.,"other patrons who checked out this book also borrowed these items"), similar to Amazon and related online services;
- allowing users to create personalized subject headings for library materials through social tagging platforms like Delicious or GoodReads; and
- providing patrons the ability to evaluate and comment on particular items in a library's collection through rating systems, discussion forums, or comment threads (Casey and Savastinuk 2007; Courtney 2007).

To participate in and benefit from the Library 2.0 services in these examples, library patrons may have to create user accounts, divulge personal interests and intellectual activities, and risk the tracking and logging of their library activities and personal data (Zimmer 2013a, 2013b). Hence, launching Library 2.0 features challenges traditional librarian ethics regarding patron privacy discussed above (Casey and Savastinuk 2006; Litwin 2006).

Library 2.0 Ten Years Later

A review of more recent library and information science literature expands the Library 2.0 discussion in both scholarly and professional circles, starting with its purpose and function (see Huvila et al. 2013; Kwanya, Stilwell, and Underwood 2012; Anttiroiko and Savolainen 2011). Anttiroiko and Savolainen (2011) study how public libraries adopt Library 2.0 technologies to revitalize their offered services, identifying the main goals of using new technologies as communication, content sharing, social networking, and crowdsourcing.

While scholars find the continued and increasing prevalence of Web 2.0 technology in public libraries (Mannheimer, Young, and Rossmann 2016; Deodato 2014), Library 2.0 has now been introduced into academic libraries (Hess, LaPorte-Fiori, and Engwall 2015; Boateng and Liu 2014; Mahmood and Richardson 2013). There is also growing international treatment of Web 2.0 and Library 2.0 in the literature of countries such as Malaysia (Abidin, Kiran, and Abrizah 2013); Pakistan (Arif and Mahmood 2012); Africa (Lwyoga 2013); international cities (Mainka et al. 2013); and Poland (Wójcik 2015), to name a few. Additionally, a 2015 study investigated the use of social media tools to enhance library inclusion and outreach activities by comparing Web 2.0 implementation in Greater China, Switzerland, the United States, the United Kingdom, Australia, and New Zealand (Abdullah et al. 2015).

Despite the increasing use of Library 2.0, Kwanya et al. (2012) lament the lack of cohesion in standards for its implementation and management, concluding that libraries will have to adopt and adapt new technology based on the context of their unique communities. Huvila et al. (2013) find that the new technological skills required of traditional librarians can disrupt their work identity and confidence. What's more, librarians can also lack proper education in new technologies (Huvila et al. 2013) and the libraries themselves often do not have suitable privacy policies that cover patron privacy and confidentiality (Hess et al. 2015; Lambert, Parker, and Bashir 2015; Al-Suqri and Akomolafe-Fatuyi 2012; Magi, 2010). Both issues demonstrate the literature's continued treatment of privacy and librarian ethics (see Breeding 2016a; Campbell and Cowan 2016; Gressel 2014; Lambert et al. 2015; Lilburn 2015).

In addition to the above concerns, many authors highlight the prevalence of digital privacy and security issues in the modern library. Current Library 2.0 privacy issues range from privacy and security in digital libraries (Al-Suqri and Akomolafe-Fatuyi 2012) to privacy and security for now-typical library software like discovery layers (Breeding 2016a, 2016b). One example is protecting privacy when patrons from marginalized or underrepresented groups, such as the lesbian, gay, bisexual, and transgender community, use library services to research private, personal matters (Campbell and Cowan 2016). Related to privacy and security, Lilburn (2015) points out the sobering fact that companies that own many of the Web 2.0 tools used in libraries track and monitor user behavior for their own profit, as well as that commercial social media can empower governments and corporations. On a related note, a 2015 study by Lambert et al. finds that while the increased use of digital vendors provides enhanced Web 2.0 services, such use threatens patrons' privacy and intellectual freedom because these vendors have access to patrons' personal information (see also Magi, 2010).

Also of note is the broader philosophical discussion regarding Library 2.0, technology, and privacy (see Ard 2016, 2014; Hoffmann 2016; Mathiesen 2015; Magi 2011). In light of the increasing use of advanced information and communication technologies in Library 2.0, Hoffmann (2016) applies the value of self-respect from moral and political philosophy to librarians and scholars interested in social justice issues as a foundation for libraries' protection of patron privacy and intellectual freedom. Continuing the social justice trend, Mathiesen (2015) finds that privacy and intellectual freedom are increasingly thought of as human rights in the global information age. Library and information science plays a central role in facilitating communication about human rights (Mathiesen 2015). More specifically, Ard (2014) expresses concern with the surveillance and collection of patron activity and data by third-party digital content vendors. Because the traditional library privacy regime does not restrict what third-party digital service provider can do with this data, libraries should extend the privacy of reader records to *all types* of data practices to protect intellectual privacy from unwanted surveillance by *digital* intermediaries (Ard 2016, 2014).

This need for protection from unwanted surveillance by digital intermediaries inspired Gressel (2014) to argue that many librarians have neglected digital privacy issues in their rush to integrate Web 2.0 technologies into their libraries and to advocate the protection of patron privacy over the implementation of Web 2.0 technologies. And while it may be easy to dismiss privacy as no longer relevant, especially to the younger generation (Gressel 2014), Magi draws on interdisciplinary scholarship ranging from law to psychology to philosophy, among others, to offer fourteen compelling reasons why privacy still matters to individuals and to society in three categories: "(1) benefits to the individual, (2) benefits to personal relationships, and (3) benefits to society" (Magi 2011, 198). In light of the growing tension between protecting privacy and intellectual freedom and the advancement and application of new technologies in libraries, librarians must adopt a broad understanding privacy (Magi 2011).

Library 2.0 and privacy also see an expanded discussion and increasing treatment in professional circles focusing on the dual role of libraries as the providers of information and the protectors of patron privacy. Statements and tools from the ALA include 2014 updates to *Privacy: An Interpretation of the Library Bill of Rights* (ALA Council 2014) and the Privacy Toolkit (ALA IFC 2014), as well as 2016 updates to the variety of privacy guidelines issued by the Privacy Subcommittee of the Intellectual Freedom Council (ALA IFC 2016a, 2016b, 2016c). Additionally, the Trend Report (IFLA 2013) and Trend Report Update (IFLA 2016) from the International Federation of Library Associations and Institutions identify privacy and technology as the chief trends shaping and transforming the information ecosystem.

Finally, nonprofit organizations like the Library Freedom Project (2017), a partnership of librarians, technologists, attorneys, and privacy advocates, strive to address the increasing problems of surveillance and promote intellectual freedom in libraries. All of these organizations demonstrate an awareness of the possibilities and pitfalls of the increasing use of Web 2.0 technology and a growing concern over surveillance in libraries. The overall message focuses on the need for education about surveillance threats, user privacy rights, and library responsibilities to upholds intellectual freedom and privacy. The goal is to ensure the pursuit of free, open inquiry by library patrons and to combat surveillance.

> "AS PUBLIC LIBRARIES CONTINUE TO RELY ON LIBRARY 2.0 SERVICES FROM THIRD-PARTY VENDORS LIKE BIBLIOCOMMONS, REFINING AND TAILORING PRIVACY POLICIES AND PRACTICES IS CRITICAL FOR PROTECTING PATRON PRIVACY IN THE DIGITAL AGE

Context for the BiblioCommons Study

The above review of the recent scholarly and professional literature reveals a moderate increase in attention to privacy and security in Library 2.0 over the past decade. Libraries have been slow to integrate Library 2.0 platforms—and to update their privacy policies (Hess et al. 2015)—and so privacy, confidentiality, and related ethical concerns remain largely unresolved. For example, adopting the research methodology and analysis used by Magi (2010) to review the privacy policies of library vendor licenses, Lambert et al. (2015) studied the privacy policies of the top five digital content vendors at the time (Axis 360, Hoopla, OneClickDigital, OverDrive, and Zinio) to determine whether the policies (1) met the privacy standards of the American Library Association Code of Ethics, (2) met the Fair Information Practices (FIP) standards of American industry, and (3) were accessible and understandable to public library patrons (Lambert et al., 2015). The study found that while the digital content vendors largely complied with the FIP standards, their privacy policies failed to meet the heightened privacy standards of librarian ethics. Thus the increased use of digital content vendors to provide enhanced Web 2.0 services in public libraries threatens the privacy and intellectual freedom of patrons because the vendors have access to patrons' personal information (Lambert et al., 2015).

To further explore the protection of patron privacy and the implementation of Library 2.0 services, the current study investigates the relationship between the implementation and use of BiblioCommons, a cloud-based discover layer, and the privacy policies in participating public libraries.

Case Study: BiblioCommons

Drawing from a sample of the US public libraries that licensed the BiblioCommons software as of January 2015, this study investigates whether—if at all—libraries have modified their privacy policies and practices upon implementation of the Library 2.0 platform. As public libraries continue using Library 2.0 services from third-party vendors like BiblioCommons, refining and tailoring policies to new technology is critical for protecting patron privacy in the digital age. Through this analysis of privacy policies from the participating public libraries, we are better positioned to recommend best practices for library privacy policies in the era of Library 2.0.

What Is BiblioCommons?

BiblioCommons is a Canadian company that develops and hosts cloud-based software solutions for public libraries, allowing partnering libraries to enhance their traditional online public access catalog (OPAC) with a dynamic, integrated, and social discovery layer. According to the BiblioCommons website, the company's goal is "to help public libraries deliver the same kind of rich discovery and community connection experiences online that the library has always delivered in its branches—all built around the heart of the library: its collections" (BiblioCommons 2016a). At the time of this study in January 2015, there were thirty-four participating libraries in the United States, presented in table 1. As of October 2016, BiblioCommons has fifty-three participating public libraries in the United States, as well as libraries in Canada, Australia, and New Zealand (BiblioCommons 2016c).

BiblioCommons Products and Information Flows

The BiblioCommons software product is a fully managed and integrated online solution that combines the public library's circulation and cataloguing scheme, branding, etc.; the BiblioCommons connectors, code, servers, security, upgrades, updates, and support; and the worldwide community of users contributing ratings, reviews, and lists of books, movies, and more (BiblioCommons 2016b).

The main BiblioCommons software product is BiblioCore. To further the company's goal to be the "center of online discovery and connection" (BiblioCommons 2016a), BiblioCore replaces the public library traditional OPAC's account management and search functions, allowing public library staff and patrons to search the catalog, brose and explore the online stacks, and borrow materials via online user accounts. To complement BiblioCore, BiblioCommons also offers BiblioMobile, a mobile application, and BiblioWeb, an interactive, integrated website and content management tool.

The BiblioCommons environment encourages users to create their own personal collections and reading guides that lay the foundation for engagement with the library and fellow readers in various ways. The social features of the BiblioCore software include "a common platform that aggregates the shared expertise, opinions and recommendations of staff and customers alike across all libraries, and integrates those contributions back into the local catalog in intelligent ways" (BiblioCommons 2016a). It harnesses the "power of the local OPAC as a gateway to broad participation and engagement" that brings the traditional OPAC into the world of Web 2.0, making the interface more social and interactive for public library patrons (BiblioCommons 2016a; Scardilli 2015). Other social features include sharing reading experiences with others, to rate and review material and to create private or shared lists of titles.

Patrons access the BiblioCommons discovery layer through their home library's website, typically in a seamless fashion. For example, when users browse the Boston Public Library website and click on "BPL Catalog," they are routed to BPL's collection hosted on the BiblioCommons platform, maintaining the general branding and design scheme of the main BPL website. From the customized BiblioCommons platform site, patrons can browse items, read comments from other patrons, rate books, share items, and engage in other related social activities. The standard template for the BiblioCommons web interface includes a terms of use and privacy statement at the bottom of each page (see appendix A and appendix B, respectively).

Library patrons may search the library catalog anonymously via the BiblioCommons platform, but they must create an account to use other services, such as placing a hold request or saving a title for later. They must, however, create a separate account to access the full functionality of the BiblioCommons platform, which requires providing BiblioCommons their library card number, PIN and borrower ID, name, birth month and year, and email address. When used by a logged-in patron, BiblioCommons collects the patron's browsing activity on the platform, which can then be associated to the patron's account. As detailed in the "Personal Information" section of the BiblioCommons privacy statement (appendix B), BiblioCommons secures and encrypts all personal information provided by the user during the registration process and does not share information or activity with ad networks or other entities that are not directly involved in the library's services: "Information in your BiblioCommons account that personally identifies you is encrypted and stored in a secured facility." Users can access their borrowing activity (current or recent loans, due dates, fines, etc.) within BiblioCommons, but the platform does not automatically store that information within a user's account. Rather, it merely is pulled from the library's separate circulation system for display. Patron content created through the "Shared Content" features, such as providing book reviews, ratings, or creating shared lists or collections, is linked to a patron's BiblioCommons account.

Reactions to BiblioCommons in the Library Community

While BiblioCommons remains small, it is growing, and the library world has noticed. An early adopter of BiblioCommons, the New York Public Library expressed the

Table 1. Libraries participating with BiblioCommons

Library	Location
Austin Public Library	Austin, TX
Bellingham Public Library	Bellingham, WA
Boston Public Library	Boston, MA
Central Arkansas Library System	Little Rock, AK
Central Rappahannock Regional Library	Fredericksburg, VA
Chapel Hill Public Library	Chapel Hill, NC
Chicago Public Library	Chicago, IL
CLEVNET	Cleveland, OH
Daniel Boone Regional Library	Columbia, MO
Deschutes Public Library	Bend, OR
Greenwich Library	Greenwich, CT
Johnson County Library	Shawnee Mission, KS
King County Library System	Issaquah, WA
Lawrence Public Library	Lawrence, KS
Multnomah County Library	Portland, OR
New York Public Library	New York, NY
Oceanside Public Library	Oceanside CA
Olathe Public Library	Olathe, KS
Omaha Public Library	Omaha, NE
PAC2 Consortium	Petoskey, MI
Peninsula Library System	San Mateo, CA
Petoskey Library District	Petoskey, MI
Pima County Public Library	Tucson, AZ
Portland Public Library	Portland, OR
Princeton Public Library	Princeton, NJ
Pueblo City-County Library District	Pueblo, CO
San Antonio Public Library	San Antonio, TX
San Francisco Public Library	San Francisco, CA
San Mateo County Library	San Mateo, CA
Santa Clara County Library	Santa Clara, CA
Santa Monica Public Library	Santa Monica, CA
Seattle Public Library	Seattle, WA
Tulsa City County Library	Tulsa, OK
Whatcom County Library System	Bellingham, WA

excitement of partnering with the new software company "to completely transform its current online catalog, making it easier to discover the Library's vast collections while also giving users the power to create reading lists, rate the latest books, and organize groups" (NYPL 2011).[i] More recently, a 2015 review in *Information Today* highlights BiblioCommons' sophisticated search function that is akin to that of Google or Amazon: "The search function offers natural language detection, full native Unicode support, auto-suggest for misspelled keywords, and limiting through an extended set of facets, as well as relevance-ranked results that adapt to a library's data and circulation patterns" (Scardilli 2015).

BiblioCommons also received treatment in the *American Libraries* library report for 2016. In the section on public libraries, the report noted that "the public library technology sector had a relatively quiet year in 2015 with a steady churn of libraries shifting to alternative ILS [integrated library system] products in a competitive environment characterized by marginal differentiation" (Breeding 2016b). One such alternative ILS product is BiblioCommons, which, despite its growing presence in public libraries, has been slow to catch on in some communities. For example, the Columbus (OH) Metropolitan Libraries rolled out their new BiblioCommons website in January 2016 (Narciso 2016). As of April 2016, only about 84,000 people, or 16 percent of the system's 500,000 library cardholders, had signed up for BiblioCommons accounts (Narciso 2016).

Further, while most librarians recognize how services like BiblioCommons can greatly improve the delivery of library services and enhance patron activities, the increased need for the tracking, collecting, and potentially retaining of data about patron activities presents a challenge to the traditional librarian ethic regarding patron privacy (Zimmer 2013b; Litwin 2006). Such concerns are evident in numerous reports of community reactions to new implementations of BilblioCommons in local libraries (see, e.g., Narciso 2016; Warfield 2015; Greiner 2013; Breeding 2011). For example, Narciso (2016) reports that when BiblioCommons launched at the Columbus Metropolitan Libraries, "aversion to change" discouraged library patrons from signing up for an account: only "about 84,000 cardholders—just 16 percent of the system's more than 500,000 cardholders—signed up, surprising some library officials." Additionally, Warfield (2015) cited patrons' privacy concerns with the implementation of BiblioCommons at the San Francisco Public Library stemming in large part from the library's "long history of making decisions without public input."

Research Methodology

In light of these concerns about patron privacy and the use of third-party Library 2.0 services, this study investigated whether—if at all—libraries have modified their privacy policies and practices upon implementation of the BiblioCommons platform. Specifically, the study sought answers to these exploratory research questions:

RQ1: Did participating public libraries *adjust their privacy policies* upon implementing BiblioCommons services?
RQ2: Did participating public libraries *adjust their privacy practices* upon implementing BiblioCommons services?
RQ3: Did participating did libraries *communicate with patrons* regarding privacy implications of the BiblioCommons service?

The research design for this study was to engage in a document analysis of materials acquired from libraries using the BiblioCommons cloud-based discovery layer software. Purposive sampling was used to target the thirty-four U.S. public libraries using BiblioCommons at the time of initial data collection (January 2015). Open records requests were sent to each participating library requesting the following documents:

1. all contracts, agreements, or related legal/vendor documents the public library might have with BiblioCommons
2. all internal policies, documented procedures, or other materials related to the initial installation and continued implementation of BiblioCommons products and services
3. all notices provided to patrons related to the library's collection and use of patron data, including the library's privacy policy (if extant)

A sample of the open records request is attached to this report as appendix C.

Thirty-three of the thirty-four participating public libraries responded to the records request, with thirty-two

[i] At the time of data collection in January 2015, the New York Public Library had a contract with BiblioCommons. Though as of October 12, 2015, the New York Public Library no longer had a library service agreement with BiblioCommons, its inclusion as part of the sample is relevant and instructive to the data collection and analysis at hand.

of the respondents providing materials.[ii] Materials received included library subscription agreements with BiblioCommons, internal BiblioCommons implementation documents, library privacy policies, and related items. One of the weaknesses of requesting documents from participating public libraries, even via an open records request, was the lack of, or the incompleteness of, the information received. Upon a preliminary assessment of the comprehensiveness of materials received, we used online sources like the BiblioCommons website, participating public library websites, and the Internet Archive Wayback Machine to retrieve missing documents and locate historical versions of received materials.

After collecting the, we conducted a document analysis (Bowen 2009) to investigate answers to our exploratory research questions, focusing on a close reading of materials provided as well as comparisons of materials across participating libraries.

Data Analysis

Privacy Policies

Each of the thirty-four public libraries with service agreements with BiblioCommons use the boilerplate BiblioCommons privacy statement (appendix B), made accessible to patrons at the bottom of the discovery layer's main page. As these privacy policies are located and maintained on the BiblioCommons web servers, all of the policies were the most recent version of the boilerplate (updated January 19, 2015), and none of the language varied across the different partner libraries, save for customization of the library's name in the opening paragraph and other relevant passages.

Significant variance exists, however, in the privacy policies of the partner libraries themselves. Of the thirty-four participating libraries, thirty-two also had an internal library privacy policy in place in addition to the boilerplate BiblioCommons privacy statement (see appendix B), with two libraries (Central Rappahannock Regional Library and Lawrence Public Library) lacking any general privacy policy available on their website. Of those libraries with privacy policies online, only four linked directly to their internal privacy policies from their websites' homepages: Central Arkansas Library System, Multnomah County (OR) Library, New York Public Library, and San Antonio Public Library. The remaining libraries made their privacy policies available to patrons elsewhere on their websites, most commonly in the "About the Library" or "Using the Library" sections. Often, the internal privacy policy was buried deep in the library's website and only accessible after much determined searching. For example, as of the time of this analysis, the Austin Public Library required the following path to access its internal privacy policy: Home > Using the Library > About the Library > Policies and Information > Privacy Statement.

Examining the publication dates of the partner libraries' internal privacy policies, nearly one-third (nine of twenty-eight with version dates) predate the existence of a contract with BiblioCommons. Further, only eight of the thirty-two libraries' internal privacy policies analyzed directly reference the use of BiblioCommons third-party services, and its related privacy policies and practices (see table 2).

Privacy Practices

The request for internal policies, documented procedures, or other materials related to the initial installation and continued implementation of BiblioCommons products and services yielded minimal materials for analysis. Most libraries indicated they did not have any internal policies or formal documented procedures related to the use BiblioCommons, and others simply provided copies of the BiblioCommons installation and training guidelines. We did not receive any information indicating a library implemented or adjusted any internal privacy-related practices in response to the use of BiblioCommons.

In attempting to respond to this request, many libraries provided internal communications and materials to help train library staff on the features and benefits of BiblioCommons, as well as how to communicate with patrons regarding the change. Some of the materials mentioned patron privacy, focusing largely on how to show patrons where the privacy settings are located, or to alleviate general concerns. For example, some training presentations (such as from the Peninsula Library System and the San Francisco Public Library) discussed how patrons could create "Shelves" or "Lists," and noted the ability to made make such features public or private through the platform's privacy settings.

Other training documents (Bellingham [WA] Public Library and Chicago Public Library, for example) showed library staff how to guide patrons through the privacy settings of their BiblioCommons account, and another library (Whatcom County [WA] Library) created an internal training wiki that featured a detailed section on

[ii] The New York Public Library declined to provide materials because, as a private, non-profit educational organization, it was not subject to open records laws (Jacqueline F. Bausch, personal communication, January 9, 2015). Its privacy policies were available online.

Table 2. Participating libraries with BiblioCommons reference in privacy policy

Library	BiblioCommons Reference Wording	Policy Type
Greenwich (CT) Library	"Third Party Services and Internet Communications. . . . The Library encourages users to review the privacy policies of all third-party providers. Users who use the Library's new online public access catalog are encouraged to read the BiblioCommons privacy policy."	Privacy and Confidentiality of Library Records (April 14, 2015)
Johnson County Library, Shawnee Mission, KS	"Catalog Privacy Statement. Our catalog is provided by BiblioCommons and with its own distinct Privacy Statement. Upon registration, you agree to Privacy Statement as part of the BiblioCommons Terms of Use."	Website Policies: Online Privacy (2014, 2016)
Multnomah County Library, Portland, OR	"Third party vendor services. . . . Policies for our discovery software for the on-line catalog: Bibliocommons (MyMCL)."	Privacy and Confidentiality of Library Records (May 7, 2015)
New York (NY) Public Library	"V. Third-Party Partners. . . . Users who use the Library's new online public access catalog are encouraged to read the BiblioCommons privacy policy as well as this privacy overview."	Privacy Policy (October 21, 2011) * No BiblioCommons contract as of October 12, 2015
New York (NY) Public Library	"As part of the catalog transition, all information associated with your user account was transferred from the old system (BiblioCommons) to NYPL on October 12, 2015. PLEASE NOTE that, unless you have already taken steps to deactivate your BiblioCommons account, you will still have an active BiblioCommons account. You should coordinate directly with BiblioCommons if you no longer want an account with them. Your interactions with the new catalog are covered by the NYPL Privacy Policy and not by the BiblioCommons Privacy Statement."	Changes to the Online Catalog: Your Information and Privacy (October 12, 2015
Oceanside (CA) Public Library	"C. Release of Information. 1. . . a. BiblioCommons, Inc. provides the Library's online catalog. If a customer provides them with his or her Library card number, The Library will transmit certain data to them including name, birth date, and e-mail address."	Policy Manual, 4.2 Confidentiality (November 25, 2013)
San Francisco Public Library	"Discovery Layer Interface . . . 13. . . . In acceptance of the BiblioCommons Terms of Use, a user agrees to abide by the BiblioCommons Privacy Statement; users are advised to please read the BiblioCommons Terms of Use and Privacy Statement carefully . . . ." (multiple references)	Privacy Policy (January 1, 2015)
Whatcom County Library System, Bellingham, WA	"What staff may do: . . . At any time it is relevant, staff may show patrons how to register in BiblioCommons, access their account information online or via telephone messaging, use self-checkout, pay fines online, sign up for ELF notification, or any other self-service options." "What a patron may do: . . . When a patron would like information about their account, he or she may view it online via BiblioCommons or ELF, access it via Telephone Messaging, or ask a staff member for assistance."	Patron Confidentiality Administrative Procedure 501.01 (June 18, 2014)

privacy and provided sample text on how to reply to patrons' concerns. Princeton Public Library provided a set of privacy-related "frequently asked questions" (apparently developed by BiblioCommons) to help guide staff responses to concerned patrons.

Communication with Patrons

In response to the request for any communications to patrons related to a participating library's collection and use of patron data, nearly all libraries provided copies of their internal privacy and confidentiality policies, copies of the BiblioCommons terms of use and privacy statement accessible to patrons from the website, or related policy statements (see "Privacy Policies," above, for a discussion of privacy policies).

Several libraries provided supplementary communication materials indented to help patrons understand their privacy within the library, broadly. For example, Daniel Boone Regional Library (Columbus, MO) shared its information brochure designed for new patrons, which notes the library's privacy and confidentiality practices, as did a welcome brochure from the Santa Clara County (CA) Library. Others shared forms used to obtain a library card or create an account, which referred patrons to the library's existing privacy policies.

Only a few libraries provided communication materials specifically designed to help patrons understand the privacy implications of the new BiblioCommons platform. For example, Greenwich (CT) Library produced colorful bookmarks that highlighted various features of the new discovery layer and included mention of how personalized "Shelves" and "Lists" could be set as private or public; it also referred patrons to the library's confidentiality policy as well as the BiblioCommons terms of use for more information about how their information might be shared. Greenwich Library also produced screencast tutorials to help walk patrons through the new features, which included tips on making "Shelves" and "Lists" private or public. Other libraries, such as the Portland Public Library and the Seattle Public Library, shared general help and FAQ pages designed to assist patrons when creating and using BiblioCommons accounts, which typically mentioned and linked to the library's privacy policies as well as the BiblioCommons privacy statement and terms of use.

Based on the materials received from partner libraries, the most comprehensive communication to patrons regarding the privacy implications of BiblioCommons originated from the New York Public Library. In advance of the implementation of the platform in 2011, the library distributed patron fliers and created a webpage titled "Overview of Privacy Issues for NYPL's New Catalog," providing details about the information that will be collected in connection with NYPL's new discovery layer, as well as a summary of how BiblioCommons and NYPL will use that information. The library also made it clear that users did not have to create accounts or use the BiblioCommons interface, and it maintained the legacy catalog interface for patrons who didn't wish to opt into the new platform.

Discussion, Recommendations, and Future Research

Our first exploratory research question was to understand whether participating public libraries adjusted their privacy policies upon implementing BiblioCommons services. The analysis revealed that while eight libraries updated their privacy policies to make specific mention of BiblioCommons, most did not, and nine libraries had policies that have not been updated at all in the time since first contracting with the cloud service provider. This reveals an uneven approach to ensuring that internal policies reflect the technological changes occurring within library services. Our recommendation is that all libraries should adjust their privacy policies to reflect the use of third-party cloud service providers and provide details on how any patron information might be shared, as well as any steps taken to protect patron privacy. Libraries should also ensure privacy policies are easily accessible by patrons, ideally provided directly on the library homepage, which would demonstrate a library's commitment to making the privacy policies transparent and available to patrons.

The consequences of this oversight are, perhaps, mitigated by the fact that the BiblioCommons platform itself has a separate privacy statement that is automatically displayed on each library's installation of the service. This policy statement, along with the terms of use, are frequently updated by BiblioCommons and automatically pushed out to all participating libraries so patrons will always see the most recent version. It is uncertain if participating libraries are knowingly relying on the BiblioCommons privacy policy instead of updating their own, and future research could investigate the motivations behind participating libraries' approach to their internal privacy policies. There is concern that libraries might begin to rely solely on third-party providers to maintain updated privacy policies, especially since libraries' historical commitment to patron privacy might not fully align with the interests of third-party technology providers.

Our second exploratory research question sought to understand if participating public libraries adjusted their privacy practices upon implementing BiblioCommons services. We received limited data that was directly responsive to this request and therefore saw little direct evidence that indicated any library implemented or adjusted its internal privacy-related practices in response to the use of BiblioCommons. Some libraries provided training materials in an attempt to show evidence of some form of internal practices and activities related to the launch of BiblioCommons, and our analysis of these revealed a varied approach to bringing staff up to speed on how users can manage their privacy through BiblioCommons. Not all libraries chose to provide this material (as it was not specifically requested), so a full analysis is not possible.

To better investigate this question of whether libraries changed their data practices in reaction to the use of BiblioCommons, a more targeted data gathering strategy is necessary, and future research might engage in case studies of specific libraries to gain richer qualitative data from personnel directly involved in the implementation and installation of BiblioCommons.

Our third exploratory research question asked how participating libraries communicated with patrons regarding any privacy implications of the BiblioCommons service. While all libraries make available the BiblioCommons privacy statement that automatically appears on the footer of each webpage on the platform, only a handful provided additional material specifically-tailored to communicate with patrons about the new platform. General tutorials often mentioned how certain social features could be set to private or public, but there was little discussion of the type of information that BiblioCommons itself might have access to regarding patron activities. The best practice came from New York Public Library, who took additional steps to ensure patrons were made aware of the new platform and the data sharing that might occur. Our recommendation is for more libraries to follow this example and provide direct and meaningful communication with patrons about what it means to create an account on the BiblioCommons platform.

This study revealed a mixed approach to addressing patron privacy among the libraries using the BiblioCommons cloud-based discovery layer. Future research can build from these exploratory questions and home in on the core issues of whether privacy policies are staying up to date, whether libraries are changing their overall data and privacy practices after engaging with cloud-based services, and how (and to what effect) libraries are communicating with patrons regarding any privacy implications. As public libraries continue to rely on Library 2.0 services from third-party vendors like BiblioCommons, refining and tailoring privacy policies and practices is critical for protecting patron privacy in the digital age.

References

Abdullah, N., S. Chu, S. Rajagopal, A. Tung, and Y. Kwong-Man. 2015. “Exploring Libraries’ Efforts in Inclusion and Outreach Activities Using Social Media.” *Libri* 65, no. 1: 34–47. https://doi.org/10.1515/libri-2014-0055.

Abidin, M. I., K. Kiran, and A. Abrizah. 2013. “Adoption of Public Library 2.0: Librarians’ and Teens’ Perspective.” *Malaysian Journal of Library and Information Science* 18, no. 3: 75–90. https://www.researchgate.net/publication/287559472_Adoption_of_Public_Library_20_Librarians’_and_teens’_perspective.

Al-Suqri, M. N., and E. Akomolafe-Fatuyi. 2012. “Security and Privacy in Digital Libraries: Challenges, Opportunities and Prospects.” *International Journal of Digital Library Systems* 3, no. 4: 54–61. https://doi.org/10.4018/ijdls.2012100103.

Arif, M., and K. Mahmood. 2012. “The Changing Role of Librarians in the Digital World.” *Electronic Library* 30, no. 4 469–79. https://doi.org/10.1108/02640471211252184.

American Library Association (ALA) Council. 1996. “Library Bill of Rights.” http://www.ala.org/advocacy/intfreedom/librarybill.

———. 2004. “Policy Concerning Confidentiality of Personally Identifiable Information about Library Users.” http://www.ala.org/advocacy/intfreedom/statementspols/otherpolicies/policyconcerning.

———. 2008. “Code of Ethics.” http://www.ala.org/advocacy/proethics/codeofethics/codeethics.

———. 2014. “Privacy: An Interpretation of the Library Bill of Rights.” http://www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy.

American Library Association Intellectual Freedom Committee (ALA IFC), Privacy Subcommittee. 2014. “Privacy Toolkit.” http://www.ala.org/advocacy/privacyconfidentiality/toolkitsprivacy/privacy.

———. 2016a. “Library Privacy Guidelines for Public Access Computers and Networks.” http://www.ala.org/advocacy/library-privacy-guidelines-public-access-computers-and-networks.

———. 2016b. “Library Privacy Guidelines for Library Websites, OPACs, and Discovery Services.” http://www.ala.org

/advocacy/library-privacy-guidelines-library-websites-opacs-and-discovery-services.

———. 2016c. “Library Privacy Guidelines for Data Exchange Between Networked Devices and Services.” http://www.ala.org/advocacy/library-privacy-guidelines-data-exchange-between-networked-devices-and-services.

Anttiroiko, A.-V., and R. Savolainen. 2011. “Towards Library 2.0: The Adoption of Web 2.0 Technologies in Public Libraries.” *Libri* 61, no. 2: 87–99. http://doi.org/10.1515/libr.2011.008.

Ard, B. J. 2014. “Confidentiality and the Problem of Third Parties: Protecting Reader Privacy in the Age of Intermediaries.” *Yale Journal of Law and Technology* 16, no. 1: article 1. http://digitalcommons.law.yale.edu/yjolt/vol16/iss1/1.

———. 2016. “Librarians as Privacy Advocates.” *Journal of Law and Policy for the Information Society* 12. Retrieved from http://ssrn.com/abstract=2812703.

BiblioCommons. 2016a. “About Us.” http://legacy.bibliocommons.com/about/about-us.

———. 2016b. “How We Work.” http://legacy.bibliocommons.com/how-we-work/how-we-work.

———. 2016c. “Participating Libraries: United States.” http://legacy.bibliocommons.com/about/participating-libraries/united-states.

Bingsi, F., and H. Xiaojing. 2006. “Library 2.0: Building the New Library Services.” *Journal of Academic Libraries* 1: 2–5. http://en.cnki.com.cn/Article_en/CJFDTOTAL-DXTS200601002.htm.

Boateng, F., and Y. Q. Liu. “Web 2.0 Applications’ Usage and Trends in Top US Academic Libraries.” *Library Hi Tech* 32, no. 1 (2014): 120–38. https://doi.org/10.1108/LHT-07-2013-0093.

Bowen, G. 2009. “Document Analysis as a Qualitative Research Method.” *Qualitative Research Journal* 9, no. 2: 27–40. http://connection.ebscohost.com/c/articles/47652758/document-analysis-as-qualitative-research-method.

Boxen, J. 2008. “Library 2.0: A Review of the Literature.” *Reference Librarian* 49, no. 1: 21–34. https://doi.org/10.1080/02763870802103597.

Breeding, M. 2011. “New York Public Library Partners with BiblioCommons.” *Smart Libraries Newsletter* 31, no. 9: 2–4. https://librarytechnology.org/repository/item.pl?id=16143.

———. 2016a. “Issues and Technologies Related to Privacy and Security.” *Library Technology Reports: Privacy and Security for Library Systems* 52, no. 4: 5–12. https://journals.ala.org/ltr/article/view/5973.

———. 2016b. “Power Plays: Library Systems Report 2016.” *American Libraries* (blog), May 2. https://americanlibrariesmagazine.org/2016/05/02/library-systems-report-2016/.

Campbell, D. G,. and S. R. Cowan. 2016. “The Paradox of Privacy: Revisiting a Core Library Value in an Age of Big Data and Linked Data.” *Library Trends* 64, no. 3: 492–511. https://www.ideals.illinois.edu/bitstream/handle/2142/89851/64.3.campbell.pdf?sequence=2.

Casey, M. 2005. “Working Towards a Definition of Library 2.0.” *LibraryCrunch* (blog), October 21. http://www.librarycrunch.com/2005/10/working_towards_a_definition_o.html.

Casey, M. E., and L. C. Savastinuk. 2006. “Library 2.0: Service for the Next-Generation Library.” *Library Journal* 131, no. 1: 40–42. https://www.researchgate.net/publication/234619983_Library_20_Service_for_the_Next-Generation_Library.

———. 2007. *Library 2.0: A Guide to Participatory Library Service.* Medford, NJ: Information Today, Inc.

Courtney, N., ed. 2007. *Library 2.0 and Beyond: Innovative Technologies and Tomorrow’s User.* Westport, CT: Libraries Unlimited.

Deodato, J. 2014. “The Patron as Producer: Libraries, Web 2.0, and Participatory Culture.” *Journal of Documentation* 70, no. 5: 734–58. https://doi.org/10.1108/JD-10-2012-0127.

Doyle, C. 2003. “Libraries and the USA PATRIOT Act.” Congressional Research Service Report for Congress RS21441. Washington, DC: Congressional Research Service, Library of Congress. http://www.ala.org/advocacy/sites/ala.org.advocacy/files/content/advleg/federallegislation/theusapatriotact/CRS215LibrariesAnalysis.pdf.

Evans, B. 2008. “Library 2.0: The Consumer as Producer.” *Information Today* 25, no. 9: 1–54. http://connection.ebscohost.com/c/articles/34584073/library-2-0-consumer-as-producer.

Farkas, M. G. 2007. *Social Software in Libraries: Building Collaboration, Communication, and Community Online.* Medford, NJ: Information Today.

Foerstel, H. 1991. *Surveillance in the Stacks: The FBI’s Library Awareness Program.* New York: Greenwood.

———. 2004. *Refuge of a Scoundrel: The Patriot Act in Libraries.* Westport, CT: Libraries Unlimited.

Goldner, M. R. 2010. “Winds of Change: Libraries and Cloud Computing.” *BIBLIOTHEK Forschung Und Praxis* 34, no. 3: 270–75. http://docplayer.net/2025170-Winds-of-change-libraries-and-cloud-computing.html.

Gorman, M. 2000. *Our Enduring Values: Librarianship in the 21st Century.* Chicago: American Library Association.

Greiner, T. 2013. “Hold that Book, But You’re Risking Your Privacy: Guest Opinion.” *Oregonian: Oregon Live*, July 12. http://www.oregonlive.com/opinion/index.ssf/2013/07/hold_that_book_but_youre_riski.html.

Gressel, M. 2014. “Are Libraries Doing Enough to Safeguard Their Patrons’ Digital Privacy?” *Serials Librarian* 67, no. 2: 137–42. https://doi.org/10.1080/0361526X.2014.939324.

Hess, A. N., R. LaPorte-Fiori, and K. Engwall. 2015. “Preserving Patron Privacy in the 21st Century Academic Library.” *Journal of Academic Librarianship* 41, no. 1: 105–14. https://doi.org/10.1016/j.acalib.2014.10.010.

Hoffmann, A. L. 2016. “Privacy, Intellectual Freedom, and Self-Respect: Technological and Philosophical Lessons for Libraries.” In *Perspectives on Libraries as Institutions of Human Rights and Social Justice*, edited by P. T. Jaeger and J. Bertot, 49–69. Bingley, UK: Emerald. https://doi.org/10.1108/S0065-283020160000041003.

Huvila, I., K. Holmberg, M. Kronqvist-Berg, O. Nivakoski, and G. Widén. 2013. “What is Librarian 2.0: New Competencies or Interactive Relations? A Library Professional Viewpoint.” *Journal of Librarianship and Information Science* 45, no. 3: 198–205. https://doi.org/10.1177/0961000613477122.

International Federation of Library Associations and Institutions (IFLA). 2013. “IFLA Trend Report.” http://trends.ifla.org/.

———. 2016. “IFLA Trend Report 2016 Update.” http://trends.ifla.org/update-2016.

Kennedy, B. 1989. “Confidentiality of Library Records: A Survey of Problems, Policies and Laws.” *Law Library Journal* 81, no. 4: 733–67. http://works.bepress.com/aallcallforpapers/51/.

Kwanya, T., C. Stilwell, and P. G. Underwood. 2012. “Library 2.0 Versus Other Library Service Models: A Critical Analysis.” *Journal of Librarianship and Information Science* 44, no. 3: 145–62. https://doi.org/10.1177/0961000611426443.

Lambert, A. D., M. Parker, and M. Bashir. 2015. “Library Patron Privacy in Jeopardy: An Analysis of the Privacy Policies of Digital Content Vendors.” *Proceedings of the Association for Information Science and Technology* 52, no. 1: 1–9. https://www.asist.org/files/meetings/am15/proceedings/submissions/papers/98paper.pdf.

Lankes, R. D., J. Silverstein, S. Nicholson, and T. Marshall. 2007. “Participatory Networks: The Library as Conversation.” *Information Technology and Libraries* 26, no. 4: 17–33. Retrieved from http://www.informationr.net/ir/12-4/colis/colis05.html.

Library Freedom Project. 2017. https://libraryfreedomproject.org/.

Lilburn, J. 2015. “‘Secrets Are Lies’: Academic Libraries and the Corporate Control of Privacy in the Age of Commercial Social Media, a Reading of Dave Eggers’ *The Circle*.” Paper presented at CAPAL15: Academic Librarianship and Critical Practice, Ottawa, Ontario, Canada, May 31-June 2. http://capalibrarians.org/wp/wp-content/uploads/2015/06/2B_Lilburn_paper.pdf.

Litwin, R. 2006. “The Central Problem of Library 2.0: Privacy.” *Library Juice* (blog), May 22. http://libraryjuicepress.com/blog/?p=68.

Lwyoga, E. T. 2013. “Measuring the Success of Library 2.0 Technologies in the African Context: The Suitability of the DeLone and McLean’s Model.” *Campus-Wide Information Systems* 30, no. 4: 288–307. https://doi.org/10.1108/CWIS-02-2013-0011.

Magi, T. 2011. “Fourteen Reasons Privacy Matters: A Multidisciplinary Review of Scholarly Literature.” *Library Quarterly* 81, no. 2: 187–209. http://scholarworks.uvm.edu/cgi/viewcontent.cgi?article=1004&context=libfacpub.

———. 2010. “A Content Analysis of Library Vendor Privacy Policies: Do They Meet Our Standards?” *College & Research Libraries* 71, no. 3: 254–72. http://scholarworks.uvm.edu/cgi/viewcontent.cgi?article=1005&context=libfacpub.

Magi, T., and M. Garnar, eds. 2015. *Intellectual Freedom Manual*, 9th ed. Chicago: American Library Association.

Mahmood, K., and J. V. Richardson. 2013. “Impact of Web 2.0 Technologies on Academic Libraries: A Survey of ARL Libraries.” *Electronic Library* 31, no. 4: 508–20. https://doi.org/10.1108/EL-04-2011-0068.

Mainka, A., A. Hartmann, L. Orszullok, I. Peters, A. Stallmann, and W. G. Stock. 2013. “Public Libraries in the Knowledge Society: Core Services of Libraries in Informational World Cities.” *Libri* 63, no. 4: 295–319. https://doi.org/10.1515/libri-2013-0024.

Maness, J. M. 2006. “Library 2.0 Theory: Web 2.0 and Its Implications for Libraries.” *Webology* 3, no. 2. http://www.webology.org/2006/v3n2/a25.html.

Mannheimer, S., S. W. H. Young, and D. Rossmann. 2016. “On the Ethics of Social Network Research in Libraries.” *Journal of Information, Communication and Ethics in Society* 14, no. 2: 139–51. https://doi.org/10.1108/JICES-05-2015-0013.

Mathiesen, K. 2015. “Human Rights as a Topic and Guide for LIS Research and Practice.” *Journal of the Association for Information Science and Technology* 66, no. 7: 1305–22. https://doi.org/10.1002/asi.23293.

McFadden, R. 1987. “F.B.I. in New York Asks Librarians’ Aid in Reporting on Spies.” *New York Times*, September 18. http://www.nytimes.com/1987/09/18/nyregion/fbi-in-new-york-asks-librarians-aid-in-reporting-on-spies.html?pagewanted=all.

Morgan, C. 2006. “Intellectual Freedom: An Enduring and All-Embracing Concept.” In *Intellectual Freedom Manual*, 7th ed., edited by C. Morgan, 3–13. Chicago: American Library Association.

Murphy, D. 2003. “Some Librarians Use Shredder to Show Opposition to New F.B.I. Powers.” *New York Times*, April 7. http://www.nytimes.com/2003/04/07/us/some-librarians-use-shredder-to-show-opposition-to-new-fbi-powers.html.

———. 2007. “What Is All the Fuss about Library 2.0.” *Law Library Journal* 100, no. 1: 197–204. https://papers.ssrn.com/sol3/papers2.cfm?abstract_id=1022343.

Narciso, D. 2016. “Few Patrons Using Columbus Metropolitan Library’s New Online System.” *Columbus Dispatch*, April 29. http://www.dispatch.com/content/stories/local/2016/04/29/few-patrons-using-columbus-metropolitan-librarys-new-online-system.html.

New York Public Library. 2011. “The New York Public Library and Bibliocommons Partner to Create a New Innovative, Interactive Online Experience.” Press release, June 20. https://www.nypl.org/press/press-release/2011/06/20/new-york-public-library-and-bibliocommons-partner-create-new-innovati.

Olmstead v. U.S., 277 U.S. 438 (1928) (Brandeis, J., dissenting). https://www.law.cornell.edu/supremecourt/text/277/438.

Richards, N. 2013. “The Perils of Social Reading.” *Georgetown Law Journal* 101, no. 3: 689–724. https://georgetownlawjournal.org/articles/134/perils-of-social-reading/pdf.

———. 2015. *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age*. New York: Oxford University Press.

Robbins, L. 1991. “Toward Ideology and Autonomy: The American Library Association’s Response to Threats to Intellectual Freedom, 1939–1969.” PhD diss., Texas Woman’s University, Denton, Texas. https://www.researchgate.net/publication/35558832_Toward_ideology_and_autonomy_the_American_Library_Association’s_response_to_threats_to_intellectual_freedom_1939-1969.

Rustad, M. L. 2016. *Global Internet Law in a Nutshell*, 3rd ed. St. Paul, MN: West Academic Publishing.

Sanchez, R. 2003. “Librarians Make Some Noise over Patriot Act.” *Washington Post*, April 10. https://www.washingtonpost.com/archive/politics/2003/04/10/librarians-make-some-noise-over-patriot-act/91bcbbc6-65a6-41d2-855d-d78b4c7945d2/.

Scardilli, B. 2015. “Four Discovery Services to Watch.” *Information Today*, October 6. http://newsbreaks.infotoday.com/NewsBreaks/Four-Discovery-Services-to-Watch-106716.asp.

Warfield, P. 2015. “Privacy Concerns Abound over BiblioCommons.” *Bay Area Reporter*, January 15. http://ebar.com/openforum/opforum.php?sec=guest_op&id=497.

Wójcik, M. 2015. “The Use of Web 2.0 Services by Urban Public Libraries in Poland: Changes Over the Years 2011-2013.” *Libri* 65, no. 2: 91–103. https://doi.org/10.1515/libri-2015-0017.

Zimmer, M. 2008. “Preface: Critical Perspectives on Web 2.0.” *First Monday* 13 (3). Accessed March 15, 2017. http://firstmonday.org/article/view/2137/1943.

———. 2013a. “Assessing the Treatment of Patron Privacy in Library 2.0 Literature.” *Information Technology and Libraries* 32, no. 2: 29–41. https://ejournals.bc.edu/ojs/index.php/ital/article/viewFile/3420/pdf.

———. 2013b. “Patron Privacy in the 2.0 Era: Avoiding the Faustian Bargain of Library 2.0.” *Journal of Information Ethics* 22, no. 1: 44–59. https://doi.org/10.3172/JIE.22.1.44.

———. 2014. “Librarians’ Attitudes Regarding Information and Internet Privacy.” *Library Quarterly* 84, no. 2: 123–215. https://doi.org/10.1086/675329.

Protecting Patron Privacy: A LITA Guide

Editors _ **Bobbi Newman and Bonnie Tijerina**
Publisher _ Rowman & Littlefield, 2017. 152 p. Hardcover $90. ISBN: 978-1-4422-6969-9
Reviewer _ **Rudy Leon**, Evoke: Words for Hire

Libraries have long been committed to protecting patron records, but it might be said that we have not kept up with the technologies that challenge that commitment. I attended library school immediately following the passage of the USA PATRIOT ACT, and the conversations at the time were still surrounding circulation records. Fifteen years later, *Protecting Patron Privacy: A LITA Guide* (edited by Bobbi Newman and Bonnie Tijerina) makes a timely and essential entrance on the scene. The material covers basics (privacy law in the United States and library interpretations and applications), ethics, a discussion of how third-party systems trade information across systems, and it provides ideas for training staff and patrons. It is both a useful textbook for students pursuing their MLS degrees and an essential primer for all library workers. It is also written (mostly) in a manner very accessible to nontechnical public services people (at least, to this one).

The book most focuses on four topics: (1) foundations of privacy law and implementation of privacy practices in libraries; (2) ethics of library patron data collection and use; (3) third-party systems and their impacts on library patron privacy; and (4) training staff and patrons for more effective privacy protections. The chapters vary between being practical, theoretical, and descriptive. I find the balance works for the individual topics under discussion.

The four sections of the book are clearly organized and mostly excellent. The one exception is "Third-Party Services in Libraries" by William Marden. The material is too dense and not explained at the level of the majority of the book. My sense is that this chapter suffers from trying to force what should be a book in its own right into a single chapter précis. In its current state, the chapter raises more questions than it answers, but it certainly stands as enough of an introduction to allow readers to effectively research any questions they develop over the course of the reading. The subject matter is worthy of expansion, and I hope Marden will consider book-length treatment of the material.

Matt Beckstrom's "Use, Security, and Ethics of Data Collection: Data Collection, Retention, Use, and Security" is an example of one of the highly descriptive chapters. Beckstrom provides information I personally have long wished to have—a narrative map of how library tools interact with each other and with third-party systems, identifying where patron information might pass from system to system, vendor to vendor. The elucidation of these complex systems, in a manner accessible to people who never work with the technical side of library systems, is incredibly valuable. I suspect this value is also present for many library staff working on the technical side. This chapter alone allows for asking more informed questions of our vendors and ourselves.

In addition to the excellent coverage of the material, Beckstrom's chapter also excels at laying out one of the primary concerns of the book: that librarians interested in patron privacy recognize that privacy must be protected with decisions at the levels of collection, retention, and use, as well as how we share information about our patrons inadvertently or through ignorance.

The remaining chapters are all quite good. "Foundations of Privacy in Libraries" (Michael Zimmer and Bonnie Tijerina) and "Privacy Law and Regulation" (Michael Zimmer and Deborah Caldwell-Stone) should become required readings in Library Foundations courses. The chapters providing examples of staff and patron privacy training, "Privacy Training for Staff and Patrons: The Data Privacy Project at Brooklyn Public Library" (Melissa Morrone) and "Privacy Training for Staff and Patrons: Privacy Initiatives at The City University of New York (CUNY)" (Martha Lerski and Stefanie Havelka), were inspiring, so much so that I began designing workshops of my own after reading them. This book lends itself to that kind of practical action.