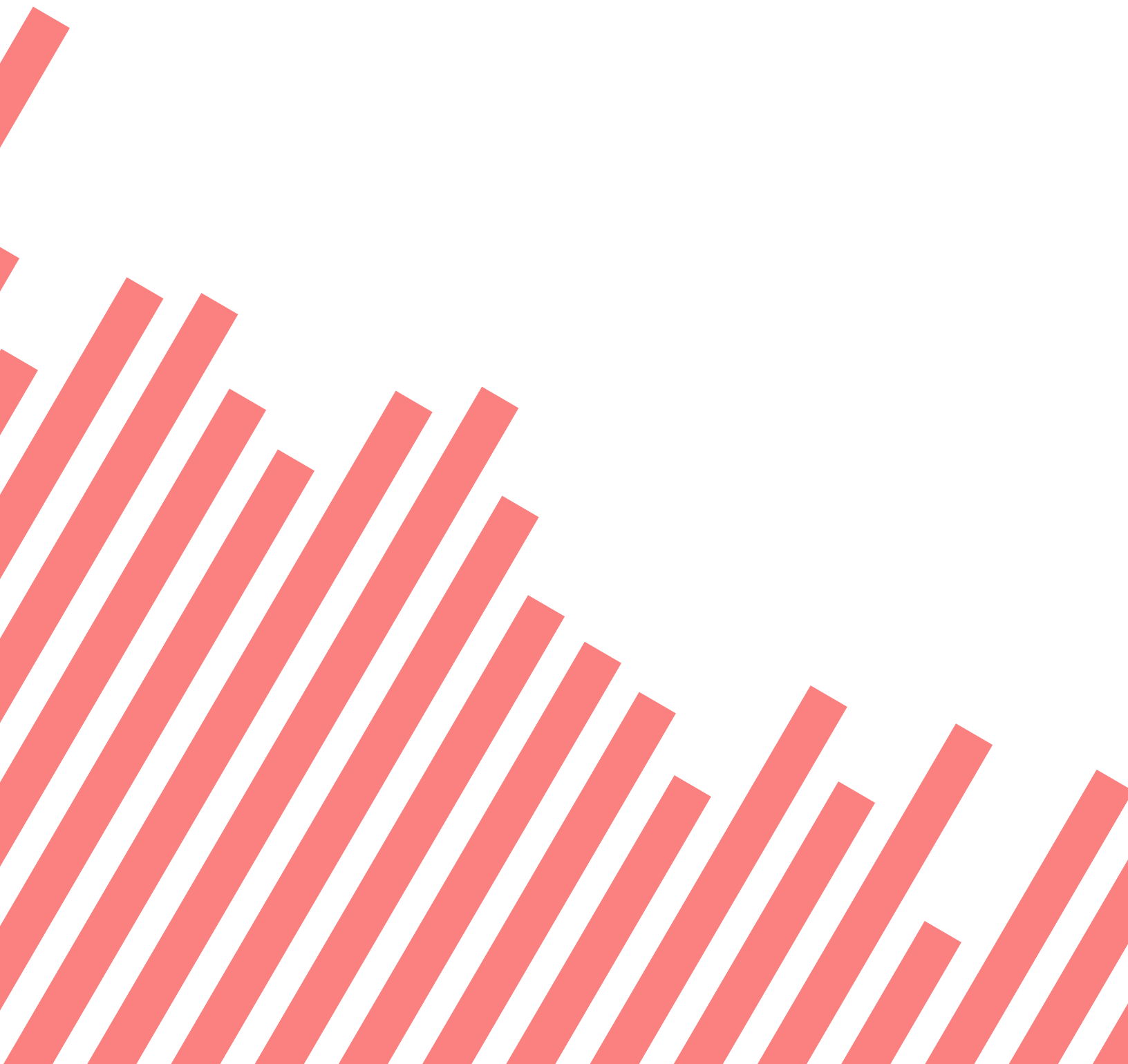


# **Research Library Issues**

## RLI 297: The Current Privacy Landscape

2019

/ ASSOCIATION  
OF RESEARCH  
LIBRARIES /



## In This Issue

<b>Introduction</b>	<b>3</b>
<b>Reader Privacy: The New Shape of the Threat</b>	<b>7</b>
Introduction	
Fundamental Reader Privacy Threat Scenarios	
Disclosure by the Library	
Collection by Third Parties	
Library Analytics: An Emerging Dilemma	
The Most Important Steps to Take Now	
<b>Legal Landscape of Consumer/User Data Privacy and Current Policy Discussions</b>	<b>15</b>
Introduction	
Current Privacy Landscape in the United States	
International Privacy Developments	
On the Horizon in the United States	
The Upshot	
<b>Privacy in Public Libraries</b>	<b>38</b>
Foundations of Privacy in Libraries	
New Technology and Privacy	
Current Projects	
NYPL Initiatives	
Conclusion	

## Introduction

**Mary Lee Kennedy**, Executive Director, Association of Research Libraries

Recently, the *New York Times* began The Privacy Project to explore privacy in contemporary life. The opening sentences are:

Companies and governments are gaining new powers to follow people across the internet and around the world, and even to peer into their genomes. The benefits of such advances have been apparent for years; the costs—in anonymity, even autonomy—are now becoming clearer. The boundaries of privacy are in dispute, and its future is in doubt.<sup>1</sup>

This is not new to most readers, but it reflects a broader public discussion about what we know to be true—the idea of privacy as we once knew it is in flux.

In this first issue of *Research Library Issues* (*RLI*) in 2019, the authors explore privacy from a legal, digital, and applied perspective, with a focus on the implications and opportunities for research libraries. The current privacy landscape highlights the need for a nuanced understanding of the complicated nature of privacy today. Research libraries need to collaborate with other privacy-related constituents within institutions and in the public policy and legislative arenas, and act as trusted institutions within a democratic society. The Association of Research Libraries (ARL) places privacy in the top tier of its priorities for advocacy and public policy. We hope this issue of *RLI* will help the reader identify institutional privacy policies and practices to investigate and adopt amid changes in the interfaces between users and information, and within the broader context of the US and international policy landscape.

“The idea of privacy as we once knew it is in flux.”

Not a day goes by without news of data breaches, and coverage related to consumer, student, and institutional privacy policy and

practices. Privacy is a topic of prime importance for our partners in higher education, government, and civic society—represented by its relationship to learning analytics, freedom of speech, the right to be forgotten, disinformation, and algorithmic bias. Research libraries may find themselves in a challenging position to educate users in a complex context, collaborate with peers on policy and practices, and influence decision-makers. The situation is complicated by users' expectations of convenience and varying expectations of confidentiality, and decision-makers' expectations of impact measures, timely outcomes, and risk management. **Clifford Lynch**, executive director of the Coalition for Networked Information, highlights three categories of threat for research libraries to understand, and concludes with recommendations on the most important steps to take now. He emphasizes the importance of institutional partnerships in doing so.


There is an increased interdependence of privacy laws worldwide, as evidenced by the European Union's General Data Protection Regulation, the Canadian privacy hearings, and US federal and state laws. This interdependence is at least partially driven by the increased sophistication of global digital data collection practices by both for-profit and nonprofit organizations. As a result, the legislative, regulatory, and public policy privacy landscape is in motion in the United States, Canada, and internationally—with uncertain yet ongoing discussion, now specifically focused on consumer privacy. As a collaborative partner in the research and learning ecosystem, research libraries have an opportunity to shape, inform, and ensure their institutions' policies and practices, as well as to participate in broader public policy discussions—recognizing that there are no easy answers. **Krista Cox**, director of public policy initiatives at ARL, provides the reader with an update on the current US and international privacy context—highlighting the patchwork nature of the US privacy landscape and the federal approach to privacy in Canada. She provides the background to potential for change in the US in 2019. Cox includes guidance on how research libraries can evaluate the current US discussion on consumer privacy as they consider convenience over

privacy as a value, something that will most certainly impact the research and learning community.

Ultimately each research library must develop and implement privacy policies and practices within its own institution. Research libraries partner, or may lead, in institutional policy development—usually requiring the creation of a clear and shared understanding of digital and physical privacy decision implications among key stakeholders, including boards, staff, and users. On a day-to-day basis staff need the knowledge of privacy practices in order to assist users, and as needed, evaluate, explain, and act on, privacy events. Privacy practice requires policy compliance in any physical and digital interaction—and with that the institutional capacity to assess and address compliance.

**Bill Marden**, director of privacy and compliance, and **Greg Cram**, associate director of copyright and information policy, both at The New York Public Library, share important distinctions between privacy and confidentiality, and how New York City public libraries and national endeavors are assisting with privacy policy and practice.

We hope you find useful knowledge on privacy in this issue, and we thank the authors for sharing their expertise with you.

A handwritten signature in grey ink, appearing to read 'MLK' followed by a stylized flourish.

Mary Lee Kennedy

## Endnote

1. The Privacy Project, *New York Times*, accessed April 29, 2019, <https://www.nytimes.com/interactive/2019/opinion/internet-privacy-project.html>.

© 2019 Mary Lee Kennedy



This article is licensed under a Creative Commons Attribution 4.0 International License. To view a copy of this license, visit <https://creativecommons.org/licenses/by/4.0/>.

**To cite this article:** Mary Lee Kennedy. “Introduction.” *Research Library Issues*, no. 297 (2019): 3–6. <https://doi.org/10.29242/rli.297.1>.

## Reader Privacy: The New Shape of the Threat

**Clifford A. Lynch**, Executive Director, Coalition for Networked Information

### Introduction

This essay briefly summarizes the current range of threats to reader privacy and makes some high-level suggestions that research library leadership might consider to address them. It is not comprehensive, and does not go into much technical detail; those interested in a place to start might see my paper “The Rise of Reading Analytics and the Emerging Calculus of Reader Privacy in the Digital World,”<sup>1</sup> keeping in mind that it’s now two years out of date.

I also note recent projects funded by the Institute of Museum and Library Services intended to provide guidance for libraries of all types: Library Values and Privacy in Our National Digital Strategies<sup>2</sup> and the National Forum on Web Privacy and Web Analytics,<sup>3</sup> as well as a very recent and welcome statement of principles in a posting by Mimi Calter of Stanford University on *The Scholarly Kitchen*.<sup>4</sup> These may also be helpful.

### Fundamental Reader Privacy Threat Scenarios

Threats to reader privacy fall into three major categories.

The first is eavesdropping on the interactions between a reader and various systems that help the reader to discover and obtain information. To a first approximation, in the digital world this can be effectively addressed by routine (but properly configured!) encryption of such interactions. Surprisingly, as recently as, say, four years ago, implementation of this strategy was relatively rare and libraries had been slow to demand it from vendors. Today such encryption is becoming increasingly commonplace, particularly in research libraries. I shall not consider this further here.

The second threat is disclosure of information that the library is holding about what a patron is reading, perhaps through legal mechanisms (subpoenas or national security letters, for example), or because the library is hacked; it might even be due to accidental misconfiguration of a library system. Aspects of this threat have been a concern since long before libraries computerized their operations—and that was a long time before digital content became dominant.

The third category of threat, which is new to the age of digital content, involves data that is collected by **external** vendors who provide licensed content to libraries (and indeed, also external suppliers of content that is “freely” available, subject to click-through terms and conditions). This is, in my view, the least understood and most dangerous threat to reader privacy today.

### **Disclosure by the Library**

Libraries have addressed this threat on several levels. The first is a recognition that they can’t disclose information that they don’t have, so they have typically collected as little as possible, and retained it for as short a period as possible (for example, only while a book is out on loan is the loan tracked)—notably, often, with the exception of special collections. The second is to be as rigorous as possible in defending disclosure of information that they do hold, particularly legally. I am less confident that library systems are subjected to the same kind of periodic and rigorous security requirements and audits that are now commonplace for various kinds of enterprise administrative systems; these are expensive and time-consuming, and also tend to increase the overhead costs of running systems. This is an area where at least an exploratory conversation with your IT leadership may be informative.

It can be very challenging to be confident that you are collecting as little information as possible and retaining it for as short a time as possible. There are backups, and there are logs at various levels. Even if you are anonymizing logs it may be possible to re-identify them in various ways, so one should be very cautious about relying on anonymization.



Finally, it's important to recognize that taking an absolutist approach to information collection, as opposed to more nuanced, transparent, and opt-in collection of data about user activities and interests, has meant that library systems appear to the user as far inferior to commercial offerings; they are unable to make recommendations to users, or to remind them of past history. I believe that re-assessing these choices is long overdue, but doing so will further demand that libraries carry out a much more complex and subtle risk assessment; it will also challenge them to convey the implications and risks of various choices to their patrons.

“I am less confident that library systems are subjected to the same kind of periodic and rigorous security requirements and audits that are now commonplace for various kinds of enterprise administrative systems.”

### **Collection by Third Parties**

Third-party platforms offer access to various databases or collections of content such as journal articles. The platform providers know a tremendous amount of information about **what** is being read, and the patterns of reading. Particularly to the extent that they can associate this information with **who** is doing the reading, they have frighteningly detailed data. Even if they can't associate it with a given individual by name, there is still potential power in knowing that someone at a specific institution, or perhaps in a specific department within that institution, is following a specific trail of information over time.

These platform operators can do various things with the information they collect, potentially: in addition to using it for their own purposes, they could share it with others, or resell it. Furthermore, it is subject to disclosure—by legal means, by hacking, or by human error. There are no a priori limits to how long this data can be retained, and normally, if control of a company changes (through acquisition or bankruptcy, for example), the data is just one more corporate asset.

It's also worth noting that there are really two layers of attack on privacy on these external platforms. Not only can the platform operators collect data themselves, but they also sell advertising in most cases, which means that they are also contributing participants in the gigantic internet surveillance apparatus for monetizing users, in much the same way as online newspapers (which also use a mixed advertising and subscription model).

For licensed resources, language in contracts can address all of these issues: limit or forbid data collection, retention, reuse, and redistribution; include criteria about how that data is protected, both legally and technically; forbid third-party advertising.

However, some limited surveying suggests that, as of at least two years ago, contract language dealing with these points was relatively rare. It

“In situations where vendors will not accept contract language regarding reader privacy, institutions will need to make choices about what minimal levels of privacy assurance are acceptable before they walk away.”

is also unclear how resistant content providers are to such language. An examination of the posted privacy policies of some of the major content providers does not inspire confidence in the absence of specific overriding contractual stipulations. It would be very useful to have some more

current data about research library contractual practices in this area, and perhaps also to have model language available. In situations where vendors will not accept contract language regarding reader privacy, institutions will need to make choices about what minimal levels of privacy assurance are acceptable before they walk away.

For resources that the library does not license (but that their patrons may rely on for various purposes), there's not much that the library can do other than help their users to understand terms and conditions, privacy policies, and risks. But doing this is an important part of improving digital and information literacy.

It's also important to explicitly recognize a large class of online learning materials and electronic textbooks as potential environments for massive data collection as well. Here, historically, the library hasn't been involved in the licensing process or terms, and it's often extremely unclear whether student privacy is even being considered, much less protected, or whether data that would be helpful to the university for various reasons is actually being made available to the institution (or what happens to it if it is made available). Unlike research materials, students often have no choice about using these educational resources. My expectation is that, for many reasons (escalating costs, privacy liability, the uptake of open educational resources, etc.), libraries are going to become much more involved in these arrangements going forward. They have a great deal of expertise to bring, not just in privacy but also in other areas, such as preservation and archiving. The current ways in which most institutions select and contract for these resources is deeply problematic and overdue for re-examination.

One of the biggest questions in understanding data collection by third parties is whether they can identify individual users accessing their platform. Even today, a great deal of authentication of users is done via proxy servers, which verify that a user is a member of a given university community and, once validated, pass that user (and all other validated users) on to external services from a common address known to the external service as only sending validated traffic.

Ever since proxy servers came into use in the 1990s (indeed, there are forms of proxies that pre-date the web), there has been a belief that this process effectively anonymized traffic to external services and, hence, rendered the reader privacy issue largely moot as long as proxies were employed. This was probably at least generally true in the early days of the web. More than 20 years later, the various technologies for user tracking and re-identification have advanced greatly, fueled by the demands of various advertising and data collection platforms. It would require a very careful, determined, and sophisticated user to have much hope of avoiding tracking and re-identification today, with or without

the intercession of a proxy service—hence the need to address the problem contractually.

There are other authentication technologies in use. Most notably, there is Shibboleth, which many universities use with major content suppliers. Here, the data that the institution passes to the third party about a given user is determined by the institution's attribute release policies. There have been

instances where institutions were releasing very specific, individually identifying information to external platforms as standing policy. If your institution is using Shibboleth to handle authentication for licensed content, it's vital that you understand the details of this attribute release policy and that your users understand it as well. If you've not had this conversation with your institution's IT policy leadership, it's past due.

Note that the experimental RA21 initiative is really, as I understand it, just an effort to make Shibboleth a bit less cumbersome to use. From a reader privacy perspective, it's no better and no worse than the local Shibboleth implementation, though I know it's been viewed by some with considerable suspicion.

### **Library Analytics: An Emerging Dilemma**

As the costs of digital content continue to increase and library budgets are stretched, it's very valuable for libraries to have good data about what's actually being used, and who (individually or demographically) is using it. Libraries are also being pressured to demonstrate impact, particularly with regard to student outcomes. Indeed, there have been some uncomfortable conversations between institutional leadership determined to develop the most powerful analytics for predicting student outcomes, and library leadership unwilling to collect and supply some of the data that the analytics developers would like to have.

“Libraries are going to need to think very carefully about what data they want to collect and what risks it represents.”

Libraries are going to need to think very carefully about what data they want to collect and what risks it represents. Then they will need to consider how to inform their users about what is being collected, how it is being used, and where the data collection is going to happen. They may need to share some additional information (role, school, or departmental affiliation, for example) about users with external platforms if they want the platform to return usage data faceted by those attributes. Emerging techniques and technologies, such as differential privacy, may ultimately prove very helpful here.

### **The Most Important Steps to Take Now**

This brief paper suggests many issues that library leadership needs to consider with regard to reader privacy, but three stand out to me as most urgent:

1. If you are using Shibboleth for authentication to external content platforms at your institution, be sure that you understand your institution's attribute release policy and the governance around the development and maintenance of that policy.
2. As new licenses for content and services are established, or as existing ones are renewed, add language dealing with reader privacy as a routine matter.
3. Develop a strategy and a program for informing and educating the university community about reader privacy issues broadly. In my view, this is ideally done by the library in partnership with other organizations (such as information technology, general counsel, registrar, instructional technology, etc.) in a coordinated and holistic way. In any event, it's essential that this communication be put in place sooner rather than later, even if the library must act alone for a time while an effort is being made to develop a more strategic institution-wide conversation about the issues.

## Endnotes

1. Clifford A. Lynch, “The Rise of Reading Analytics and the Emerging Calculus of Reader Privacy in the Digital World,” *First Monday* 22, no. 4 (April 3, 2017), <https://doi.org/10.5210/fm.v22i4.7414>.
2. “Project Report: ‘Library Values & Privacy in Our National Digital Strategies: Field Guides, Convenings, and Conversations,’ ” Center for Information Policy Research, University of Wisconsin–Milwaukee, August 2, 2018, <https://cipr.uwm.edu/2018/08/02/project-report-library-values-privacy/>.
3. “National Web Privacy Forum,” Montana State University Library, accessed April 28, 2019, <https://www.lib.montana.edu/privacy-forum/>.
4. Mimi Calter, “Guest Post—Protecting Patron Privacy in Digital Resources,” *The Scholarly Kitchen*, March 13, 2019, <https://scholarlykitchen.sspnet.org/2019/03/13/guest-post-protecting-patron-privacy-in-digital-resources/>.

© 2019 Clifford A. Lynch



This article is licensed under a Creative Commons Attribution 4.0 International License. To view a copy of this license, visit <https://creativecommons.org/licenses/by/4.0/>.

**To cite this article:** Clifford A. Lynch. “Reader Privacy: The New Shape of the Threat.” *Research Library Issues*, no. 297 (2019): 7–14. <https://doi.org/10.29242/rli.297.2>.

## Legal Landscape of Consumer/User Data Privacy and Current Policy Discussions

**Krista L. Cox**, Director of Public Policy Initiatives, Association of Research Libraries

### Introduction

Privacy has long been deemed an essential right, but this right has been threatened by current practices in the digital era, in which vast swaths of data are collected from individuals each day. Although privacy is not directly mentioned in the United States Constitution, courts, including the Supreme Court of the United States, have recognized a right to privacy based on the First, Fourth, and Fourteenth Amendments. Additionally, numerous states explicitly provide for a right to privacy in their constitutions or through state laws. Privacy, which was famously defined as a right to be left alone,<sup>1</sup> relates to a number of areas of everyday life, including family, health, and—of particular importance to library—the ability to seek and impart information.

The American Library Association’s (ALA) Library Bill of Rights explicitly recognizes that, “All people, regardless of origin, age, background, or views, possess a right to privacy and confidentiality in their library use. Libraries should advocate for, educate about, and protect people’s privacy, safeguarding all library use data,

“Privacy, which was famously defined as a right to be left alone, relates to a number of areas of everyday life, including...the ability to seek and impart information.”

including personally identifiable information.”<sup>2</sup> In interpreting this right, ALA defines privacy in the library context as “the right to open inquiry without having the subject of one’s interest examined or scrutinized by others.” ALA widely applies the right to privacy to search records,

reference questions, circulation records, and personally identifiable information about uses of services and materials. ALA also notes, “best



practice leaves the user in control of as many choices as possible” and that libraries should refrain from sharing personally identifiable information with third parties or vendors without permission from the users.<sup>3</sup>

While patron privacy has long been a fundamental value to libraries, the digital world complicates traditional notions of privacy because of the vast amounts of data collected when users encounter technology. In the digital age, research libraries are tasked with addressing broader privacy concerns than in the analog world because they must account for more than the records libraries themselves create and keep, but also the personal data that may be collected by services, applications, and vendors that libraries work with. Indeed, this personal data can prove valuable for third-party vendors and services, but also for libraries seeking to enhance user experience. Libraries today must carefully consider how to balance core values of privacy—and the inherent trust that is placed in them by patrons—with improved delivery of service to their users.

“Libraries today must carefully consider how to balance core values of privacy...with improved delivery of service to their users.”

As libraries evaluate best practices to protect patron privacy in the digital era and policy makers determine how to move forward with legislation to protect consumers, it is clear that there are no easy answers. All stakeholders and policy makers in the privacy debates must consider a range of complicated issues. Some of the biggest issues to consider in determining what elements should be included in a comprehensive, consumer privacy regime are:

- **How broadly should the law apply?** In order to avoid the current problems with the sectoral approach, a comprehensive solution must address broader privacy issues. Stakeholders in the privacy debate have differed as to whether federal privacy laws should apply solely to the technology sector or to all companies;



whether federal laws will only apply to companies of a certain size, in order to ensure that compliance costs are not overly burdensome for new entrants to the market; whether there should be carve outs for certain types of companies or data.

- **What types of data will the law apply to?** Policy makers must determine whether to create different classes of data or treat specific types of consumer data differently. While some advocate for “sensitive” data, such as medical data, to have heightened protections, others note that with interconnected systems and the ways data is shared today, such distinctions may be meaningless. Additionally, many advocates have raised concerns about the use of de-anonymized data, pointing to studies that have precisely identified individuals or connected users with personal information through aggregation of supposedly anonymous information.
- **What rights will be guaranteed?** From the outset, policy makers must determine which rights a federal bill will cover. While the right to information or transparency seems to be non-controversial, will consumers have rights to access, portability, correction, restriction, erasure, minimization, and objection? How broadly will these rights be framed and to what type of data will it apply? What exceptions might exist to these rights? From a library perspective, a right to erasure/deletion, which in the European Union (EU) is also framed as a right to be forgotten, raises particular concerns with respect to accurately preserving the cultural and historical record. The right to be forgotten has inherent tensions with the First Amendment rights under the United States Constitution and also raises ethical concerns. The right to delisting, meaning that it cannot be indexed in a search engine, is a related concern which alters accessibility and discoverability of the information.
- **What do meaningful notice, transparency, and consent mean?** While all stakeholders appear to agree that notice and

transparency are critical features of any privacy law, in order to make these elements meaningful, users must be able to easily access and understand what data is being collected and how it is being used prior to such collection. One issue that has been hotly debated is whether opt-out systems should satisfy consent requirements, or whether default opt-in provisions should be required. Another question is whether terms of service that are framed as a take-it-or-leave-it policy allow for meaningful consent.

- **Who will enforce the legislation and what remedies should be provided?** Most stakeholders agree that the Federal Trade Commission (FTC) is the most logical agency to enforce violations of a federal consumer privacy framework. Indeed, bills such as Senator Ron Wyden's draft (discussed more below), would provide for increased hiring at the FTC to investigate and enforce violations. The fines that the FTC could impose and whether criminal sanctions are appropriate are issues that policy makers will debate. Additionally, policy makers must determine whether to leave enforcement solely in the hands of government agencies, or whether to create a private right of action that allows citizens to bring companies to court for failure to comply with federal privacy laws.
- **What safe harbors should be granted to companies for complying with legislation?** Depending on the remedies provided in federal legislation, some stakeholders have noted that safe harbors may be necessary to provide assurances for companies that, as long as they comply with particular requirements, they will not face extensive penalties for security or other breaches.
- **Should the federal baseline be a floor or ceiling?** Preemption is another issue that policy makers must confront and determine whether any federal legislation should be a floor or a ceiling. If federal legislation serves as a ceiling, states would be prohibited

from enacting more stringent rules. Should federal legislation fail to provide meaningful data protection, states may wish to provide further privacy protections for their citizens. However, by allowing states to create stronger privacy rules, companies and organizations will continue to run into a patchwork system.

- **Will federal legislation provide incentives for privacy research and development?** Some advocates for a federal framework have urged for inclusion of incentives for cybersecurity research and development of new models to address privacy concerns. Some have noted that incentives for companies to proactively protect data and prevent security breaches will better serve consumers than systems that simply rely on notice or after-the-fact disclosures.

As will be discussed further below, there are no easy answers nor consensus around these issues. However, stakeholders and policy makers are determined to move discussions around privacy forward, with many holding an ultimate goal of creating new legislation in the United States in 2019.

## **Current Privacy Landscape in the United States**

### *Federal Approach to Privacy*

The legal privacy landscape in the United States currently can be described as a patchwork system, at best, that relies on sector-specific federal laws and widely divergent state legislation. The United States does not currently have a comprehensive consumer privacy law, meaning that different types of data are treated differently and there is no baseline standard for consumers to expect protection of personally identifiable information. Privacy laws currently existing at the federal level are sector-specific, such as the Health Insurance Portability and Accountability Act (HIPAA) covering protected health information, or the Family Education Rights and Privacy Act (FERPA) covering certain student records, or the Gramm-Leach-Bliley Act covering consumers' financial information. This sectoral approach, however,

creates compliance problems, with different classes of data and varying standards of privacy. It also results in gaps and inconsistencies regarding how the same data may be treated, depending on where it is shared or conveyed. Many policy makers have expressed an interest in addressing these gaps through enactment of comprehensive federal privacy legislation.

While there appears to be an increased interest and urgency in creating a federal standard, it should be noted that the FTC has repeatedly called on Congress to enact comprehensive privacy laws to protect consumers for nearly two decades.<sup>4</sup> The FTC has long advocated federal regulation, in part because the Fair Information Practice Principles (FIPPs) are principles and not enforceable as law, though the commission can police certain behavior deemed unfair or deceptive. While FIPPs provide an excellent starting point as guiding principles for companies engaged in data collection, compliance is largely voluntary. As a result, the United States has largely relied on market mechanisms to protect consumer privacy. In other words, the US has operated under the assumption that if consumers were unhappy about privacy policies or data collection practices, companies would be forced to change. Unfortunately, reliance on market corrections has not resulted in the changes that users would like, in part because privacy policies or terms of services are often hidden, not accessible until after signing up for the platform, or are lengthy and legalistic documents that do not plainly explain data collection practices. Users often do not fully understand what data is collected, how it is used, who else can view it, or whether they can opt-out.

“The legal privacy landscape in the United States currently can be described as a patchwork system, at best, that relies on sector-specific federal laws and widely divergent state legislation.”

In 2012, the Obama Administration released its report, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*,<sup>5</sup> largely based on

FIPPs. The purported intention behind the report's release was to call on Congress to enact the Consumer Privacy Bill of Rights contained within the paper into legislation. President Obama noted in the report:

Never has privacy been more important than today, in the age of the Internet, the World Wide Web and smart phones. In just the last decade, the Internet has enabled a renewal of direct political engagement by citizens around the globe and an explosion of commerce and innovation creating jobs of the future. Much of this innovation is enabled by novel uses of personal information. So, it is incumbent on us to do what we have done throughout history: apply our timeless privacy values to the new technologies and circumstances of our times....

One thing should be clear, even though we live in a world in which we share personal information more freely than in the past, we must reject the conclusion that privacy is an outmoded value. It has been at the heart of our democracy from its inception, and we need it now more than ever.<sup>6</sup>

Ultimately, Congress did not act on the Obama Administration's report and the United States still lacks comprehensive consumer privacy protections.

The FTC does oversee internet privacy through its authority over "unfair or deceptive acts or practices in or affecting commerce."<sup>7</sup> These FTC cases generally result in a settlement with the companies due to the lack of authority to impose civil penalties unless the company has violated an existing FTC order.

### *State Approach to Privacy*

While states each have their own privacy laws, these laws are often older, do not address the swaths of data that exist in the digital age, or are limited in scope. Like the federal approach, where states have enacted laws addressing privacy in the digital environment, they are generally narrowly focused and target discrete populations or are sector-specific. For example, California and Delaware have

specific laws aimed at protecting the privacy of minors.<sup>8</sup> Many states, including Arizona, California, Delaware, and Missouri have specific laws governing e-reader privacy, which vary from protecting library

“While states each have their own privacy laws, these laws are often older, do not address the swaths of data that exist in the digital age, or are limited in scope.”

patron records to more generally applying to all e-book browsing, including from commercial bookstores.<sup>9</sup> Several states, including California, Connecticut, Delaware, Minnesota, Nevada, and Oregon, also address privacy policies for websites or for personal information held by internet service providers. All states now have some form of data breach notification laws, and some

states have amended these rules in recent months. While these states have addressed important issues related to online privacy, with the exception of California’s recently enacted privacy legislation, these laws do not comprehensively address consumer data collected during the everyday course of using online services, platforms, and applications.

More recently, attention to comprehensive consumer privacy has increased as a result of the European Union’s General Data Protection Regulation (GDPR) (discussed in greater detail below). Soon after GDPR went into force, California quickly enacted the California Consumer Privacy Act of 2018 (CCPA).<sup>10</sup> This bill, scheduled to go into effect in 2020, purports to follow GDPR in many respects, but is narrower in scope than its EU counterpart and has come under a wave of criticism from nearly all stakeholders involved. CCPA focuses on the collection of data and—in contrast to GDPR—limits its application only to certain companies: those with gross revenue exceeding \$25 million, or that sell data on more than 50,000 consumers each year, or derive 50% or more of their revenue from selling personal data. Ultimately, many criticized the rush to enact the legislation, with virtually no time for close analysis or meaningful debate.



From a consumer advocacy perspective, CCPA has been criticized as a weakened version of GDPR, heavily relying on notice provisions, rather than requiring consumers to opt-in to data collection and processing; for providing only limited availability to data portability; for including at least a limited right to deletion or right to be forgotten; for applying only to a specific definition of “businesses”; and, in some respects, for lacking appropriate enforcement mechanisms. On the other hand, some have criticized CCPA as overly expansive in its application by eliminating the distinction between sensitive and non-sensitive personal information or by requiring high costs for compliance, thereby disadvantaging smaller technology companies.

While other states do not have comprehensive consumer privacy legislation in place, several are reportedly considering it.<sup>11</sup> Washington State, for example, is currently considering the Washington Privacy Act.<sup>12</sup> This bill would apply to personally identifiable data, but largely excludes de-identified data. It includes provisions on the right to access, the right to delete and the right to opt-out. It also specifically governs facial recognition technology. The Washington Privacy Act, as currently drafted, would empower the state Attorney General’s office to enforce its provisions, but would not create a private right of action for consumers. Regardless of the provisions that might be included if the Washington Privacy Act becomes law, it is clear that there would be stark differences between this bill and CCPA, as well as GDPR. Other state legislation is also likely to have small and large differences, resulting once again in a patchwork of state provisions governing different aspects of consumer data, with different standards of protection.

### **International Privacy Developments**

Consumer data privacy has been a topic of active discussion internationally, as well. Most notably, in 2018, the EU’s General Data Protection Regulation (GDPR) went into effect and has resulted in a domino effect in terms of compliance by private businesses as well as new legislation in other countries.

Although GDPR applies to EU citizens and residents, it affects companies and organizations worldwide both because of ties to those in the EU, as well as the practical difficulties in handling EU personal data differently from personal data collected in other parts of the world. GDPR grants individuals six specific rights with respect to their data:

1. Information and access (the right to know that their personal data is being processed and have access to this data free of charge)
2. Data portability (data collected under certain circumstances must be provided “in a structured, commonly used, and machine-readable form”)
3. Rectification (ability to correct inaccurate personal data or to complete information)
4. Erasure (also known as the “right to be forgotten,” applicable only under certain circumstances)
5. Restriction (individuals may restrict data controller from processing data further under certain circumstances)
6. Objection (the right to object to processing of one’s data)

Significantly, GDPR requires explicit consent from the user for collection and processing of data in an opt-in system, rather than simply allowing individuals to opt-out. As Anne T. Gilliland notes, the enactment of GDPR matters to companies and libraries worldwide: “Because of their various ties to Europe and EU citizens, such as exchange programs, study abroad opportunities, visiting scholars, and satellite campuses in other countries, universities and research libraries are among the organizations that now must come to terms with the GDPR’s requirements.”<sup>13</sup>

As a result of GDPR, other countries, such as Canada, Argentina, Brazil, Israel, and Japan, have enacted similar privacy legislation that is at least compatible with the EU’s approach.<sup>14</sup> Canada, for example, updated



the Personal Information Protection and Electronic Documents Act (PIPEDA), which has governed data privacy since 2000.<sup>15</sup> While the updates included amendments regarding data security breaches, Canada is considering more sweeping changes. The Standing Committee on Access to Information, Privacy and Ethics published the report, “Addressing Digital Vulnerabilities and Potential Threats to Canada’s Democratic Electoral Process” recommending additional amendments to PIPEDA, in line with GDPR.<sup>16</sup> In 2018, the Canadian government held national digital and data consultations, including roundtables in Ottawa, Vancouver, Calgary, Regina, Winnipeg, Waterloo, Toronto, Ottawa, Montreal, Quebec, Fredericton, Charlottetown, Halifax, St. John’s, and Whitehorse, in addition to a roundtable in Silicon Valley in the United States.<sup>17</sup> However, legislation has not yet been introduced in Canada to create a GDPR-like law.

“In 2018, the EU’s General Data Protection Regulation (GDPR) went into effect and has resulted in a domino effect in terms of compliance by private businesses as well as new legislation in other countries.”

Because companies, even those based outside the EU, may interact with those in the EU and must comply with GDPR, it is easier to take a uniform approach to data collection. As the months following GDPR’s effective date demonstrate, one natural result has been an effort in several countries to update their own privacy laws to ensure a compatible standard. The growing number of countries adopting GDPR-like laws places the United States as an outlier because of the lack of comprehensive, uniform privacy laws. Without comprehensive federal legislation, the United States risks losing credibility and leadership on the issue of privacy.

### **On the Horizon in the United States**

The interest in protecting consumer privacy in the United States likely stems from a number of events. First, as a practical matter, the notice-and-consent regime that has formed the basis for many services

and platforms is proving inadequate in a growing digital economy. It is less realistic or rational to place the burden on consumers to read through every, generally lengthy, terms-of-service statement and then opt-out of data collection services, when so many services that are central to today's communications and interactions grow. Second, the rising number of data breaches at companies holding millions—sometimes billions—of users' information, including Equifax, Yahoo, and Uber, among others, has given rise to concerns about the security or vulnerability of personal information and the amount of data collected and retained by services. Third, a growing concern that

“With a growing number of states interested in a GDPR-like system, the concern of a patchwork system with potentially conflicting laws grows. Strong, comprehensive legislation at the federal level could address these concerns.”

personal data is used for political purposes emerged after news broke that Cambridge Analytica mined the data of millions of Facebook accounts, without the users' consent, using the data for political purposes, such as to support the campaigns of President Trump and Senator Ted Cruz. Fourth, as noted above, the European Union's data protection law resulted in a number

of companies, including those in the United States, being forced to comply with these rules. Policy makers, advocates, and consumers have objected to what has often resulted in a two-tiered system, where United States-based companies provide greater privacy protections to those in Europe than to those domestically. With a growing number of states interested in a GDPR-like system, the concern of a patchwork system with potentially conflicting laws grows. Strong, comprehensive legislation at the federal level could address these concerns.

### *United States Congress*

Comprehensive federal privacy legislation is likely to be a priority for the United States Congress in 2019. Congress has held multiple hearings on the topic of consumer privacy and policy makers released discussion drafts and bills on this issue in the last Congress. The

attention to federal privacy legislation will undoubtedly continue as this issue has the support of Congressional leadership. The Senate Commerce Committee chair Roger Wicker (R-MS) has expressed support for enacting a federal privacy law in 2019; ranking member Maria Cantwell (D-WA) has similarly been engaged on privacy issues and has supported legislation to protect privacy rights of consumers. House Committee on Energy and Commerce chair Frank Pallone (D-NJ) noted support for comprehensive federal legislation; ranking member Greg Walden (R-OR) pointed out last year that state privacy legislation “has heightened calls for federal privacy legislation” and encouraged the technology industry to come to a unified position.<sup>18</sup>

A wide range of stakeholders, including businesses, consumers, academics, and advocates support efforts to enact federal privacy legislation, though the right approach to federal privacy laws and nuances to a federal framework is contentious. Nevertheless, given the urgency in addressing data privacy and security with strong bipartisan support, privacy legislation could be enacted this year. Indeed, as Senator John Thune (R-SD) noted as chair of the Senate Commerce Committee in the last Congress, legislative efforts abroad and in the states “have all combined to put the issue of consumer data privacy squarely on Congress’s doorstep. The question is no longer **whether** we need a federal law to protect consumers’ privacy. The question is **what** shape it should take.”<sup>19</sup> (emphasis added)

“A wide range of stakeholders, including businesses, consumers, academics, and advocates support efforts to enact federal privacy legislation.”

Beginning in late 2018, numerous bills and discussion drafts—from members of Congress, businesses, and advocates—were introduced. Below are some of the most prominent drafts, which could potentially provide the starting point for discussions. In general, these proposals would shift the burden away from the current model, which requires consumers to proactively manage their data to a system that would

place the burden on companies to ensure meaningful consent and protections. Virtually all discussions assume FTC enforcement and oversight.

Senator Ron Wyden (D-OR), who has long been an advocate for privacy, released a discussion draft of the Consumer Data Protection Act, which would “create radical transparency into how corporations use and share their data...”.<sup>20</sup> Wyden’s bill would give consumers the power to control the sharing of their data and allow companies to charge consumers who want to use their services but opt-out of data collection and processing. Wyden’s bill envisions harsh penalties, including steep fines and potential prison terms for violations of the act. However, the bill’s scope is limited to larger companies or ones engaged in particularly high volumes of data collection.

Senator Brian Schatz (D-HI) released his own draft bill, the Data Care Act,<sup>21</sup> also in fall 2018, which garnered co-sponsorship of 14 other Democratic Senators.<sup>22</sup> The key elements of the Data Care Act would impose duties of care, loyalty, and confidentiality on companies; for example, the bill would prohibit companies from using data that would result in reasonably foreseeable physical or financial harm to the individual.

More recently, on April 12, 2019, Senator Edward Markey (D-MA), a member of the Senate Commerce, Science, and Transportation Committee, introduced a comprehensive privacy bill. In addition to providing the rights to notice and control, the Privacy Bill of Rights Act would: explicitly prohibit companies from using personal information in discriminatory ways (such as targeted advertisements related to housing), limit the information that companies can collect to only what is needed to provide the requested services, and allow for suits by state attorneys general and a private right of action by individuals. The bill also prohibits both “take-it-or-leave-it” policies and financial incentives (such as a discount for services) in exchange for opt-in approval of the use and sharing of personal information.

While these bills put forth by Wyden, Schatz, and Markey received much attention, other drafts have also been circulated, such as the Customer Online Notification for Stopping Edge-provider Network Transgressions (CONSENT) Act introduced by Senators Markey and Richard Blumenthal (D-CT), and the Social Media Privacy Protection and Consumer Rights Act by Senators Amy Klobuchar (D-MN) and John Neely Kennedy (R-LA).

In addition to bills by members of Congress, a number of companies, associations, consumer advocacy groups, academics, and other stakeholders have discussed various principles and elements that should be included in federal privacy legislation.

Significantly, in late 2018, Intel Corporation released draft privacy legislation and allowed for interactive, public comment.<sup>23</sup> In welcoming public engagement and comment, Intel made clear that its draft is a work in progress and it has already gone through at least one revision. In the initial draft, Intel intentionally did not adopt CCPA's data minimization model and would provide for federal preemption of state laws. It provides for significant criminal fines and potential for jail time, as well as civil penalties. Intel's initial draft would apply to companies that collect data of more than 5,000 people and appears to introduce a privacy-by-design element, in prohibiting companies from collecting data beyond the companies' purpose. In this way, companies would not be able to collect vast swaths of data with an unknown purpose, the practice many technology companies have engaged in to date.

The Center for Democracy and Technology (CDT) released a draft federal privacy bill in December 2018.<sup>24</sup> CDT's bill grants consumers several rights, including the right to access and correction, data portability, and deletion. Some of these rights apply only to certain types of data; the right to correction, for example, would apply only when used for eligibility determinations for credit, insurance, housing, employment, educational opportunity, or health information. CDT's bill also explicitly addresses biometric information—including location data—limiting when it could be collected. The bill also provides a list

of unfair data uses and specifically addresses issues related to targeting based on data collection, that could result in civil rights violations and discrimination. It does not, however, provide users with the right to object, instead relying on users to agree to terms of service or walk away. It also provides significant exceptions to the provisions, which raises concerns that these exceptions could be exploited by companies. Like other bills, CDT's envisions that the FTC would have a role in enforcing the legislation and provides federal preemption of state laws.

Most recently, in February 2019, the US Chamber of Commerce released model privacy legislation, entitled the Federal Consumer Privacy Act.<sup>25</sup> The Chamber of Commerce model legislation focuses heavily on notice and transparency and would allow consumers to opt-out of data sharing and permit a right to deletion, subject to some exceptions. Like other models, the Chamber of Commerce's draft would empower the FTC to enforce these rules. It would also preempt state laws on data privacy, instead favoring a uniform piece of legislation across the United States. Most companies, such as those working with the Chamber of Commerce, have advocated for a uniform standard, rather than requiring compliance with a patchwork of state regulations.

In addition to efforts in Congress to create a federal legislative solution, the National Telecommunications and Information Administration (NTIA), on behalf of the Department of Commerce, has also noted interest in a federal privacy framework. In September 2018, NTIA published

a request for comment in a number of areas related to federal privacy regulations: "NTIA is seeking public comments on a proposed approach to this task that lays out a set of user-centric privacy outcomes that underpin the protections that should be produced by

“More than 200 individuals, organizations, and companies, including ARL, submitted comments to the NTIA, largely focusing on the importance of strong transparency and meaningful consent, making opt-in the default position.”



any Federal actions on consumer-privacy policy, and a set of high-level goals that describe the outlines of the ecosystem that should be created to provide those protections.”<sup>26</sup> The request for comment sought feedback in a number of areas including transparency of collection, use and sharing of personal information; user control over personal information, reasonable minimization of collection, use, storage and sharing; security safeguards to protect data; user access and ability to correct personal data; risk management; and accountability.<sup>27</sup> The NTIA’s notice clearly envisions federal preemption of state privacy laws and FTC enforcement.

More than 200 individuals, organizations, and companies, including ARL, submitted comments to the NTIA,<sup>28</sup> largely focusing on the importance of strong transparency and meaningful consent, making opt-in the default position. ARL’s comments also note that a right to deletion implicates freedom of expression and the importance of preserving the cultural record and therefore such a right must be carefully considered and likely requires a highly nuanced approach.<sup>29</sup> The NTIA noted in its request for comment that other agencies are working on similar efforts, including the National Institute of Standards and Technology’s voluntary privacy framework and the International Trade Administration’s effort to increase global regulatory harmony on privacy.

Congress will continue working on a federal data privacy framework in the United States in 2019. Both Houses of Congress have explored various aspects of data privacy. The House of Representatives Committee on Energy and Commerce held a hearing on “Protecting Consumer Privacy in the Era of Big Data” on February 26, 2019.<sup>30</sup> One day later, the Senate Committee on Commerce, Science, and Transportation convened a hearing on “Policy Principles for a Federal Data Privacy Framework in the United States.”<sup>31</sup> In announcing the hearing, Chairman Wicker noted, “It is this committee’s responsibility and obligation to develop a federal privacy standard to protect consumers without stifling innovation, investment or competition. As we continue to examine this critically important issue, I hope this

first hearing will offer valuable insights that will help set the stage for meaningful bipartisan legislation,”<sup>32</sup> indicating that additional hearings should follow, with the intention of a bipartisan effort to enact privacy legislation. Several additional hearings in Congress and the FTC have been held.

As the numerous hearings and bills, as well as the NTIA’s request for comment illustrate, legislating in this area will require thoughtful debate and, ultimately, a nuanced approach in many areas. While all of the discussion drafts and comments have been criticized by various stakeholders, elements of any of the drafts could find their way into federal privacy legislation.

### **The Upshot**

Any legislation in the United States would likely require libraries to evaluate their contracts with vendors and services, their own privacy policies, and data collection policies to which they agree. For example, while libraries may rely on outside services as platforms, libraries must fully understand what these services collect and why, as well as how this is communicated to patrons. Additionally, while research libraries

“Any legislation in the United States would likely require libraries to evaluate their contracts with vendors and services, their own privacy policies, and data collection policies to which they agree.”

are committed to improving user experience, they must consider what collection of data is appropriate and how to improve informed consent. Should some form of a right to deletion/right to be forgotten be included, libraries must determine how to balance these rules with the First Amendment or how to use any exceptions to such a right

to preserve cultural heritage. Many of the issues a research library might face are ethical ones that depend on best practices, but could potentially fall under federal laws depending on how broadly or comprehensively a legislative solution is framed.



Similarly, although Canada is much further along than the United States in comprehensive, national legislation protecting data privacy, it is clear that Canada is considering additional amendments to its laws. Canadian research libraries should watch for updates from the Canadian government's 2018 roundtables and potential amendments to its laws to determine whether changes to their privacy policies are legally necessary.

## Endnotes

1. Samuel D. Warren and Louis D. Brandeis published an article, "The Right to Privacy," in the *Harvard Law Review* 4, no. 5 (December 15, 1890): 193–220, in which they urged for a "right to privacy" or "right to be let alone." This article proved to be highly influential and a right to privacy was subsequently adopted in court decisions.
2. "Library Bill of Rights," American Library Association, last amended January 29, 2019, <http://www.ala.org/advocacy/intfreedom/librarybill>.
3. "Privacy: An Interpretation of the Library Bill of Rights," American Library Association, amended July 1, 2014, <http://www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy>.
4. See, for example, Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress* (May 2000), 36–38, <https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000text.pdf>.
5. The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (February 2012), <https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf>.
6. The White House, *Consumer Data Privacy*.
7. Section 5 of the Federal Trade Commission Act of 1914.

8. Privacy Rights for California Minors in the Digital World, California Business and Professions Code, Section 22580, [http://leginfo.legislature.ca.gov/faces/codes\\_displaySection.xhtml?sectionNum=22580&lawCode=BPC](http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=22580&lawCode=BPC); Online and Personal Privacy Protection, Delaware Commerce and Trade Code, Chapter 12C, <http://delcode.delaware.gov/title6/c012c/index.shtml>.
9. See Privacy of User Records: Violation, Classification, Definition, Arizona Revised Statutes, Section 41-151.22, <https://www.azleg.gov/ars/41/00151-22.htm>; Reader Privacy Act, California Civil Code, Section 1798.90, [http://leginfo.legislature.ca.gov/faces/codes\\_displaySection.xhtml?sectionNum=1798.90.&lawCode=CIV](http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1798.90.&lawCode=CIV); Online and Personal Privacy Protection, Delaware Commerce and Trade Code, Chapter 12C, <http://delcode.delaware.gov/title6/c012c/index.shtml>; Disclosure of Library Records: Definitions, Missouri Revised Statutes, Section 182.815, <https://law.justia.com/codes/missouri/2011/titlexi/chapter182/section182815/>.
10. California Consumer Privacy Act of 2018, Assembly Bill No. 375, [https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill\\_id=201720180AB375](https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375).
11. Rhode Island, for example, is considering a bill on data protection. See “Rhode Island Lawmaker Proposes Data Transparency And Protection Act,” *Daily Dashboard*, International Association of Privacy Professionals, January 25, 2018, <https://iapp.org/news/a/ri-state-representative-proposes-data-transparency-and-protection-act/>.
12. Washington Privacy Act, Senate Bill 5376, <http://lawfilesexternal.wa.gov/biennium/2019-20/Pdf/Bills/Senate%20Bills/5376.pdf>.
13. Anne T. Gilliland, *Issue Brief: The General Data Protection Regulation: What Does It Mean for Libraries Worldwide?* (Washington, DC: Association of Research Libraries, May 2018), [https://www.arl.org/storage/documents/IssueBrief\\_GDPR\\_May2018.pdf](https://www.arl.org/storage/documents/IssueBrief_GDPR_May2018.pdf).
14. See, for example, King & Spalding, “Canada to Update Data Law to GDPR Standard as a Minimum,” *JD Supra*, June 29, 2018, <https://>

[www.jdsupra.com/legalnews/canada-to-update-data-law-to-gdpr-16052/](http://www.jdsupra.com/legalnews/canada-to-update-data-law-to-gdpr-16052/); Angelica Mari, “Brazil Moves Forward with Online Data Protection Efforts,” *ZDNet*, July 5, 2018, <https://www.zdnet.com/article/brazil-moves-forward-with-online-data-protection-efforts/>.

15. Prior to these updates, the Standing Committee on Access to Information, Privacy and Ethics held hearings on PIPEDA. The Canadian Association of Research Libraries (CARL) testified, addressing concerns regarding the right to be forgotten: “CARL Appearance before the ETHI Committee Hearing on the Personal Information Protection and Electronic Documents Act (PIPEDA),” June 1, 2017, <http://www.carl-abrc.ca/wp-content/uploads/2017/11/CARLOpening-Statement-to-ETHI-on-RTBF-version-31-05-17-bilingual.pdf>.
16. Standing Committee on Access to Information, Privacy and Ethics, *Addressing Digital Vulnerabilities and Potential Threats to Canada’s Democratic Electoral Process: Report of the Standing Committee* (Ottawa, Ontario: House of Commons, June 2018), <https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP9932875/ethirp16/ethirp16-e.pdf>.
17. “National Digital and Data Consultations,” Government of Canada, accessed April 2, 2019, <https://www.ic.gc.ca/eic/site/084.nsf/eng/home>.
18. John D. McKinnon and Marc Vartabedian, “Tech Firms, Embattled over Privacy, Warm to Federal Regulation,” *Wall Street Journal*, August 6, 2018, <https://www.wsj.com/articles/tech-firms-embattled-over-privacy-warm-to-federal-regulation-1533547800>.
19. John Thune’s opening remarks presented in “Thune Leads Hearing Examining Safeguards for Consumer Data Privacy,” press release, September 26, 2018, <https://www.thune.senate.gov/public/index.cfm/2018/9/thune-leads-hearing-examining-safeguards-for-consumer-data-privacy>.

20. Ron Wyden United States Senator for Oregon, “Wyden Releases Discussion Draft of Legislation to Provide Real Protections for Americans’ Privacy,” press release, November 1, 2018, <https://www.wyden.senate.gov/news/press-releases/wyden-releases-discussion-draft-of-legislation-to-provide-real-protections-for-americans-privacy>.
21. McKinnon and Vartabedian, “Tech Firms, Embattled over Privacy.”
22. Co-sponsors include Senators Maggie Hassan (D-NH), Michael Bennet (D-CO), Tammy Duckworth (D-IL), Amy Klobuchar (D-MN), Patty Murray (D-WA), Cory Booker (D-NJ), Catherine Cortez Masto (D-NV), Martin Heinrich (D-NM), Ed Markey (D-MA), Sherrod Brown (D-OH), Tammy Baldwin (D-WI), Doug Jones (D-AL), Joe Manchin (D-WV), and Dick Durbin (D-IL).
23. “Legislation,” Intel Corporation, accessed April 2, 2019, <https://usprivacybill.intel.com/legislation/>.
24. *CDT’s Federal Baseline Privacy Legislation Discussion Draft*, Center for Democracy and Technology, December 13, 2018, <https://cdt.org/insight/cdts-federal-baseline-privacy-legislation-discussion-draft/>.
25. Federal Consumer Privacy Act (draft), US Chamber of Commerce, accessed April 2, 2019, [https://www.uschamber.com/sites/default/files/uscc\\_dataprivacymodellegislation.pdf](https://www.uschamber.com/sites/default/files/uscc_dataprivacymodellegislation.pdf).
26. National Telecommunications and Information Administration, Request for Comments on Developing the Administration’s Approach to Consumer Privacy, September 25, 2018, <https://www.ntia.doc.gov/federal-register-notice/2018/request-comments-developing-administration-s-approach-consumer-privacy>.
27. National Telecommunications and Information Administration, “NTIA Seeks Comment on New Approach to Consumer Data Privacy,” press release, September 25, 2018, <https://www.ntia.doc.gov/press-release/2018/ntia-seeks-comment-new-approach-consumer-data-privacy>.

28. NTIA released the comments responding to its request for comments. See “Comments on Developing the Administration’s Approach to Consumer Privacy,” NTIA website, November 13, 2018, <https://www.ntia.doc.gov/other-publication/2018/comments-developing-administration-s-approach-consumer-privacy>.
29. Association of Research Libraries comment on “Developing the Administration’s Approach to Consumer Privacy,” Docket No. 180821780-8780-01, accessed April 2, 2019, [https://www.ntia.doc.gov/files/ntia/publications/ntia\\_privacy\\_220ct2018.pdf](https://www.ntia.doc.gov/files/ntia/publications/ntia_privacy_220ct2018.pdf).
30. “Hearing on ‘Protecting Consumer Privacy in the Era of Big Data,’” US House of Representatives Committee on Energy and Commerce, February 26, 2019, <https://energycommerce.house.gov/committee-activity/hearings/hearing-on-protecting-consumer-privacy-in-the-era-of-big-data>.
31. “Policy Principles for a Federal Data Privacy Framework in the United States,” hearing announcement and webcast, US Senate Committee on Commerce, Science, and Transportation, February 27, 2019, <https://www.commerce.senate.gov/public/index.cfm/hearings?ID=CBA2CD07-4CC7-4474-8B6E-513FED77073D>.
32. “Policy Principles for a Federal Data Privacy Framework,” US Senate Committee on Commerce, Science, and Transportation.

© 2019 Krista L. Cox



This article is licensed under a Creative Commons Attribution 4.0 International License. To view a copy of this license, visit <https://creativecommons.org/licenses/by/4.0/>.

**To cite this article:** Krista L. Cox. “Legal Landscape of Consumer/ User Data Privacy and Current Policy Discussions.” *Research Library Issues*, no. 297 (2019): 15–37. <https://doi.org/10.29242/rli.297.3>.

## Privacy in Public Libraries

**Bill Marden**, Director of Privacy and Compliance, The New York Public Library

**Greg Cram**, Associate Director of Copyright and Information Policy, The New York Public Library

Privacy. The subject of how our personal information—including some of the most intimate details of our daily lives—gets used and sometimes abused has become a common topic in the media and in daily conversations. Americans and the world at large are trying to come to grips with a new paradigm that determines what is and what can be known about all of us through the collection of data in all its forms. Congress has made this topic a key area of focus in its current session. Senator John Thune (R-SD), Majority Whip, opened a pair of hearings last fall by stating that developing a privacy law for the United States enjoys bipartisan support. All signs point to Congress taking on the issue of privacy over the next two years, but it is not clear yet what shape the privacy law will take. As Congress develops a comprehensive privacy proposal, libraries will play a critical role in shaping that law. This article illuminates the challenges faced by public libraries, elucidates the role of libraries in the privacy landscape, and identifies new projects designed to help libraries respond to the privacy challenges presented by new technology.

“Public libraries face myriad privacy challenges, both external and internal.”

Today, public libraries face myriad privacy challenges, both external and internal. There is a constant need to assess and use the data that libraries routinely collect and store. Data, whether in its old-fashioned analog form (think paper call slips) or digital, is a desirable and highly sought-after commodity in our current world. On the more benevolent side of this usage is data analytics used by libraries to determine the effectiveness of their programs and resources. On the less benevolent side is the use of such data for surveillance or crime solving by law



enforcement, or the possible unauthorized use by third-party vendors. For example, law enforcement may seek video recordings from security cameras to collect information about an alleged crime. A database vendor might resell data about a patron or might market to a patron without the library's permission. On the truly darker side is the ever-present danger that library data could be stolen (and occasionally held ransom) by hackers or unwittingly left out in the open, available for anyone to discover it. Finally, when libraries strive to provide improved, more-personalized services tailored to their patrons, they often find themselves forced into making difficult, ethical choices about the use of cutting-edge technology that easily allows them to track and analyze how, where, and when patrons are using library materials. If a library is offering a program on a topic that is likely to be of interest to a particular patron, how might the library target an email to that patron (aside from the patron proactively signing up to receive such notices)?

These scenarios raise important privacy and confidentiality challenges, including a patron's right to opt in and opt out of how and when the library collects her personal information. Although we often use the words privacy and confidentiality interchangeably, there is a distinct difference between the two concepts. Privacy, by definition, is an individual's right to control the collection, use, and disclosure of personal information. For example, an individual makes certain decisions about her privacy when seeing a doctor for an exam. The individual grants permission to the doctor to conduct an examination that will reveal personal information to the doctor about the individual's health. Confidentiality, on the other hand, is the obligation of an individual, organization, or business to protect personal information and not misuse or wrongfully disclose that information. In the example of the doctor visit, the doctor has a duty of confidentiality to protect the information learned during the individual's exam and must abide by the patient's decisions about what information, to whom, and when it can be shared.



## Foundations of Privacy in Libraries

Libraries facing these challenges can look to the principles of the profession to understand how to collect and disseminate information about their patrons. Since 1939, the American Library Association (ALA) has affirmed the right of privacy for library patrons. Article 11 of the original Code of Ethics for Librarians states, “It is the librarian’s obligation to treat as confidential any private information obtained

“Since 1939, the American Library Association (ALA) has affirmed the right of privacy for library patrons.”

through contact with library patrons.”<sup>1</sup> The current Code of Ethics states, “We protect each library user’s right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired or transmitted.”<sup>2</sup> Patron privacy is crucial to freedom of inquiry and access to library resources for all users.

ALA’s Intellectual Freedom Committee and its Privacy Subcommittee have worked to provide forums and guidelines, and act as a clearinghouse for library privacy issues and ideas, including the annual Choose Privacy Week, a privacy section in the weekly *Intellectual Freedom News*,<sup>3</sup> and a website: [chooseprivacyeveryday.org](http://chooseprivacyeveryday.org).

Beyond the principles of the profession, all libraries are subject to state laws that dictate how personal data can be collected and used within libraries specifically. In the 1980s, states began passing statutes protecting the confidentiality of library records. New York State passed such a statute in 1981 that prohibits the disclosure of library records and prohibits their use “except when necessary for the proper operation of the library” and in response to subpoenas, warrants, and law enforcement requests. The legislators who wrote the bill noted in their supporting documentation:

The library, as the unique sanctuary of the widest possible spectrum of ideas, must protect the confidentiality of its records in order to insure its readers’ right to read anything they wish, free from the

fear that someone might see what they read and use this as a way to intimidate them....Without such protection there would be a chilling effect on our library users as inquiring minds turn away from exploring varied avenues of thought because they fear the potentiality of others knowing their reading history.<sup>4</sup>

By affirming that privacy is an essential value of American libraries, the New York State legislature provided the means and authority for libraries to truly protect the personal information of their patrons.

### **New Technology and Privacy**

Innovations in technology have created—and continue to create—new privacy challenges for public libraries. The amount of personal data that can conceivably be collected today, compared to even a decade ago, is monumental. For example, by employing commercially available marketing tools, libraries can now track how patrons are engaging with a library’s website and the websites of others. This information could potentially be used to target ads and announcements toward specific users to inform them of programs or events that are likely to be of interest. The question is whether libraries **should** make use of such technologies simply because they are legally available and because they are used in the larger world of marketing and commerce.

“Innovations in technology have created—and continue to create—new privacy challenges for public libraries.”

### **Current Projects**

Given the ease with which such information can be collected, libraries are on the forefront of creating privacy-related training and procedures to help safeguard personal information. ALA’s Privacy Subcommittee and ALA’s Library Information Technology Association (LITA) both hold regular forums and presentations on privacy at ALA’s Annual Conference and through webinars and other programs throughout the year. State and regional library associations, graduate school library

science programs, and the academic community (including academic journals, such as *RLI*) are also increasingly engaged in this topic. In addition, various external grant-making organizations are funding privacy projects. In 2017, the Institute of Museum and Library Services

“Libraries are on the forefront of creating privacy-related training and procedures to help safeguard personal information.”

(IMLS) awarded a grant to the Center for Information Policy Research at the University of Wisconsin–Milwaukee in partnership with Data & Society, ALA’s Office of Intellectual Freedom, and The New York Public Library. The grant made it possible to host a series of meetings, including a national forum in May 2018 to explore what privacy means in the digital world. The grant investigators identified

a set of common themes that summarized the growing need and challenges to maintain libraries’ commitments to patron privacy.<sup>5</sup>

Other recent grant awards have focused on training public librarians to become privacy leaders at their institutions. Funded by IMLS, New York University and Library Freedom Project have launched the Library Freedom Institute, a six-month train-the-trainers course for librarians.<sup>6</sup> The participants spend time each week learning how to install and use privacy software, educate communities on privacy practices, promote privacy as a design principle within their libraries, and advocate for privacy-first policies and legislation. In what is perhaps the largest, most-encompassing library-privacy initiative in the country, the three major New York City library systems—New York Public Library, Brooklyn Public Library, and Queens Library—joined together to create the NYC Digital Safety: Privacy & Security training program in 2018.<sup>7</sup> The ongoing program trains New York City’s front-line librarians in preparing them to answer questions from New Yorkers about how to safely navigate the world of digital information. As the project’s manager, Davis Erin Anderson, noted during the program’s launch:

Many New York City residents use digital technology nearly every waking hour of their day. From using email at work to browsing social media on the subway to streaming television shows at home, we are consistently delivering a wealth of data about who we are and what we do online to Internet Service providers and myriad online entities. This information can be utilized to influence our behavior, and, more pressingly, can be used against us in the event of, for example, a successful phishing attempt or a data breach.<sup>8</sup>

The NYC Digital Safety project received financial support from the City of New York and was overseen by the Metropolitan New York Library Council (METRO). It resulted in a set of online modules that are now freely available, not just for librarians, but for anyone to use. The topics cover a wide range of basic information, including:

1. Introduction to Digital Safety
2. Internet Technologies and the Information Flow
3. Who Collects Data; Connecting Securely
4. Securing Accounts and Devices
5. Preventing Tracking
6. Avoiding Scams and Malware; Minimizing Your Digital Footprint
7. Privacy and Security in the Library

For more information see [nycdigitalsafety.org](http://nycdigitalsafety.org).

In late April 2019, METRO announced that it would be launching a second phase of this project, which will include updates to the existing online modules, a program to bring library staff together to implement a public-facing approach to online privacy, an NYC Library Privacy Week planned for the fall of 2019 and 2020, and a one-day Privacy Summit for New York City's public library staff.

## NYPL Initiatives

The New York Public Library is also paving the way in creating other privacy standards and controls that meet the demands of the 21st-century library. The data that flows through most modern libraries, one could argue, is actually in the hands of third-party vendors. Many products and services the library depends on, such as integrated library systems (ILS), customer relationship management (CRM) databases, software programs for educational use, analytics software, cloud storage, and website hosting, are outside the library's direct and complete control and rely on contractual agreements. The question for libraries is how to best control these agreements and outside

“The New York Public Library is also paving the way in creating other privacy standards and controls that meet the demands of the 21st-century library.”

relationships. NYPL has a workflow that involves the director of privacy, the legal department, IT, and a risk manager from purchasing in reviewing any vendor contracts that involve the collection and use of personally identifiable information (PII) about patrons,

making certain that that PII is safeguarded and properly controlled by the vendor throughout the data life cycle (starting from the point of collection, to its storage, its access, and ending with its proper retention and disposal).

NYPL also proudly boasts that it is the first and (still) only library in the country to have a full-time privacy officer, a position which has existed here since 2015. In his role as NYPL director of privacy and compliance, Bill Marden has formed a Privacy Advisory Committee comprised of representatives from every division of the library, who meet monthly to discuss and help decide various initiatives and issues related to privacy at NYPL. With the help of the members of this committee, NYPL is embarking on a complete inventory of its data-collection practices, including a risk assessment of how well the library safeguards data containing PII.

## Conclusion

Protecting the privacy of patrons remains an essential principle for public libraries. The commitment to this principle is regularly challenged by a variety of pressures, including the ease of data collection and dissemination created by technological advances. Although these challenges are sharpened by technology, libraries can draw on their history of offering a sanctuary for intellectual freedom. New projects focusing on understanding these pressures and training librarians will help guide public libraries through these challenges.

## Endnotes

1. 1939 Code of Ethics for Librarians, American Library Association, accessed April 30, 2019, <http://www.ala.org/Template.cfm?Section=coehistory&Template=/ContentManagement/ContentDisplay.cfm&ContentID=8875>.
2. Code of Ethics of the American Library Association, ALA, last amended January 22, 2008, [http://www.ala.org/advocacy/sites/ala.org/advocacy/files/content/proethics/codeofethics/Code of Ethics of the American Library Association.pdf](http://www.ala.org/advocacy/sites/ala.org/advocacy/files/content/proethics/codeofethics/Code%20of%20Ethics%20of%20the%20American%20Library%20Association.pdf).
3. *Intellectual Freedom News*, Office for Intellectual Freedom, American Library Association, accessed April 30, 2019, <https://www.oif.ala.org/oif/?cat=393>.
4. Memorandum of Assemblyman Sanders, *New York State Legislative Annual 1982* (New York: New York Legislative Service, 1982), 25, cited in *Quad/Graphics, Inc. v. Southern Adirondack Library System*, 174 Misc. 2d 291, 294 [Sup. Ct. 1997], <https://caselaw.findlaw.com/ny-supreme-court/1481617.html>.
5. “Project Report: ‘Library Values & Privacy in Our National Digital Strategies: Field Guides, Convenings, and Conversations,’ ” Center for Information Policy Research, University of Wisconsin–Milwaukee, August 2, 2018, <https://cipr.uwm.edu/2018/08/02/project-report-library-values-privacy/>.

6. Library Freedom Institute website, accessed April 30, 2019, <https://libraryfreedomproject.org/lfi/>.
7. NYC Digital Safety: Privacy & Security website, accessed April 30, 2019, <https://nycdigitalsafety.org/>.
8. Davis Erin Anderson, “New Privacy Resources Available from NYC Digital Safety,” *Voices for Privacy Blog*, December 5, 2018, <https://chooseprivacyeveryday.org/new-privacy-resources-available-from-nyc-digital-safety/>.

© 2019 Bill Marden and Greg Cram



This article is licensed under a Creative Commons Attribution 4.0 International License. To view a copy of this license, visit <https://creativecommons.org/licenses/by/4.0/>.

**To cite this article:** Bill Marden and Greg Cram. “Privacy in Public Libraries.” *Research Library Issues*, no. 297 (2019): 38–46. <https://doi.org/10.29242/rli.297.4>.



## Research Library Issues

*Research Library Issues (RLI)* focuses on current and emerging topics that are strategically important to research libraries. The articles explore issues, share information, pose critical questions, and provide examples. Suggestions for potential themes, articles, and authors are welcome. Please [submit suggestions via this online form](#).

ISSN 1947-4911 <https://doi.org/10.29242/rli>

Editor-in-chief: Mary Lee Kennedy

Managing editor: Elizabeth A. Waraksa

Guest editor: Krista L. Cox

Copy editor: Kaylyn Groves

Layout editor: Katie Monroe

© 2019 Association of Research Libraries

ARL policy is to grant blanket permission to reprint as long as full attribution is made. Exceptions to this policy may be noted for certain articles. This is in addition to the rights provided under sections 107 and 108 of the Copyright Act. For more information, contact ARL Publications, [pubs@arl.org](mailto:pubs@arl.org).

Current and back issues are available on the ARL Digital Publications website, [publications.arl.org/rli](http://publications.arl.org/rli). The website is also where you may sign up for alerts to new releases of *Research Library Issues*.

**Association of Research Libraries**

21 Dupont Circle, NW  
Suite 800  
Washington, DC 20036  
T 202.296.2296  
F 202.872.0884

ARL.org  
[pubs@arl.org](mailto:pubs@arl.org)