2015

Privacy and Competing Library Goals: How Can Library Directors Lead When Values Collide?

Anne Klinefelter

Follow this and additional works at: https://scholarship.law.unc.edu/faculty_publications

Part of the Legal Writing and Research Commons, and the Privacy Law Commons

Publication: Academic Law Library Director Perspectives
Privacy and Competing Library Goals: How Can Library Directors Lead When Values Collide?

Anne Klinefelter
Associate Professor of Law
Director of the Law Library
University of North Carolina School of Law

Privacy is easy for librarians to appreciate until the discovery that other library interests—like information access; personalization of services; new services; security of people, places and data; and even variations on privacy itself—can compete with privacy. During the late 20th century, librarians and United States’ culture embraced the idea of reader privacy and particularly privacy of library use, but the 21st century has introduced many new privacy challenges. Librarians now face novel privacy implications as we consider how to make the most of new technologies and practices such as digitization of special collections, data mining of our collection use patterns, and any number of social approaches to scholarly communications. We also have an abundance of new privacy challenges relating to user information and digitized materials containing personal information, as well as a number of privacy obligations not unique to libraries such as website privacy policies, data security, and employee privacy. The tradeoffs required to protect library-related privacy are becoming more costly, and the choices are increasingly complicated by an evolving set of federal and state privacy laws and shifting policy norms which librarians must master and even help to shape.

This chapter is offered as support for librarians who must lead libraries through this fraught territory where privacy and other values collide. Privacy choices involve law, policy, and practical concerns, and each of these three considerations is subject to change due largely to rapidly developing technologies and perhaps slightly less rapidly evolving cultural norms. Librarians and especially academic law library directors are charged with taking a long view of managing a library’s collection and services, so this chapter provides a broad overview of the complex areas of related privacy law and policy to provide some guidance with more lasting utility than an examination of the many specific privacy-related challenges facing libraries at the time of this writing. The chapter begins with a brief history and current context for libraries and privacy and then identifies some approaches to addressing privacy, drawing on a sample of issues relating to privacy of library users, of individuals represented in library collections, and of library employees.

1 Anne Klinefelter thanks Deborah Gerhardt, Dave Hansen, Woody Hartzog, and Michelle Wu for their astute and generous insights and Daniel Parisi for his outstanding research support.
Libraries’ Mixed History with Privacy (of Library Users)

Libraries’ greatest connection with privacy has been with protecting the confidentiality of library use, but United States libraries did not always have a clear commitment to reader privacy and the related concepts of reader autonomy and unfettered intellectual freedom to explore ideas. Historically, libraries have not only shaped what was acceptable to read through careful collection management, but libraries have also collected information about who reads what and even exposed or actively shared those records of library users’ reading habits. United States’ university libraries in the 19th century and early 20th century maintained circulation registry books that preserved for any curious researcher the names of library users and the dates when they borrowed and returned particular titles from the collection. Public libraries built with Carnegie funds were imbued with twin goals of moral uplift and a sort of bootstrap financial betterment of society, and librarians guided library users to books deemed by the institution as best serving these goals. Privacy-related concepts of autonomy, dignity, agency, liberty, intellectual freedom, and anonymity were not major conceptual influences on libraries, or even in society, until the latter part of the 20th century.

The idea that libraries and their staff would treat library use as confidential needed both cultural and technological supports to develop. The earliest formal recognition that library use should be confidential may have been the American Library Association’s 1939 Code of Ethics which stated “it is the librarian’s obligation to treat as confidential any private information obtained through contact with library patrons.” Whether “private information” referred to by the 1939 Code was intended to include book titles consulted is not clear from the text. Signature cards filed in book pockets or viewable circulation registry books would have revealed who had read a particular book.

---

2 Arthur E. Bostwick, The American Public Library 42–43 (1917) (describes “the ledger system” as still in use at the time). For an example of this sort of ledger, see Univ. of N.C. at Chapel Hill Library Circulation Dep’t, Records of the Circulation Department, 1886–1944. The catalog record is available at: http://search.lib.unc.edu/search?R=UNCh2449992.

3 Andrew Carnegie explained his philanthropic interest in building public libraries were based in appreciation for his own boyhood access to a library he said inspired his achievements both moral and material. Abigail A. Van Slyck, Free to All: Carnegie Libraries & American Culture, 1890–1920, at 9 (1995). Perhaps we can call this library culture one that promoted hoisting oneself by one’s own bookstrap.


The 1960s and 1970s were a time of great social change empowering individuals, and the privacy-related concepts of autonomy, agency, and dignity gained influence throughout society. At the same time, technologies such as photocopiers and computers changed the way libraries could be used and managed. Individuals could make copies of parts of library materials instead of checking them out, and computer-based circulation systems began to replace signature cards that had blatantly shared the names and handwriting of individuals checking out library books. Of course, computerized circulation systems simply presented a different way that library use might be tracked, recorded, and shared.

Disgust over government surveillance relating to Watergate and the Civil Rights movement combined with fears of government’s misuse of a growing number of databases led to the passage of both freedom-of-information laws and some exceptions to those laws to protect the privacy of individuals represented in these databases. Library privacy probably received a responsive boost when university librarians reported the federal government was attempting to spy on library users suspected of exporting scientific and other information during the Cold War. Against this backdrop of social and technological change, throughout the 1970s and into the 1980s, state legislatures began to pass laws that protected the confidentiality of library use. State laws and some federal laws protecting library use vary, but they all provide some protection against access to records of individuals’ use of public libraries, publicly accessible libraries, and even private libraries.

As the 21st century began, reader privacy and libraries were again in the news as librarians rushed to oppose expanded government surveillance under the USA PATRIOT Act and related federal laws. A case involving federal access to library

---

8 Henry Tseng, The Ethical Aspects of Photocopying As They Pertain to the Library, the User and the Owner of Copyright, 72 Law Libr. J. 86 (1979) (suggesting ethical approaches for balancing the interests of librarians, teachers, and publishers in adjusting to the disruptive technology of the photocopier machine); Howard Fosdick, The Microcomputer Revolution, 105 Libr. J. 1467 (1980) (chronicling the development of the microcomputer and predicting that libraries will have many uses for them).
use records was instrumental in securing modest but important limitations on these laws, particularly as they relate to First Amendment activities. In addition, lawsuits challenging Google Books on copyright and antitrust grounds inspired a number of amicus briefs from privacy advocates contrasting the reader privacy provided by libraries with reader tracking practices of Google. Librarians’ ethical commitment to confidentiality of library use and state library privacy laws have created a strong reputation for libraries as havens for confidential reading, but the issues to be outlined in this article demonstrate that confidentiality of library use in the 21st century library is a difficult goal for libraries to meet without frustrating other library goals and innovations.

Legal and Policy Foundations for Reader Privacy

Reader privacy and the related idea of confidentiality of library use are asserted on the basis of an interweaving of law and policy considerations. Reader privacy has been justified as essential in serving many First Amendment principles relating to freedom of speech and freedom of the press. Scholars and courts have promoted unimpeded expression and access to information as necessary for an informed electorate, innovation, liberty, and other values fundamental to the United States. Librarians and others have asserted that when reading is monitored, individuals are less willing to explore controversial ideas or reveal interests that would convey vulnerabilities like illness or marital discord or which might expose sexual interests.


15 Klinefelter, supra note 12.

16 Neil M. Richards, The Perils of Social Reading, 101 GEO. L.J. 689, 708-09 (2013) (“we need intellectual privacy to make up our minds, but we often need the assistance and recommendations of others as part of this process, be they friends, librarians, or search engines. The norms of librarians suggest one successful and proven solution to this paradox”).


18 Michael Zimmer, Librarians’ Attitudes Regarding Information and Internet Privacy, 84 LIBR. Q. 123, 125–26 (2014) (expressing the idea that the freedom to read and receive information
Some have argued that freedom of the press requires unimpeded readers to make the work of the press meaningful. More broadly, Constitutional privacy rights have been described as protecting certain types of decisions from government interference and to prevent disclosure of personal information. Privacy interests are generally considered to be at the core of several parts of the Bill of Rights, including the Fourth and Fifth Amendments. Federal constitutional protections for reader privacy are bolstered or even broadened in some states by state constitutional protections for privacy or freedom of speech. State statutes specifically protecting confidentiality of library use cover forty-eight states, and Attorney General opinions fill in for the other two states. The District of Columbia has similar statutory protection, and a federal statute provides confidentiality for the use of the Library of Congress.

Alan Rubel, *Claims to Privacy and the Distributed Value Rule*, 44 SAN DIEGO L. REV. 921, 929 (2007) (discussing the possibility that privacy allows room for ideas to develop in a democracy); Neil Richards, *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age* (forthcoming 2015) (exploring the relationship between freedom of speech and privacy and asserting the importance of intellectual privacy in supporting exploration of ideas before those ideas are fully shaped and ready for broad sharing). The writers’ group, PEN, has reported that members are self-censoring their social media, telephone, email, and other communications as a result of 2013 revelations that the United States government has been conducting extensive surveillance, *Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor*, PEN American Center (Nov. 12, 2013), available at http://www.pen.org/sites/default/files/2014-08-01_Full%20Report_Chilling%20Effects%20w%20Color%20cover-UPDATED.pdf.

Susan Nevelow Mart, *The Right to Receive Information*, 95 LAW LIBR. J. 175, 180 (2003) (examining the development of the right to receive information as a necessary corollary of the right of free speech); see also *Reno v. Am. Civil Liberties Union*, 521 U.S. 844, 874 (1997) (finding that certain provisions of the Communications Decency Act, which were meant to protect children, unconstitutionally repressed the right of adults to receive information).

Whalen v. Roe, 429 U.S. 589, 598–600 (1977) (summarizing prior precedent as involving “at least two different kinds of interests” including “the individual interest in avoiding disclosure of personal matters” and “independence in making certain kinds of important decisions”); *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449 (1958) (holding that the state of Alabama could not require the NAACP to divulge the names and addresses of its members because it would infringe upon the freedom of these individuals to associate); *United States v. U.S. Dist. Court (Keith)*, 407 U.S. 297 (1972) (requiring warrants for domestic surveillance in order to protect rights of speech and privacy that encourage private political dissent).

Some state privacy rights are explicit while others are derived from other language in the text of the state constitution. See Tattered Cover v. City of Thornton, 44 P.3d 1044 (Colo. 2002) (holding that Colorado’s constitutional right to freedom of speech was broader than the federal right and included the right to purchase books anonymously); see also Privacy Rights Based on State Constitutional Provisions, 16B Am. Jur. 2d Constitutional Law § 654 (Westlaw, updated May 2014).

Other laws might also be relevant to reader privacy or library user privacy. The Family Educational Rights and Advocacy Act, FERPA, can provide additional protection to students’ library records which are likely to qualify as education records under the statute and so overlap with state library privacy laws.\(^23\) Federal and state consumer protection laws may also apply, particularly if a library fails to live up to any promises to keep library use confidential.\(^24\) California and a few other states have specific laws that require website privacy policies if California residents are targets for the site, and California now requires notice of the use of website cookies.\(^25\) And, no matter what promises may or may not have been made by a library, if certain sensitive information like Social Security Numbers are left vulnerable to third parties, state data security breach notification laws may apply.\(^26\) Privacy torts currently have narrow and therefore limited viability in general, but they could have some applicability to libraries, particularly if the older tort of breach of confidentiality takes on renewed vigor.\(^27\)

Policies within library professional associations justify reader privacy both as an interpretation of Constitutional protections and as an important transcendent value akin to a human right. The American Library Association has tied reader privacy to intellectual freedom, sometimes defined as an individual’s liberty to choose what she wants to read.\(^28\) When reading is monitored, the assertion is that individuals’ reading is restricted by the chilling effect of that surveillance.

Another law and policy related justification for reader privacy has particular impact on law libraries. Law librarians arguably have additional reader privacy responsibilities because we provide access to the law and to law-related materials—


content often considered core to First Amendment speech protections, and research that could be subject to attorney-client confidentiality interests. The American Association of Law Libraries (AALL) Ethical Principles Preamble focuses on this role of the law library as integral to making “this ideal of democracy a reality.” The evidentiary privilege protecting client communications can be waived if not treated as confidential, and other interests at risk in legal research could be the attorney’s work product protection from opposing counsel’s discovery and the broad ethical commitments attorneys must uphold for all information relating to representation of a client.

Law librarians in the United States, through our national professional association, have a collective commitment to confidentiality of library use. AALL’s Ethical Principles include that statement, “We uphold a duty to our clientele to develop service policies that respect confidentiality and privacy.” The AALL website includes a page devoted to “Privacy” that contains advocacy statements and letters to government officials regarding legislation and policies that the association identifies as threats to privacy from government surveillance and other practices. The association does not limit advocacy to privacy issues that are exclusive to library use but extends its reach to any government practices likely to impact library use.

Librarians might well question whether reader privacy policy and law are grounded in appreciation for a quaint value now overtaken by competing interests. The chilling effect of reader monitoring that is often invoked can seem counter to general trends that indicate privacy is not actually valued enough to merit continuing protection. In particular, the growth of social media suggests that people find benefits in sharing personal and even intimate information, and privacy is simply not the prevailing cultural norm. So, librarians might well question whether the societal benefits of privacy-compromising activities outweigh individual privacy concerns, either in the library context or in other contexts.

Privacy advocates offer a number of responses to such skepticism. First, as a Constitutional or human rights matter, individual rights like privacy are considered zones of protection for minorities in a majoritarian democracy. While any individual’s human or Constitutional rights might not be absolutely unassailable by competing majoritarian interests, the role of rights in general can be seen as protec-

---

29 Klinefelter, supra note 13.

30 The first paragraph of the Preamble states, “When individuals have ready access to legal information, they can participate fully in the affairs of their government. By collecting, organizing, preserving, and retrieving legal information, the members of the American Association of Law Libraries enable people to make this ideal of democracy a reality.” AALL Ethical Principles, Am. Ass’n of Law Libraries (Apr. 5, 1999), http://aallnet.org/main-menu/Leadership-Governance/policies/PublicPolicies/policy-ethics.html.

31 Klinefelter, supra note 13.

32 AALL Ethical Principles, supra note 30.

tion against “the tyranny of the majority.”34 Second, privacy law scholar Dan Solove suggests that framing privacy as an individual right fails to recognize significant societal benefits when individuals have privacy-related protections, especially in a democracy.35 Similarly, Anita Allen argues that even though privacy laws may be paternalistic, they are necessary for both societal and individual good because individuals cannot effectively secure privacy in the marketplace.36 Third, an apparent societal trend towards sharing could fail to acknowledge granular privacy choices that include selective sharing with particular individuals or groups and self-editing at a broader level of comments that are exchanged on social media. And, some have documented how users attempt to avoid privacy-compromising terms of service by using inaccurate personal information to sign up for accounts.37 Theories of contextual privacy and of practical obscurity articulate the reality that individuals believe that they can share selectively rather than making dichotomous choices between making their actions or information either public or private.38 Fourth, some studies and success of new start-ups are showing that people are indeed very interested in privacy. For example, a study of Google search terms pre- and post-Snowden revelations of United States government surveillance practices indicates that some sensitive topics were avoided as news of search monitoring was widely reported.39 Social

34 ALEXIS DE TOCQUEVILLE, DEMOCRACY IN AMERICA (Harvey C. Mansfield & Delba Winthrop trans., Univ. of Chi. Press 2000) (1835) (warning against the “tyranny of the majority”).
35 Daniel J. Solove, “I’ve Got Nothing to Hide” and Other Misunderstandings of Privacy, 44 SAN DIEGO L. REV. 745, 760–64 (2007) (discussing the social value of privacy, beyond thinking of privacy solely in terms of value to the individual).
36 ANITA L. ALLEN, UNPOPULAR PRIVACY: WHAT MUST WE HIDE? (2011) (examining when the law should and should not mandate privacy, drawing on such examples as non-nudity laws and insider trading laws to suggest that society should not allow individuals to reject privacy in some situations because of the negative impact on society).
37 Lee Rainie et al., Anonymity, Privacy, and Security Online, Pew Research Ctr. 4 (Sept. 5, 2013), http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/ (providing results of a survey showing that 18% of adults say that they have used a fake name and 13% have given inaccurate information to maintain online anonymity); see also Danah Boyd & Alice E. Marwick, Social Privacy in Networked Publics: Teens’ Attitudes, Practices, and Strategies 19–24 (presented at Oxford Internet Inst., A Decade in Internet Time: Symposium on the Dynamics of the Internet and Soc’y 2011), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1925128 (describing alternate privacy strategies for social networks including toggling account activation and using “social steganography” or hiding information in plain sight through obscurity). For an historical examination of both positive and negative uses of anonymous speech, thereby, shedding light on today’s anonymous online speech, see generally Victoria Smith Ekstrand, The Many Masks of Anon: Anonymity as Cultural Practice and Reflections in Case Law, 18 J. TECH. L. & POL’Y 1 (2013).
media have taken these concerns to heart, with Safari Internet browser software shifting its default search engine to DuckDuckGo, a service that markets itself as a privacy-protecting search option. Further, a number of new applications and tools like the Blackphone have been introduced and are reportedly thriving.\textsuperscript{40} The efforts of larger social media companies to distinguish their own tracking of individuals with government surveillance demonstrate that these businesses recognize that users value privacy and might avoid their services in light of these concerns.\textsuperscript{41} Fifth, much privacy law and policy is based on fundamental concepts of Notice and Choice, and many suggest that apparent disinterest in privacy is more a failure of effective Notice and meaningful Choice in the marketplace.\textsuperscript{42}

The context for privacy as a cultural norm is further complicated by the law and policy of government surveillance. Recent Supreme Court opinions suggest that the “third party doctrine” of the 1970s may have outlived its acceptability as a way for the government to obtain, without a warrant, information that an individual shared chilled the use of personally sensitive internet search terms both domestically and internationally); \textit{see also} Daniel Castro, \textit{How Much will PRISM Cost the U.S. Cloud Computing Industry?}, Info. Tech. & Innovation Found 2–3 (2013), available at http://www2.itif.org/2013-cloud-computing-costs.pdf (estimating that NSA spying may cause U.S. cloud companies to lose $35 billion in business to non-U.S. cloud companies by 2016); \textit{Chilling Effects, supra} note 18 (finding a dramatic increase in self-censorship by U.S. writers post-Snowden revelations); Voycee, http://voycee.me/ (last visited Sept. 24, 2014) (providing a history-free social networking experience); Steve O’Hearn, \textit{Voycee Is a Social Network that Eats Itself}, Tech Crunch (May 21, 2014), http://techcrunch.com/2014/05/21/www-will-eat-itself/ (describing how the Voycee social network works).


\textsuperscript{41} See Eric Schmidt, \textit{How the ‘New Digital Age’ Is Reshaping the World}, Inc. Live (Mar. 2014), http://www.inc.com/eric-schmidt-jared-cohen/for-data-businesses-depend-on-trust.html (distinguishing between governmental and corporate access to an individual’s data by arguing that governments have a monopoly on the use of force while privacy laws, marketplace competition, and the fear of losing customers’ trust will restrict a corporation’s actions).

with a commercial entity or tool such as a smartphone. These decisions suggest that we may have reached a tipping point in the rush to “get over” privacy. On the other hand, surveillance statutes may not see much revision even after the Snowden disclosures that the NSA has been conducting sweeping tracking of both foreigners’ and citizens’ online and communications activities.

**Legal and Policy Foundations—Beyond Reader Privacy**

The privacy issues of the 21st century library go beyond reader privacy into new and broader territory relating to privacy of individuals represented in our collections and into employee privacy. Collection content-related privacy issues in particular are uncomfortable territory for librarians unaccustomed to engaging with content in any way other than trying to facilitate access. Employee privacy is in some sense new territory because the law continues to change to address access to background information for candidates as well as current employees, public records laws for public institutions, and data security.

Libraries do not have a strong tradition of advocacy for the privacy of individuals represented in publications or electronic resources made available through the library. We are mostly all about access, about information wanting to be free, and about the value of increasing the marketplace of ideas and especially transparency in government. These ideals of robust information access can clash with privacy and some other library interests. A sizeable quantity of 20th century library professional literature concerns librarians’ struggle to parse distinctions between a professional’s discretion in selection of appropriate content for the library collection and censorship. Since the mid-20th century, libraries and library associations have developed policies and ethical statements that promote access to all points of view, with respect for the reader as capable of providing his or her own labels or interpretations of content. Some librarians are free speech absolutists, promoting access to informa-

---

43 Riley v. California, 134 S. Ct. 2473, 2488–93 (2014) (holding that cell phone searches by police incident to arrest require a warrant); United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (stating that it may be necessary to reexamine the third-party doctrine that no reasonable expectation of privacy exists once individual data has been voluntarily shared with third-parties).
45 See Marjorie Fiske, Book Selection and Censorship (1959) (chronicling a variety of practices such as labeling controversial books with a donation stamp). For a longer retrospective, see LOUISE S. ROBBINS, CENSORSHIP AND THE AMERICAN LIBRARY: THE AMERICAN LIBRARY ASSOCIATION’S RESPONSE TO THREATS TO INTELLECTUAL FREEDOM, 1939–1969 (1996).
tion as a matter of respect for the individual who can evaluate that information. Other librarians and much of First Amendment jurisprudence is based on recognition that some impositions on expression and access to information are justified for purposes of using copyright to promote innovation, furthering national security and immediate safety, limiting obscenity, and even protecting privacy. To complicate the First Amendment analysis even further, some privacy protections, such as a right to receive information anonymously, are actually grounded in freedom of speech.

Law libraries that are also publishers take on these roles as special contributions, but most of us have not immersed ourselves in questions of privacy law that might restrict publication. We might, however, be asked to help researchers who intend to quote heavily from rare or other special collections, and we might have to consider how to structure access to donated collections that appear to be covered by privacy interests like attorney-client confidentiality. In some of these situations the law is unclear, and librarians must weigh the policy arguments for and against


49 Tattered Cover, supra note 21 (holding that the right to read books anonymously is critical to protecting free speech and protected under the Colorado constitution).


51 Anne Klinefelter & Marc C. Laredo, Is Confidentiality Really Forever: Even if the Client Dies or Ceases to Exist?, 40 LITIG. 47 (2014) (exploring the problems of libraries receiving donated materials presumptively protected by attorney-client privilege long after the death of the person or persons with authority to assert the privilege); see Douglas Peddicord et al., A Proposal to Protect Privacy of Health Information While Accelerating Comparative Effectiveness Research, 29 HEALTH AFF. 2082, 2083–84 (2010) (advocating that medical researchers present credentials to be given full access to health care records now protected by federal privacy laws and allowed to link data sets without legally required redaction to conduct effective research); Joseph L. Saxs, Not So Public: Access to Collections, 1 RBM: J. RARE BOOKS, MANUSCRIPTS & CULTURAL HERITAGE 101 (2000) (noting options for special collections access including sequestraton for a period of time during which privacy interests presumably fade and excluding access to all but a favored group; also providing a nuanced and thorough review of privacy and other interests that argue for and against access to materials collected by libraries and others).
privacy. We are also not entirely accustomed to thinking about format as a factor that transforms content, although we know that improvements in indexing and remote access have altered legal research and scholarly communication patterns. In terms of privacy, format can transform our traditional open stacks from what has been described as “practical obscurity” into easily discovered and data mined content when libraries digitize content and post it to the web.

Privacy and access compromises can raise policy concerns of their own, and redaction of digitized content to avoid broad dissemination of information like Social Security numbers or credit card numbers or names of rape victims can be seen as distorting the content or even creating a false version of that original content. Privacy advocates might counter that if the redactions are obvious, the changes to the content are at least not secret and satisfy transparency in the redaction itself. But, any privacy solution that involves compromising access and use of information has burdened the utility of that information in some way. Privacy scholars and others talk about the loss of utility of data and about how particular uses of data might require full access without any transformation of data through redaction or other methods. While some privacy advocates suggest that these tradeoffs are not actually necessary, others promote privacy risk and competing benefits analyses, or even suggest that privacy could hamper a sort of pure science exploration of unfiltered access to increasing quantities of big data.

The privacy law relating to individuals in library content is immature, except when financial harm such as identity theft is a risk. Torts relating to privacy vary state by state, and several states have rejected some of these causes of action as offensive to rights of freedom of speech and freedom of the press, while courts that accept these torts nonetheless generally do not find proof of harm. State identity-

52 For example, the Freedom of Information Act (FOIA) generally gives any person the right to request information from the executive branch agencies of the federal government. FOIA, supra note 10. However, information that falls under the exemptions listed in section 552(b) need not be disclosed. Id. at § 552(b). Generally, the agency responding to the FOIA request must specify the amount of information deleted and the exemption that applied. Id. However, the agency can omit such disclosure if such an “indication would harm an interest protected by the exemption … under which the deletion is made.” Id. See also Judith A. Weiner & Anne T. Gilliland, Balancing Between Two Goods: Health Insurance Portability and Accountability Act and Ethical Compliancy Considerations for Privacy-Sensitive Materials in Health Sciences Archival and Historical Special Collections, 99 J. MED. LIB. ASSOC. 15, 20 (2011) (“Researchers should be made aware of the types of information that may be missing in redacted records.”)

53 See infra sections on privacy-by-design and risk and risk/benefits analysis. The sort of pure science potential was raised by Christopher Wolf who posed the question of how one might evaluate potential benefits of unfettered access to big data if a researcher simply wanted to see what emerged from the data, without having any clear expectation at the outset to balance against potential privacy harms. Discussion at the Future of Privacy Forum Advisory Board Retreat, National Harbor, MD (June 3, 2014).

54 Hall v. Post, 323 N.C. 259, 268–70 (1988) (refusing to adopt the tort of publication of private facts and suggesting that the tort of intentional infliction of emotional distress could be used instead); see generally Restatement (Second) of Torts § 652D (1977) (restating the tort of publicity given to private life). Six states currently reject the publication of private facts tort: New York, North Carolina, North Dakota, Nebraska, Montana, and Virginia. Jared A. Wilkerson, Battle for
theft laws, though, might apply in situations when Social Security numbers, bank account numbers, and other related data elements are made widely available. Federal laws regulate access to credit relevant information that can be used to deny credit or employment, and even if these laws do not directly apply to libraries who might digitize content with this type of information, the laws can inform a library’s sense of cultural norms. Similarly, state and federal statutes and court rules relating to redaction of sensitive information in documents made Internet-accessible can serve as guidelines to libraries with projects that involve scanning materials that might contain similar data elements.

Other influential laws include HIPAA, which prevents certain types of health care entities from sharing patient data unless 17 specific data elements are redacted or some specialized statistical anonymization tool is used, or unless the data is accessed by researchers bound by contract and oversight through an institutional review board. Libraries with health related information might look to HIPAA not as binding law but as a policy guide.

Other laws that might directly apply to libraries or influence policy of libraries in terms of collection management include California’s website privacy policy laws and the controversial right to be forgotten which is gaining traction in the European Union. Both state and federal laws prohibiting “unfair or deceptive trade practices” can also provide guidance for libraries for upholding promises including promises relating to privacy and meeting reasonable standards for data security. FERPA might be an influence if, for example, older student records not directly covered by the statute were offered to the library as part of a special collection or if the library had responsibility for managing education records of students. Another federal law with some relevance is the Communications Decency Act which frames some liability limitations for hosts of Internet content and which might support libraries’
digitization projects, even those in which the library redacts sensitive information to meet privacy goals.\textsuperscript{58}

As this overview of privacy law sources demonstrates, most privacy law in the United States is tied to particular industries or to particular government entities or to a particular form or scope of publication. Libraries, like other public or private entities, must continually update their assessment of this body of law, because it changes rapidly, and because the law so far has failed to develop clarity on jurisdictional boundaries when the Internet is involved.\textsuperscript{59} Fortunately, a number of excellent privacy law treatises are updated regularly, and as awareness and interest increase, new support for monitoring and evaluation library privacy issues are being developed.

**Some Practical Approaches for Addressing Privacy**

*Management of Privacy Is a Moving Target*

The list of privacy challenges facing libraries is growing fast as new information technologies, services, practices, and trends develop. Privacy protections and privacy invasions are in some contexts a sort of leap-frogging battle of stamina and creativity. A number of compromise solutions have proven to be startlingly imperfect, and yet many privacy professionals are settling on good-enough solutions. The rest of this chapter will identify some approaches for addressing privacy that can help libraries to develop their own paths to addressing privacy. Some of these approaches are broad managerial and planning tools, while others are specific techniques.

**Incorporation of the Fair Information Practice Principles**

The Fair Information Practice Principles are arguably simply highly influential policy, but because they cover some specific privacy approaches, they are included here as a practical guide. The FIPPs, as they are often called, were developed under

\textsuperscript{58} The Communications Decency Act, Section 230, provides safe harbor protection for defamation and privacy tort liabilities for content providers who are not publishers of the content. Communications Decency Act (CDA) of 1996, 47 U.S.C. § 230 (2012). However, editing is generally allowed without losing immunity if the editing is merely for accuracy or civility and does not materially change the content. Publishing the Statements and Content of Others, Digital Media Law Project, http://www.dmlp.org/legal-guide/publishing-statements-and-content-others (last visited Sept. 24, 2014). Section 230(c)(2)(A) specifically states that no provider shall be held liable for “any action taken in good faith to restrict access to … material that the provider … considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable ….” 47 U.S.C. § 230 (c)(2)(A) (2012) (emphasis added). The Seventh Circuit which has generally taken a narrow reading of Section 230(c)(1), states regarding Section 203(c)(2) that “A web host that does filter out offensive material is not liable to the censored customer. Removing the risk of civil liability may induce web hosts and other informational intermediaries to take more care to protect the privacy and sensibilities of third parties.” Chi. Lawyer’s Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc., 519 F. 3d 666, 669–70 (2008) (second emphasis added) (quoting Doe v. GTE Corp., 347 F.3d 655, 659 (2003)).

the oversight of the Department of Health, Education and Welfare in 1973, when the growth of federal agency databases was starting to inspire some anxiety about privacy of individuals in these databases. The FIPPs have been a frame of reference for a number of United States laws and serve as a guide when the application of laws is underdeveloped or simply unclear. These principles are:

- There must be no personal-data record-keeping systems whose very existence is secret.
- There must be a way for an individual to find out what information about him is in a record and how it is used.
- There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.
- There must be a way for an individual to correct or amend a record of identifiable information about him.
- 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 reasonable precautions to prevent misuse of the data.

These principles provide ways for librarians to frame discussions about and approaches to addressing privacy. For example, the first principle, on notice, would suggest that libraries should provide some mechanism for alerting library users about any data collected about them during the course of their use of library services and resources. Privacy policies posted to websites are a common vehicle for notice, though debates rage about whether policies should be simple or thorough. The notice-and-choice model for privacy is much criticized as inadequate for many reasons, but it remains the foundational principle for much of privacy law and policy, especially in the United States.

---


61 Sec’y’s Advisory Comm. on Automated Pers. Data Sys., supra note 60, at 41.

62 California’s Online Privacy Protection Act (CalOPPA), Cal. Bus. & Prof. Code §§ 22575–22579 (2014) (requiring the posting of website privacy policies if the website targets any California residents and as a practical matter sets the standard for websites with national use); see also State Laws Related to Internet Privacy, Nat’l Conference of State Legislatures, http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx/#Policies (last visited Sept. 24, 2014) (providing a summary of state laws affecting website privacy policies). See Susan Gindin, Nobody Reads Your Privacy Policy or Online Contract? Lessons Learned and Questions Raised by FTC’s Action Against Sears, 8 NW J. TECH. & INTELL. PROP. 1 (2009) (reviewing the FTC’s finding that Sears’ privacy policy was deceptive because notice of surprising amounts of consumer tracking both online and offline was not adequately disclosed in the privacy policy and user license agreement for software provided by Sears.)
Another influential privacy concept is that of “privacy by design” which a librarian could use as a reminder that privacy should be part of ground-level planning for acquisition of a product or development of a service or structure. This approach was promoted by Ann Cavoukian during her tenure as Information and Privacy Commissioner of Ontario. The principles of privacy-by-design have been outlined as:

1. Proactive, not reactive; preventative, not remedial;
2. Privacy as the default setting;
3. Privacy embedded into design;
4. Full functionality—positive-sum, not zero-sum (multiple, legitimate business interests must coexist with privacy; the requirement of tradeoffs as an outdated notion);
5. End-to-end security—full lifecycle protection;
6. Visibility and transparency; and
7. Respect for the user—Keep it user-centric.

This approach seems abstract and even obvious, but remembering privacy during the excitement or stress of securing a new product or service can be difficult. For example, when a publisher of e-books denies any service to a library for fear that library access controls will not protect the publisher’s return on investment, a library’s most persuasive lead negotiating point may not be user privacy. On the other hand, when a library develops a way for users to keep track of their past circulation records, the library can decide to make the service an opt-in rather than an opt-out default. Other possibilities of privacy-by-design could be making sure that Internet browsers have defaults that would allow users to see privacy-enhancing search options such as DuckDuckGo or Ixquick. Simply including privacy-protecting options as easy choices for library users adds a bit of privacy into the design. Any number of design choices in the library facility can support privacy, including limiting surveillance cameras and providing places like carrels for research that can be shielded from prying eyes. Another common consideration is making a plan for securing law faculty members’ permission regarding requests for books they may already have checked out. For example, faculty may be comfortable with the library identifying them to their law faculty colleagues if they have a book that a colleague is seeking. Or, the library might simply develop a plan to play intermediary on moving the book along from one to the other.

64 See Cavoukian, supra note 63, at 12 (stating “The 7 Foundational Principles of Privacy by Design”).
The Harvard Library’s Stacklife project incorporated privacy into the design of this crowd-sourced indicator of the popularity of particular titles to add value to the online catalog services. The library consulted with experts in data anonymization and devised several strategies for designing the project to provide a vehicle for informed, opt-in consent for library users’ data to be shared and for various ways to mask the library use patterns of individuals who did not opt-in. This project was designed to build on popular reader advisory trends in social media, but library-use privacy commitments prevented the library from the sort of transparency used when all users of these services opt-in to transparency through the terms of the service. At the time of this writing, the project continues to be labeled as a prototype.

**Privacy Risk Analysis or Privacy Risk/Competing Benefit Analysis**

Another approach to privacy is something librarians do regularly—a risk and benefit analysis. The library would evaluate the legal and policy risks for not protecting privacy in a particular way and would also assess the likely benefit of compromising privacy in pursuit of some competing goal. This assessment is, however, not without weaknesses. Both privacy risks and competing benefits are difficult to predict given that information uses evolve in unexpected ways. Nonetheless, librarians can assess the risks and benefits that are predictable.

This process is especially important in situations where allowing individual library users to make discrete choices is not practical. For example, when an interlibrary loan system shares names of individual users with libraries that are not subject to the same level of legal protection for library users, the borrowing library may evaluate that tradeoff and decide that the risk to users’ privacy is low while the benefits to having staff able to exploit the full range of lending libraries as speedily as possible is a better choice. Another solution, however, might be a purchase and overnight delivery from Amazon, in which the name of the library user is not required, so that a new approach can facilitate both efficient library service and patron privacy.

**Privacy Audits (for Privacy and Information Security)**

Privacy audits were heralded by librarians in the years just after passage of the USA PATRIOT Act and were promoted as a way to discover all the ways a library might

---


collect personally identifying information about library users. The idea of reviewing the library’s current information collection and privacy practices, though, is a good precursor to updating a privacy policy and privacy practices. Privacy audits necessarily include data security audits and thorough reviews of staff training practices. A thorough review would address library patron privacy as well as library employee privacy. The Association of Research Libraries created a SPEC Kit on Library Patron Privacy in 2003, but the changes in information technologies makes this resource at best a starting point for an audit of privacy risks.

Refrain from Collecting, Refrain from Storing, Purge

Libraries have also simply refrained from collecting or retaining sensitive data as a way to protect reader privacy. Many ILS systems can be set to disentangle the user record from the book record once the book is returned on time. Other records are more difficult for the library to manage, but the Association of College and Research Libraries has provided some guidance on their Tech Blog to help librarians purge information from public computers through browser settings and other practices. Law libraries might require public patrons to sign into their systems using some identifying information as a way to manage limited resources, but if privacy is part of the design of that system, the library might separate the login from personal identification and therefore limit any computer tracking of that individual, at least through the library’s actions. However, libraries might wish to retain some personally identifying data if they determine, using a privacy risk and competing benefits analysis, that the data is important for other goals such as protecting library rare materials. No one practice will fit every library’s set of contextual factors.

However, if the library collects certain types of personally identifying information, state and other laws might require that certain elements are carefully protected from unauthorized access. Social Security numbers are one example, since this information has been used as a tool for identity-theft. If the library is considering risk, the likelihood that this data would be exposed inappropriately should be evaluated. In fact, since the widespread adoption of state data security breach notification laws, many companies have had to provide this type of breach notification, and privacy lawyers now increasingly recommend the purchase of insurance to handle

---

67 Walt Crawford, *Time for a Privacy Audit*, 34 AM. LIBR. 91 (2003) (urging libraries to review their practices and avoid unnecessary collection and retention of personally identifying records of library use).


the cost of these breaches.\textsuperscript{71} If data, such as Social Security numbers of library users, is not collected, the privacy risks are minimized.

\textbf{Encryption (Data Security as Support for Privacy)}

Encryption is a way of making data unreadable by another unless that reader has a key to decrypt the data. This tool has been the backbone of many security and privacy practices to prevent unintended access. State data security breach notification laws widely provide exemptions for data that was lost or exposed while being encrypted.\textsuperscript{72} Recent reports of encryption vulnerabilities suggest that this approach is not fool-proof, especially when the information is sent over the Internet, but a get-out-of-notification-free card is hard to pass up.\textsuperscript{73} And, as many privacy professionals are conceding, imperfect solutions may nonetheless provide significant protections against all but the most dedicated data attackers.\textsuperscript{74}

Encryption can play a role in a number of services that the library offers. If the library wishes to increase barriers to Internet Service Provider monitoring of information a lawyer might email to herself such as results of a library database search, the library might be able to offer encrypted email.\textsuperscript{75} Likewise, the online search of the library catalog could be offered in encrypted form. Any employee data that might be saved to a laptop or jumpdrive is vulnerable to loss and data security breach, so encryption of these devices could be a reasonable approach to managing that risk.

\textbf{Training Staff, Other Forms of Data Security as Support for Privacy}

Traditionally, library-use privacy was a matter of training staff and instituting proper controls on access to the library’s records and systems, and staff training remains an important component of privacy and security in the library. Emerging concerns include risks that libraries are sharing patron records with many multi-library systems that support other library goals such as backup systems for data, interlibrary loan, and

\textsuperscript{71} J. Andrew Moss, \textit{Enhancing the Brave New World of Cyber Liabilities and Insurance Coverage}, 42 SPG-Brief 28, 31 (2013) (reviewing the increased occurrence and costs of data security breaches and recommending, “A critical piece of a comprehensive breach response plan should be insurance”).


\textsuperscript{75} Phetplace, \textit{supra} note 70.
Law school library directors can work with campus library and IT administrators to make sure contract terms and practices like destruction of stale records are in order.\textsuperscript{76} Parent institutions often have strong policies in place, but librarians might need to educate IT and even university counsel on the need to comply with state library privacy laws. Sometimes, a scholarly communications librarian can be a terrific intermediary and advocate for improvements in these areas.

Staff orientation programs should include training for staff members and any student workers who have access to circulation, interlibrary loan, and both public and staff computers. Law school libraries can generally rely on parent institutions for guidelines about employee privacy including public records issues for public institutions. Policies and procedures should outline how staff should respond to requests for access to patron and employee information. The Edward Snowden revelations suggest that library-specific requests for information have been replaced by government programs to gain access to information traffic through Internet and phone service providers, but libraries should nonetheless provide staff with clear guidelines. Perhaps the most high-profile challenge to the USA PATRIOT Act came from a librarian working for a library network.\textsuperscript{77}

Even old-school simple security is still important. Access to information should be limited to staff who need access to perform their jobs; discarded documents with sensitive information should be shredded; retired computers should be carefully scrubbed of data; and file cabinets (physical or virtual) with employee records and Social Security numbers should be locked. These types of security measures are not unique to libraries, and so the parent institution may be the best source for librarians needing to monitor current reasonable practices.

\textbf{Practical Obscurity}

Practical obscurity is an important component in any library’s honest assessment of privacy for library users or for privacy of individuals represented in the special collections or scanned content. Few libraries will actively seek to employ practical obscurity techniques, but the practical obscurity lens for privacy is likely to be a factor and assessing new approaches to providing library services. In most cases, if a library is conducting a cost/benefit analysis, the loss of practical obscurity is a measure of decreasing privacy protection for which a library should account.


Librarians might decide to introduce some new form of privacy protection to balance the loss of practical obscurity. For example, library users enter many libraries without having to identify themselves, and although their presence in the library is observable by others visiting the library, social norms and other practical realities come together to provide barriers to surveillance that make the visit somewhat confidential. Disruptive technologies, though, can weaken this type of practical obscurity, and libraries might need to consider how to address the new realities of library security surveillance cameras, library patrons’ use of smartphones with video capabilities and ease of posting to social media, and the introduction of other technologies such as face recognition technology. Librarians could balance the loss of practical obscurity by positioning security cameras so that they do not record details of information sought in the library and by introducing new policies prohibiting video recording of people in the library without their permission.

Practical obscurity applies to privacy protection for individuals represented in traditional library collections as well. Although libraries proudly offer open stacks, laudably available to the general public, newer, disruptive technologies can remove traditional barriers to access such as travel to the library during hours the facility is open and finding and perhaps paying for parking. Although libraries proudly offer online catalogs freely searchable through the Internet, a scanned, keyword searchable set of special collection documents discoverable through general search engines removes barriers of selecting a specific OPAC and knowing how to search a bibliographic record rather than a full-text document. Librarians have pointed out the privacy reducing role of Internet access to full-text documents as compared with traditional “public access” to a library stacks collection and have articulated balancing activities such as redaction of identity-theft enabling data. The privacy protecting role of practical obscurity has some grounding in the law and has been promoted by scholars as a way for the law to match individuals’ expectations.

---

78 Tammy A. Hinderman, *State Law Library Gets A 21st Century Makeover: How to Use the New Research Tools*, 32 MONT. LAW. 6 (2006) (describing how the library’s digitization of court briefs was interrupted by the realization that with the loss of practical obscurity, the library was facilitating identity theft with the posting of briefs and attachments that contained information such as Social Security Numbers, and describing the library’s decision to remove some content and redact others from the scanned material); see also David S. Byrne, *Access to Online Local Government Records: The Privacy Paradox*, 29 LEGAL REF. SERV. Q. 1 (2010) (describing the loss of practical obscurity in the context of access to court records through visits to the courthouse compared with free access through the Internet.)

Redacting, or Otherwise Scrubbing Information

Like encryption, redaction is an imperfect yet useful approach for balancing privacy and access to information. While encryption is intended to limit access to authorized users of information, redaction is generally used to provide wide access to information while removing from view particular parts of a larger set of information. Redaction is a long-used approach that is increasingly the subject of debate due to the growing risk of the redacted information being discovered through comparisons of redacted data with other publicly or privately available data sets. Individuals who are presumptively made anonymous through redaction might later be re-identified in ways that may not be anticipated at the time of the redaction and release. A number of high profile re-identification events have been seen as spoilers of this somewhat simplistic if sometimes onerous privacy approach. Netflix released redacted data about its users for a competition to develop new services, and researchers were able to use outside data to fill back in the missing data, both identifying individuals and their movie watching habits and putting Netflix at risk for violating both the Video Rental Privacy Protection Act and federal consumer protection laws. An AOL searcher was re-identified in a similar situation after supposedly anonymized data was released. Patients were also re-identified after patient/research data were supposedly anonymized in accordance with the relatively strict guidelines set out in HIPAA regulations.

Defenders of redaction suggest that re-identification is actually still quite rare, and the benefits of redaction are still strong and largely unmatchable by other contrast with the ease of access and searchability of records posted for free or near-free on the Internet). Professor Helen Nissenbaum has pointed out that traditional library print collection access is itself a form of practical obscurity, and sadly, she is probably correct. Conversation with Helen Nissenbaum, Professor, Media, Culture, and Communications, and Computer Science, New York University, Privacy Law Scholars Conference, Berkeley, CA (June 2–3, 2011).


methods.84 Statistical and computational approaches to mining data while protecting some privacy interests are in development, and laws like HIPAA acknowledge that these approaches might substitute for redaction, but these approaches may not be commercially available or cost-effective for libraries in the near future.85

Libraries might consider redaction in the context of digitization of special collections in order to meet the goals of increased access to the collection while reducing the possibility of access to particular pieces of information considered a risk for financial harm or dignitary harm. For example, libraries might scan court records otherwise unavailable electronically and then redact Social Security and bank account numbers before the records are posted freely to the Internet.86 State and federal court rules for e-filing and state laws for identity-theft and data security breach notification laws could serve as law and policy guidelines for such a project.87 Other types of data that might be redacted move into dignitary harm, and libraries are likely to feel more concerned about making choices in these categories because United States law and culture norms are not settled on which types of dignitary harms are worthy of protection. However, libraries could look to other professional ethics or best practices for guidance, for example, following journalistic ethics and choose to redact names of rape victims.88

84 Cavoukian, supra note 74.
85 Andrew Chin & Anne Klinefelter, Differential Privacy as a Response to the Reidentification Threat: The Facebook Advertiser Case Study, 90 N.C. L. REV. 1417 (2012) (reviewing whether “differential privacy” techniques of querying big data have been used by Facebook, identifying possible other applications, and considering where existing law could recognized this technique as satisfying privacy requirements).
86 Hinderman, supra note 78, at 6 (describing how the library’s digitization of court briefs was interrupted by the realization that with the loss of practical obscurity, the library was facilitating identity theft with the posting of briefs and attachments that contained information such as Social Security Numbers, and describing the library’s decision to remove some content and redact others from the scanned material).
The case for redaction of scanned content is one of balancing the loss of practical obscurity with some other form of privacy protection. Another way of considering redaction is that it supports to some extent the Fair Information Practice Principle of avoiding the surprise of an individual who finds that shared information is later used in an unexpected way. Similarly, the theory of contextual privacy, formulated by Helen Nissenbaum, might be a lens for considering that litigants expected information to be practically accessible to attorneys and parties to the litigation. On the other hand, libraries could consider law and policy that argues for transparency in court records or for an expiration of privacy interests after a certain period of time and decide that redaction is not appropriate for court records. Applicable law is still largely underdeveloped, and librarians and others may need to engage in development of best practices guidelines.89

Other library collection scanning projects might involve books no longer in copyright. Presumably, publishers have already assessed privacy risks, since the books were intended for wide distribution.90 Another scenario in which libraries might redact information is in response to a public records request. Libraries that are public institutions might redact records provided through public records requests in order to prevent identification of particular library users protected by state library privacy laws or by FERPA or to comply with state employee privacy laws.91

**Contracting for Privacy**

Contracting for privacy is an important strategy for librarians. Law school libraries have transformed in the past decade or more into what John Palfrey has called “digital-plus,” meaning we are primarily libraries of electronic resources, and in this environment much of the digital content proprietary and managed by intermediaries with whom the library would have a contract governing access.92 Data collection and analysis of individual readers unimaginable only a few years ago are potentially open to technological innovation unless contracts specifically prohibit such practices because privacy law and privacy policy are unsettled. Negotiating for privacy, however, can be difficult because the terminology can be confusing and because

---


90 See James Grimmelman, Speech Engines, 98 MINN. L. REV. 868, 939 (2014) (concluding that the Google Books project did not need to incorporate privacy considerations because books represent content that was presumably already vetted for privacy concerns by its author and publisher both as a policy matter and as a risk of liability under privacy torts like public disclosure of private facts, a tort recognized in some states).


librarians, like many consumers, do not always have a great deal of bargaining power. Kindle readers, Overdrive e-book systems, LexisNexis, Westlaw, and Bloomberg Law all are designed to track individual readers for any number of reasons including digital rights management and tailored interfaces. Fortunately, providers of legal databases should be familiar with attorneys’ need to protect the confidentiality of their research, so while individuals are tracked, contracts should specify that no third parties will gain granular access to usage data. Nonetheless, librarians should be alert to the possibility that their contract with a database provider may not prevent the provider from attempting to override user privacy terms through an end-user license that governs downloading of a related mobile application or personalized access. Overall, the challenges in this area are many and are likely expanding.

Alan Rubel and Mei Zhang reviewed database contracts of university libraries at public institutions and found that libraries have room to improve to protect the privacy of patrons using these databases, particularly in terms of limiting publishers’ sharing of usage data with third parties. They also suggest that terms requiring libraries to divulge patron information for non-authorized use investigations could run afoul of library privacy laws.

Any number of technologies used by libraries could include contract terms for privacy. Integrated library systems and cloud storage provider contracts should probably be reviewed for terms relating to potential mining of the library data, what state or country the data is stored, who has access to the data, and how the data is secured. And, although the warning may seem to veer into the tinfoil hat category of privacy anxieties, libraries should also be alert to contracts governing technologies that are part of the so-called “Internet of Things” including smartgrid sorts of furniture and lighting.

93 B. J. Ard, Confidentiality and the Role of Third Parties: Protecting Reader Privacy in the Age of Intermediaries, 16 YALE J. L. & TECH. 1, 42–45 (2013) (describing how Amazon emailed individuals who had checked out Kindle e-books from libraries and suggesting the libraries have little bargaining power with Amazon).
94 Klinefelter, supra note 13.
96 Id.
**Trading Reader Privacy for Content Privacy**

The requirement that a researcher identify himself and the purpose of his research is used in a number of regulated contexts, including gaining access to credit information and to patient data for medical research purposes. This barrier to access burdens the researcher’s privacy but furthers some interests commonly associated with privacy for individuals represented in the content.

Keeping track of who uses library resources is how a library protects its inventory, evaluates return on investment, complies with obligations to restrict subscription database access to users authorized under licensing terms, and gains insights that can guide marketing of library services and collections. Truly private, anonymous use of libraries would interfere with these goals, so libraries work to limit the burdens on library user privacy in other ways. But privacy burdens on library users can also be used to meet the goal of protecting the privacy of persons whose sensitive information is contained in a special collection. When libraries have special collections known to contain sensitive information, one approach to limiting access to create an application process in which library users must identify themselves and the purpose of their research, to limit privacy risks for individuals represented in the content. For example, researchers who promise that they will not publish bank account numbers that appear in a special collection might be given access to that special collection. This approach is sometimes used for management and even as a condition for receipt of donated special collections.

**Extending Privacy Choices to Library Users and Educating Users about Privacy**

Librarians generally prefer to let library users make their own choices about their reading interests, and most of us would prefer to let them make choices about the privacy aspects of that reading as well. The Fair Information Practice Principles are grounded in this approach. But, sometimes libraries must make a global choice or a default choice on behalf of library users. Notice and Choice model has been criticized as untenable since consumers have little way to make informed choices if indeed there are choices beyond take-it-or-leave-it.

---


100 Sax, *supra* note 51 (noting a variety of access options for donated special collections including limiting access to an exclusive group).

101 Anita Allen goes so far as to recommend that privacy be imposed upon individuals to some extent in order to protect the societal benefits from privacy. *ANITA ALLEN, UNPOPULAR PRIVACY* (2011).
Nonetheless, libraries can offer some options to its users. The catalog might be offered for fast, unencrypted access as well as encrypted searching which might be a slower option. A library user might be offered the ability to opt-in to the library’s retention of all records of books that person has checked-out. Any number of social services, like the posting of library users’ reviews of books in the catalog, might be available through an opt-in model like Amazon provides. To support library users in making these choices, the law library’s website privacy policy might offer both a short version and a long version explanation of the implications of these options.

Libraries might have new value if the growth in tracking and surveillance creates more backlash because libraries are positioned to market some services as providing a sort of privacy-intermediary between the researcher and online trackers. Libraries can play this role through many ways by offering researchers computers through which research can be conducted without tracking an individual’s browser or cell phone identifier or other technological proxies for a particular person. In effect, the library would be highlighting or even creating privacy choices for its users, some who may want more privacy for some types of research and less privacy for other types of research.

Library directors might also support efforts to provide broader education about privacy or even promote privacy choices. Many privacy risks are opaque to library users and all consumers, especially in the context of new information technologies which appear to deliver services and content for “free” while monetizing consumer tracking data. Libraries can and perhaps should play a role in bringing more transparency to debates about appropriate tradeoffs between information privacy and competing goals. The American Library Association’s Office of Intellectual Freedom has chosen to promote privacy through an educational program of “Choose Privacy Week” which organizes and supports a variety of events across the country.

---

102 Some librarians have advocated for privacy protections through the installation of self-checkout stations. A study at Central Michigan University’s Park Library found that circulation of select lesbian, gay, bisexual, and transgender materials circulated 20% more through self-check than at a staffed desk and concluded that patrons appreciated this type of library privacy. Stephanie Mathson & Jeffrey Hancks, Privacy Please? A Comparison Between Self-Checkout and Book Checkout Desk Circulation Rates for LGBT and Other Books, 4 J. LIBR. ACCESS 27 (2006). Because the law addresses many sensitive topics, this self-checkout approach could be a good development for law school libraries and might also help with library staffing efficiencies. Of course, this 2006 article predated much of the news of extensive tracking through electronic systems and widespread government surveillance, so 2014 users might feel differently about a choice between a library staff member human eyes and the possibility that an electronic system might track them in some more sinister way.


104 See Chris Jay Hoofnagle & Jan Wittington, Free: Accounting for the Costs of the Internet’s Most Popular Price, 61 UCLA L. REV. 606 (2014) (exploring the harms that consumers suffer when they are misled by the labeling of services as free rather than services offered in exchange for personal information).
during the first week of May. The international Data Privacy Day, February 28, is another galvanizing force that libraries can use as a basis for events relating to privacy.

**Conclusion**

Law library directors are not alone if they feel overwhelmed by the fast-changing mysteries of information privacy threats, the vagaries of privacy benefits and risks, questions of the worthiness of competing interests, the hit-and-miss nature of privacy law, and the uncertain efficacy of particular approaches. Staying informed is a constant challenge, and gaining insights into innovations in data collection can to inspire either an affinity for tinfoil hats or an impulse to don a wearable computer and perhaps nothing else. Despite the messiness of the issues, though, privacy is an area that law library directors can embrace with true legitimacy. We are experts in information management and in the law, and we have a collective commitment to privacy that is part of our larger professional brand. Librarians have an opportunity to provide leadership for managing information and information privacy within our home institutions and beyond.

Privacy is a topic that can be incorporated into law librarians’ teaching, writing, speaking, and advocacy. A few of us teach privacy law courses, and others cover aspects of privacy in courses such as cyberspace law, law & computers, advanced legal research, or information ethics. Conducting research is surely our domain, and shaping that research into publications and presentations on privacy topics supports reflection and develops expertise. In addition, engagement in national and local debate and initiatives relating to privacy can be an important way for law library directors and other librarians to provide leadership in this area. We are important stakeholders in debates about how to appropriately integrate privacy into the evolving information culture because we are trusted to embrace innovation and also maintain the long view that emerges from traditions of information collection, access, and preservation.

My hope is that this overview of the law and policy of library privacy and highlights of privacy approaches for libraries not only demonstrates the complexity of this area but also provides support for librarians who must forge a path in the midst of rapid change and competing values.

---