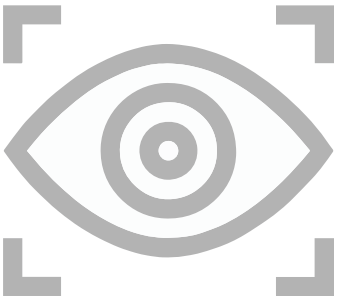
2023

Building a Culture of Privacy through Collaborative Policy Development

Margaret Heller



CHAPTER 14

BUILDING A CULTURE OF PRIVACY THROUGH COLLABORATIVE POLICY DEVELOPMENT

Margaret Heller

INTRODUCTION

Plenty of resources exist for understanding and protecting patron privacy in libraries. So too does governmental pressure, particularly for institutions subject to the European Union's General Data Protection Regulation (GDPR) or similar US state laws. While at some levels there are clearly articulated visions around the privacy of library users, the implementation of privacy practices at the local level remains spotty. Some of this is due to limited time or resources, but some of it is a lack of culture around privacy norms within institutions. Building that culture will mean that every decision someone makes at their job in the library will consider patron privacy to some degree, even if individuals disagree on appropriate measures. Like all cultural shifts, it takes time and empathy to help people to see the benefits and

requirements of new ways of thinking, and creating tangible exercises for working through these challenges is one way to address them.

I suggest ways of building and maintaining a culture of privacy through the act of writing and revising a privacy policy based on my experience at Loyola University Chicago. When approached as a holistic project to understand why decisions have been made a certain way in the past and how to shift—or radically transform—that decision-making, rewriting policy can be transformative for institutions. The process is certainly no panacea, but with a document in place and widely accepted, the process of periodic review and revision can maintain practices throughout time. More than the specific items to include in a policy, which are well-covered by many resources, this chapter guides you in how to think about decision-making as part of building or maintaining privacy culture through a case study of writing this specific policy.

LITERATURE REVIEW

In planning a project to create a culture of privacy, it is important to consider the role of staff across the library in planning and implementing policy, why privacy can be different from other aspects of library practice, and particular considerations for academic libraries in the age of learning analytics.

Changing institutional practices and professional norms requires a healthy organizational culture that can lead to overall culture shifts in the library. Understanding how organizational culture functions in libraries has been an ongoing topic of research, recently with a particular focus on the dysfunctional elements of library culture that lead to low morale and disengagement as people are not able to effect real change in areas they value. Kaetrena Davis Kendrick's 2017 work demonstrates that one way that low morale manifests for faculty librarians is a lack of the type of collaboration and professional development that would lead to cultural change, particularly at the larger institutional level.[1] That scholarship did not include staff working in academic libraries who are critical in making privacy decisions. The 2022 study by Glusker and colleagues built on Kendrick's work to look specifically at staff. While many of the participants in this study had reasonably good morale, they found the most powerful impact on staff morale was a librarian/staff divide, where staff found themselves blocked from influencing library policy, even when they have direct interactions with students.[2] Including people at all levels of institutional power in decision-making in a real way is part of maintaining a healthy culture, particularly when it comes to privacy issues.

Patron record management tends to have more legal requirements or external policies that libraries must follow than other areas of library service, but inclusive cultures can improve privacy practices at all levels. In many cases, the specific requirements around privacy may be set at a state level and interact with other education privacy regulations like FERPA. While institutions may wish to leave such decisions in the hands of institutional lawyers, individuals will still have to face daily decisions about their work. This includes front-line library workers like circulation desk clerks who may not know policy and may not understand the reasons for privacy in library records unless they have been involved in active training or had a say in the policy. This has been the case for decades, of course. In the 1970s and '80s, a government surveillance program involved the Internal Revenue Service looking for circulation records to find potential readers on subversive topics, to which Bruce S. Johnson responded in a 1989 article. Johnson argues that a 1970 ALA statement, "Advisory Statement to U.S. Libraries from the American Library Association," established a strong precedent for privacy before any case law established legal precedent and led to the end of the IRS program.[3] In this pre-internet age, Johnson lays out the thought experiment of the circulation clerk who is asked by law enforcement to share borrowing records and the role that library administrators must play in informing and empowering all staff members to resist non-lawful governmental or other requests for patron records (for example, from journalists).[4]

Over the following years, the increasing role of the internet and then the PATRIOT Act created a flurry of calls for privacy policies and a greater understanding of privacy in libraries, especially as the ALA produced the original versions of the Privacy Tool Kit in 2002. Karen Coombs noted in 2004 that libraries were just beginning to work to implement the Privacy Tool Kit but that technological advances made policies irrelevant quickly.[5] By 2007, when Stacey Voeller analyzed existing privacy policies at academic libraries, she found the majority were either nonexistent or cursory and did not reflect ALA recommendations.[6] The worry in the early 2000s was that libraries would no longer be trusted with privacy the way they had been due to the threats from the PATRIOT Act without close attention to professional standards and conduct, including a privacy audit.[7] Over the past decade, the issues have shifted somewhat to focus more on potential social or big data analytics use of library data, which has, of course, also expanded exponentially beyond borrowing records. A 2012 study by Michael Zimmer indicated that there was reason to be concerned that attitudes toward privacy were loosening compared to 2008 as the overall culture changed and perhaps was related to younger librarians who were less concerned about online privacy.[8] While a cultural move to

social media seems here to stay, recent work by Kyle M. L. Jones et al. indicates that rather than governmental oversight, the current generation of students is far more concerned about privacy in social media and the commercial realm and generally trusts libraries and universities, though without necessarily knowing what data they are collecting or fully understanding the purpose of this data collection.[9]

Yet that study also found that for students, the modern university may be perceived to be a place where intellectual curiosity or questioning is subject to oversight.[10] What academic libraries choose to do with data collection has a lot to do with library culture as well as overall institutional culture. One of the major problems with privacy in academia is that it has not always been a concern at an institutional level. It does limited good for the library to protect users if every other unit on campus is gathering and compiling data about student use of other systems on campus, such as learning management platforms. Library staff can advocate for more limited data collection, even if they cannot prevent it. Working together across areas not always considered in the privacy discussion, such as collection management and instruction, is more likely to create a staff who is knowledgeable about the privacy ecosystem and able to have these conversations with campus partners.[11] This is an issue for faculty as well. Traditionally, academic freedom purports to protect individuals' research interests, but this has only ever applied really to a small number of people, and with tenure-track positions now in the minority, there are even fewer people who will feel completely comfortable with their research interests not being protected until they are ready to make it public.[12]

The culture of privacy in libraries is not monolithic. For example, in a 2019 editorial, Russell Michalak and Monica Rysavy made an argument that gathering personally identifying information about individuals is part of the library's mission to improve service. In the editorial, they have a wish list for even more information at the vendor level about which individuals are using which features.[13] Jones et al. question this level of tracking without meaningful education and co-creation of procedures with students.[14] Such tensions point to the need for open discussions about privacy in libraries.

Despite a recent cultural trend to talk about social media and learning analytics, the threat from government oversight over what libraries buy and patrons choose to read has not disappeared, particularly at the state and local level, and this requires ongoing attention. In mid-2022, we have once again found an inflection point in the role of libraries in privacy with the *Dobbs v. Jackson Women's Health Organization* case, which made abortion immediately illegal in several states. Law enforcement used mobile search data to arrest a woman for allegedly purchasing abortion pills.[15] Ensuring that libraries remain a place where people can seek

information without fear of arrest has become a focus of professional concern again, as an August 2022 statement by the ALA Executive Board stating their commitment to protecting patrons from "unwanted surveillance" in researching reproductive health.[16] Beyond abortion, numerous news stories about censorship in schools and public libraries show that a renewed focus on providing an open yet private environment for research is critical.

CASE STUDY OF LOYOLA UNIVERSITY CHICAGO

Creating a Privacy Policy

Loyola University Chicago is a private doctoral-granting university with an enrollment of about 17,000 students, the majority of whom are undergraduates. Starting in fall 2017, I co-chaired a library privacy policy task force. This section describes that work and how we experienced the policy in action while implementing new tools and services.

At Loyola, when we set out to write the policy, our main concern was a push for learning analytics and data warehousing at a campus level. We knew that we had to get ahead of the inevitable push for collating and using library data. At the time, we were barely even aware of the critical role of a policy itself; we just knew we wanted to get the staff talking about privacy and learning what to do, and the release of the ALA Library Privacy Checklists made the work seem more possible. Initially, the Scholarly Communications Committee had discussions that led to the formation of a group. It became clear that to create a comprehensive privacy policy that covered all areas of the library, members from diverse areas with different experiences and expertise would be needed to ensure that all practices and needs were captured. For Loyola, the size of the library staff and its well-established cross-departmental collaborative culture made it straightforward to work with department heads and recruit a member from each department, with some conversations to make sure representatives had a mix of background experience. The team purposely had a mix of department heads, faculty librarians, and staff and had nine members, including two co-chairs. No one from library administration was on the team, but the administration had numerous opportunities to learn about work in progress and had final approval on the policy.

We wrote a formal charge for the group, which was called the "Patron Privacy Task Force," and created a formal project plan to keep on track, given the short timeline of August to December 2017. The project plan defined the stages of work and committee member roles. Initial stages included a reading list of articles (all

of which are cited in this chapter) and resources, such as privacy policies from other libraries, to help committee members get up to speed and create a list of questions that occurred to committee members that we could take into our work. We then conducted an inventory of systems and a privacy audit of those systems. The systems inventory was not intended to suggest that privacy was a technology problem only but rather helped the team identify how data could be jeopardized as it passed between systems. The team structure shone here. For example, we discussed user purchase requests, where we discovered that deleting the user request records from the back end of the catalog is only marginally helpful for privacy since the request was submitted via email to an inbox to which many people have access. The subject liaison knew how faculty wish to request books and have them put on hold, and the acquisitions assistant knew how the orders are placed and tracked. Together, these two understood what needs to happen to make book request records more private in a way that neither could do alone. Discussing these workflows was a critical piece of writing policy since it helped catch easy fixes to privacy problems before we described them in the policy.

We took existing lists of types of systems created by Karen Coyle for privacy audits and filled in the names of our specific software in each category as well as the primary manager for the software. In a few cases, we had elements of library services that used paper forms. We used the ALA Library Privacy Checklists level 1 priorities to create lists of practices that should be addressed. (See the appendix for more on available resources.) While it was straightforward to determine where we had immediate major gaps—for example, we did not have a privacy policy—some projects were more abstract or required coordination with other campus units. In these cases, when we wrote the policy, we tried to be honest about what our limitations were, but this became something we could record as a practice to work toward change.

One of the goals for this project that was not successful was to create an interactive procedures manual that would allow departments to map their procedures to levels of privacy as defined by the Library Privacy Checklist priority actions, which started with steps that all libraries could take and then moved on to more challenging projects. Ultimately, we were only able to review Priority 1 actions, and the interactive procedure manual was too complicated to implement.

Writing the policy was relatively straightforward. My co-chair and I used existing templates and examples from other institutions in the same jurisdiction and type to ensure that the policy was not missing any important features. We knew few people would read a privacy policy, so headings and bullet points helped people to locate the specific information they need. Committee members provided

feedback after discussions in their departments. We also asked a colleague outside the library to read a draft to check for jargon. One other issue to settle before making the policy public was determining our library privacy officer, which is a role suggested by the ALA Privacy Checklists. Ideally, this would be a person with the institutional authority to make decisions or exceptions to policy but with a strong understanding of privacy issues as well. In the case of Loyola, the person selected for this role was not on the committee but had the institutional authority to take complaints and had a general understanding of the issues.

For Loyola, highlighting our new library privacy policy was an important moment that created new opportunities. Presenting the policy at a standing academic technology review committee showcased the library as a resource for privacy questions. Almost immediately, the library received invitations to present to other groups (such as academic departments) and to consult on privacy practices at other campus units. The library was then invited to join a campus information technology-level committee on information security, which since then has had a real impact on privacy on a campus level. One of the strengths of the team was that it was not always the department member on the committee who became the privacy expert for their department; in at least one case, another department member found the process so appealing that they went on to learn more and pursue additional privacy-related projects.

Applying the Privacy Policy

The policy that Loyola created in 2017 positioned the library staff to ask questions about the choices they were making going forward. A yearly review of a policy is warranted, but privacy becomes a de facto question in all projects so the library will be able to make decisions that will not need to be undone at the next review period. Policy revision is a balance: does one change procedures to conform to a better policy or does the policy serve as an aspirational document? Ideally, both should be true. The act of writing and interpreting the policy as a team created an impetus to consider changes to procedures, especially in the moments of crisis that we all experienced throughout the pandemic with a need to reinvent services quickly and do more tracking of users for contact tracing and de-densification. In the normal course of providing library services, we need to balance convenience and privacy for both users and staff.

Two examples from Loyola's experience illustrate this. One is pandemic-based, the other is not. Both took place in 2020 when Loyola adopted OpenAthens as a federated authentication solution while at the same time creating a contactless pickup service—two completely different types of projects involving different

groups within the library but both requiring privacy conversations informed by the privacy policy process.

Adopting a new technology like OpenAthens, and fully evaluating the privacy options and settings, required a great deal of new technical learning and provided opportunities to question privacy practices and needs across our electronic resources as we learned the technology better. We began working on the project well before the pandemic, but the switch to remote work and instruction across campus highlighted the challenges inherent in using solely IP-based authentication, especially one that is locally hosted. EZProxy, our proxy server, is highly configurable to make logging usage more private, but to make it practical for troubleshooting ends up creating logs with very specific information about users and their access, particularly when everyone who uses resources is logging in through the proxy server because no one is in the library's IP range. While we still use EZProxy concurrently for certain resources, we found the process of moving to OpenAthens provided a chance to understand the realities of federated access and attributes.

Federated authentication has the potential to be much more private, but only if it is configured to do so. A proxy server requires running all traffic through a central point, so libraries can and do collect data about what resources particular users are viewing and when. While some of that is useful for troubleshooting, it creates a toxic dataset that without proper maintenance is ripe for misuse. An IP-based authorization solution can be more private, certainly, when users are on campus, but in an environment where few if any people are in the IP range, the proxy server is always in the way. A federated solution, on the other hand, separates the identification and authentication of a user from what they are authorized to do and can provide relative anonymity for users from both the library and the vendor, but only if the information passed between entities is not identifiable.

OpenAthens itself has a relatively privacy-forward outlook, but it is possible to configure data collection in such a way that could identify individuals.[17] At Loyola, this sort of individual tracking is not part of our library's privacy policy or in its guiding principles; tracking the usage of resources and platform features helps us make general decisions about what to improve. If we desired to find out more about individual needs around the library, we would design a study and have it approved by the Institutional Review Board, which would ensure that we were collecting and reviewing data in an appropriate manner. The concept of collecting everything "just in case" is an overwhelming prospect for how we would go about safely storing that data and analyzing it.

That said, for cost-sharing decisions, it would be helpful to track usage by school or department, but we have found it difficult to release the appropriate attributes in such a way that they would be useful to OpenAthens reporting. The more data that is released, the easier it is to re-aggregate. Releasing personal attributes in a way that a user cannot see is sometimes necessary for access to individual databases such as Elsevier and O'Reilly (among others), but OpenAthens makes it easy to set which attributes are available for authorization versus reporting.

The "go live" date for OpenAthens was in August 2020, but it took almost a year before we felt we had the technology working well enough and had a good enough understanding to revise the privacy policy. This means that at that time, our privacy policy was inaccurate, and that was an uncomfortable feeling. Knowing the technology well enough to understand where privacy leakage can occur takes time, however, and should be an understood part of long-term technical projects.

The time-limited projects of pandemic service warrant close attention to privacy. While the service provided during the pandemic was never going to be exactly the same, it was important to not place people in an even more difficult situation. Establishing a contactless pickup service was one such event—how to balance the need to allow people to pick up books without interacting with staff but also not to make it obvious who was picking up what when. Of course, removing friction from an already potentially stressful situation was necessary. The original plan was very privacy-focused: place books in bags identified only by the last four digits of the patron barcode. Reality very quickly changed this plan: not all students had a barcode on their IDs, and even patrons who did found it difficult to locate their bag on the shelf. This made it necessary for them to talk to the staff in the building for help, which was antithetical to the aims of the project. For that reason, we shifted to last name and barcode for identification. After an introductory period, patron complaints indicated that the bags themselves were a problem. Some people were uncomfortable with the number of plastic bags that they were using in frequent book pickups. Staff found a new solution: reusable bags and a return box for people to return the bags after they had picked up their books.

While we were able to use our 2017 policy for ongoing decision-making, it became clear in early 2021 that a policy rewrite was overdue since it did not accurately reflect the new technical infrastructure of OpenAthens and other procedural changes. We determined that the policy needed to be revised in the summer of 2021. The challenge here was to get people motivated to do the work. With so many projects and competing priorities, the privacy policy was not top of people's minds. In the end, none of the original committee members from 2017 were available,

but we were able to create a new small group that reached out to all the library departments for review and updates.

The tools used in creating the privacy policy can and should be reused in revision. Departments should build a periodic review of the systems they are using that collect personal information, and those can be used to update system inventories. Because we had asked department heads to identify items on the privacy project wish list for annual department goals, there were at least attempts to change practices to meet higher standards. Most practices did and will remain unchanged without external pressures, such as a new system like OpenAthens, or the massive reset that the pandemic required. Rather than feeling despondent about this inertia, a culture of privacy means that even if people are not undertaking big projects to fix privacy problems, they are making a few small decisions that will aid privacy over time or not choosing a new practice that will negatively impact privacy. One example is that Google Analytics released version 4 in October 2020, which is designed to work across the web and apps. The problem is that the limited privacy controls available in earlier versions are no longer available in this version. Thus, a review of the new version showed that upgrading was not necessary and would be deleterious. Google recently announced that it would stop support for the current version, so we will implement Matomo Analytics. These small inflection points create opportunities for knowledge and growth.

BUILDING A PRIVACY CULTURE WITH OR WITHOUT POLICY

While I believe the act of writing a policy can help establish privacy culture, if approached as an inclusive research and education project, libraries can follow the same process to come to a shared privacy understanding, even if the outcome is an internal document or a set of guiding principles rather than a policy. This may be more politically feasible than setting out to write a policy. When it comes down to it, a person with a commitment to privacy will be more efficacious than someone half-heartedly following a policy. As new technology and new challenges to intellectual freedom arise, a written document describing a policy is important, but it is not the only approach. The calls for more training and commitment to privacy have been consistent in the literature, but surveys of actual practice find that institutional follow-through is inconsistent. Technology seems to trend toward more tracking and surveillance, as does higher education. There are few external pressures on libraries to actually "fix" privacy, so we are less likely to apply a lot of resources to do so.

The good news is that privacy is about values and mindset, and a process that instills these will ultimately be more likely to succeed. The library profession is not a monolith when considering privacy. Some want lots of user data, others want none, and most fall in the middle. Privacy advocates may not feel that we have yet earned the right as a profession to be optimistic about the future of privacy in libraries. But creating a core set of staff who feel comfortable with privacy language and decision-making goes a long way to creating an environment at individual institutions where optimism is possible. Such efforts can filter throughout the profession.

Creating that core group of staff who feel empowered starts with culture. Culture is important because it will help when library workers cannot or do not know how to apply legal frameworks to the question of privacy. Most of us receive a cursory overview of privacy laws at some point in our training and may have to undergo more specific training. Understanding how we translate those laws into practical decisions, and where we may need to reject something that feels convenient or necessary in order to protect privacy, is an ongoing set of decisions. Positioning the library as a privacy expert and advocate will help enhance privacy across the institution.

Whether you are starting fresh with no privacy policy at all or revising an old one, a successful culture-building process starts with an inclusive and well-considered team. These will be the people who will understand the policy and be able to adapt procedures to comply with it. Teams should have a mix of perspectives, both in the type of expertise and staff role. A department manager in a public services area and an hourly worker in technical services would both be ideal members of the same team since they will each understand different areas of the library workflow to achieve the same result.

With all such work, questions of authority and ownership may crop up. For some libraries, policy created from grassroots efforts would be a problem. If this is the case at your library and you are not in library administration, your first task will be to find an administrative ally. This may be an area of interest for library leadership, but they may lack knowledge or time to pursue it and will be supportive of others heading up the work. If leadership is not supportive, you might be able to start a learning club or working group to investigate privacy issues and have conversations with colleagues in the same way you would in writing an effective policy. The outcome of this work could lead to more official documents in the future while still building a stronger privacy culture.

A related issue in deciding how to approach your policy is how it sits within a larger legal framework. For example, if your state has specific laws regarding

library privacy, your policy must follow these laws. Certainly, at the very least it should refer to them for individuals to review. Your institution may have additional requirements. For example, some institutions may not allow individual units to create a privacy policy different from the institutional privacy policy. In such cases, it may be possible to write guidelines about specific ways in which the library follows the institutional privacy policy. If it varies significantly, that would be a point of negotiation with the institution.

If a policy per se is not permissible due to campus requirements or other restrictions, a team to investigate privacy best practices and ensure compliance will still help. Either way, you may find that a more experimental and informal process helps to plan the project initially, particularly if there is a lack of existing or up-to-date knowledge. Starting with a systems inventory and privacy audit is a practical way to get into the more theoretical or technical aspects of privacy. Working through a checklist of systems helps a team think across departments about how users interact with different services, leaving their information across systems. As gaps are discovered, the team can create a privacy project wish list to inform future work, which can be revisited on a yearly basis or whenever the library makes a change to technical infrastructure.

Academic governance and policymaking are often left to who shows up and does the work, for better or worse. Proactive policy development by the library can make this for the better. When the university chooses a new technical solution to meet a perceived educational technology need, people with knowledge about privacy must be there to question the tool and push back on usage that is overly prone to surveillance. Taking the time to educate staff and students on privacy gives everyone the tools to see systems through a lens of privacy and to think through issues in a more holistic way. One example of this is with the shift to widespread remote education in 2020, students suddenly had to allow their professors, classmates, and institutions into their private spaces. Students needed advocates for their privacy during that time, and the library is a natural advocate in educational technology spaces on campus if they have already positioned themselves as such or can take the opportunity to do so.

The reality of the work it takes to position the library and its staff as an ally to privacy on campus is not minimal. Creating a collaborative policy is a way to begin this effort, but maintaining the culture of privacy over time is more of a challenge. As with many efforts in planning and administration, without dedicated personnel assigned to the task, work is lodged with ad hoc groups or individuals, and as those individuals develop new interests or leave the library, no one maintains the policy. Regularly updating policies should be part of library work, but with a culture of

privacy, there can be many opportunities for creating better procedures. In an ideal world, the privacy policy will be reviewed yearly or upon the adoption of a new system. The group that reviews it need not be a standing committee but should continue to reflect staff across the library and in different types of roles. Department heads, administrators, and external partners, such as campus IT, should be part of the conversation. Departments can "own" their part of the policy, but given the siloed nature of academic libraries, it will be necessary to make sure that some unit or group "owns" the writing of the policy, with the expectation that the cultural norms may need to be invigorated or enforced over time.

CONCLUSION

It was not until 1938 that the "Code of Ethics for Librarians" explicitly mentioned privacy as a professional library value.[18] In the following years of the twentieth century, changes in overall culture and technology made privacy an even more specific value. Still, given the threats to privacy in the library that have manifested in the last fifty years, many library workers are only dimly aware of these risks, and many libraries have not taken stock of the situation by creating a policy or even guidelines. While there are many legal requirements at the state, federal, and international levels that may affect academic libraries and require them to provide privacy protections, history indicates that the legal threat is not enough. Individuals who value privacy are not enough. They must find collaborators and build a team to begin to change the culture of their libraries and ensure this is a value that does not disappear.

APPENDIX

This is a small selection of the many resources that are available and will help institutions to learn about privacy and create a policy. Choosing the right approach for your context among these resources will take some thought and experimentation.

- "Creating a Privacy Policy from the Ground Up," ACRL TechConnect Blog, https://acrl.ala.org/techconnect/post/creating-a-privacy-policy-from-the-ground-up/. Find more resources and information about this project in this 2018 blog post.
- American Library Association Privacy Advocacy, https://www.ala.org/advocacy/privacy. The American Library Association (ALA) and its divisions have developed several resources to guide the privacy process. These date from the early 2000s in their original form but have been updated and expanded over the years. In recent years, these resources have expanded to become even more accessible, in particular the Privacy Field Guides project, funded by IMLS and led by Erin Berman and Bonnie Tijerina,[19] has created visually appealing and easy-to-understand short guides to every stage of the process and should be a first stop in planning your process and a deeper dive into the additional ALA resources.
- A National Forum on Web Privacy and Web Analytics, https://www.lib.montana.edu/privacy-forum/. The National Forum on Web Privacy and Web Analytics in 2018 was a catalyst for many projects and resources around privacy. The Action Handbook[20] is a useful toolkit for understanding different attitudes to privacy and provides many additional resources for how to gather data responsibly for library planning.
- Digital Library Federation Privacy & Ethics in Technology, https://wiki.diglib.org/Privacy_and_Ethics_in_Technology. This working group has created a number of reports and toolkits[21] to understand privacy in libraries in different areas, and their work is ongoing. Many members of this group also participated in the National Forum on Web Privacy and Web Analytics and have written about the participatory nature of both groups and the challenges and opportunities.[22]

ACKNOWLEDGMENTS

I would like to thank Niamh McGuigan, now at Brown University, who co-chaired the original Patron Privacy Task Force and co-wrote the policy with me. I would also like to thank Hong Ma, Head of Library Systems, and the entire Loyola

University Chicago Systems team who have helped with many of the planning and technical elements of privacy projects.

NOTES

1. Kaetrena Davis Kendrick, "The Low Morale Experience of Academic Librarians: A Phenomenological Study," *Journal of Library Administration* 57, no. 8 (November 17, 2017): 861, https://doi.org/10.1080/01930826.2017.1368325.
2. Ann Glusker et al., "'Viewed as Equals': The Impacts of Library Organizational Cultures and Management on Library Staff Morale," *Journal of Library Administration* 62, no. 2 (February 17, 2022): 167–68, https://doi.org/10.1080/01930826.2022.2026119.
3. Bruce S. Johnson, "A More Cooperative Clerk: The Confidentiality of Library Records," *Law Library Journal* 81, no. 4 (1989): 776.
4. Johnson, "A More Cooperative Clerk," 800–801.
5. Karen A. Coombs, "Walking a Tightrope: Academic Libraries and Privacy," *The Journal of Academic Librarianship* 30, no. 6 (November 1, 2004): 493–94, https://doi.org/10.1016/j.acalib.2004.08.003.
6. Stacy Voeller, "Privacy Policy Assessment for the Livingston Lord Library at Minnesota State University Moorhead," *Library Philosophy & Practice* (November 2007): 9–10.
7. Chris Matz, "Libraries and the USA PATRIOT Act: Values in Conflict," *Journal of Library Administration* 47, no. 3–4 (May 2008): 84, https://doi.org/10.1080/01930820802186399.
8. Michael Zimmer, "Librarians' Attitudes Regarding Information and Internet Privacy," *The Library Quarterly: Information, Community, Policy* 84, no. 2 (2014): 147, https://doi.org/10.1086/675329.
9. Kyle M. L. Jones et al., "'We're Being Tracked at All Times': Student Perspectives of Their Privacy in Relation to Learning Analytics in Higher Education," *Journal of the Association for Information Science and Technology* 71, no. 9 (2020): 1053, https://doi.org/10.1002/asi.24358.
10. Jones et al., "'We're Being Tracked at All Times,'" 1052.
11. Emily Singley, "A Holistic Approach to User Privacy in Academic Libraries," *The Journal of Academic Librarianship* 46, no. 3 (May 1, 2020): 2, https://doi.org/10.1016/j.acalib.2020.102151.
12. "The Annual Report on the Economic Status of the Profession, 2020-21," American Association of University Professors, AAUP, June 28, 2021, 14, https://www.aaup.org/report/annual-report-economic-status-profession-2021-22.
13. Monica D. T. Rysavy and Russell Michalak, "Data Privacy and Academic Libraries: Non-PII, PII, and Librarians' Reflections (Part 1)," *Journal of Library Administration* 59, no. 5 (July 4, 2019): 532–47, https://doi.org/10.1080/01930826.2019.1616973.
14. Jones et al., "'We're Being Tracked at All Times,'" 1055.
15. Patricia Hurtado and Francesa Maglione, "In a Post-Roe World, More Miscarriage and Stillbirth Prosecutions Await Women," Bloomberg.com, July 5, 2022, https://www.bloomberg.com/news/articles/2022-07-05/miscarriage-stillbirth-prosecutions-await-women-post-roe.
16. "American Library Association (ALA) Condemns Proposed State Legislation Limiting Access to Information on Reproductive Health," American Library Association, News and Press Center, August 9, 2022, https://www.ala.org/news/press-releases/2022/08/american-library-association-ala-condemns-proposed-state-legislation-limiting.
17. "About Reports and Privacy," OpenAthens, OpenAthens Documentation, accessed January 14, 2022, https://docs.openathens.net/libraries/about-reports-and-privacy.
18. Johnson, "A More Cooperative Clerk," 774.
19. "Privacy Advocacy Guides for Libraries," 2019, https://www.imls.gov/grants/awarded/lg-36-19-0073-19.
20. "A National Forum on Web Privacy and Web Analytics: Action Handbook," Montana State University, April 30, 2019, https://doi.org/10.15788/20190416.15446.

21. "Privacy and Ethics in Technology," DLF Wiki, January 12, 2022, https://wiki.diglib.org/Privacy_and_Ethics_in_Technology.
22. Scott W. H. Young et al., "Participatory Approaches for Designing and Sustaining Privacy-Oriented Library Services," *Journal of Intellectual Freedom & Privacy* 4, no. 4 (July 31, 2020): 3–18, https://doi.org/10.5860/jifp.v4i4.7134.

BIBLIOGRAPHY

American Association of University Professors. "The Annual Report on the Economic Status of the Profession, 2020-21." AAUP. June 28, 2021. https://www.aaup.org/report/annual-report-economic-status-profession-2021-22.

American Library Association. "American Library Association (ALA) Condemns Proposed State Legislation Limiting Access to Information on Reproductive Health." News and Press Center. August 9, 2022. https://www.ala.org/news/press-releases/2022/08/american-library-association-ala-condemns-proposed-state-legislation-limiting.

———. "Library Privacy Checklists." Advocacy, Legislation & Issues. February 2, 2017. https://www.ala.org/advocacy/privacy/checklists.

Coombs, Karen A. "Walking a Tightrope: Academic Libraries and Privacy." *The Journal of Academic Librarianship* 30, no. 6 (November 1, 2004): 493–98. https://doi.org/10.1016/j.acalib.2004.08.003.

Coyle, Karen. "Library Privacy Audits." kcoyle.net. Accessed January 14, 2022. http://www.kcoyle.net/privacy_audit.html.

DLF Wiki. "Privacy and Ethics in Technology." January 12, 2022. https://wiki.diglib.org/Privacy_and_Ethics_in_Technology.

Glusker, Ann, Celia Emmelhainz, Natalia Estrada, and Bonita Dyess. "'Viewed as Equals': The Impacts of Library Organizational Cultures and Management on Library Staff Morale." *Journal of Library Administration* 62, no. 2 (February 17, 2022): 153–89. https://doi.org/10.1080/01930826.2022.2026119.

Hurtado, Patricia, and Francesca Maglione. "In a Post-Roe World, More Miscarriage and Stillbirth Prosecutions Await Women." Bloomberg.com. July 5, 2022. https://www.bloomberg.com/news/articles/2022-07-05/miscarriage-stillbirth-prosecutions-await-women-post-roe.

Institute of Museum and Library Services. "Privacy Advocacy Guides for Libraries." 2019. https://www.imls.gov/grants/awarded/lg-36-19-0073-19.

Johnson, Bruce S. "A More Cooperative Clerk: The Confidentiality of Library Records." *Law Library Journal* 81, no. 4 (1989): 769–802.

Jones, Kyle M. L., Andrew Asher, Abigail Goben, Michael R. Perry, Dorothea Salo, Kristin A. Briney, and M. Brooke Robertshaw. "'We're Being Tracked at All Times': Student Perspectives of Their Privacy in Relation to Learning Analytics in Higher Education." *Journal of the Association for Information Science and Technology* 71, no. 9 (2020): 1044–59. https://doi.org/10.1002/asi.24358.

Kendrick, Kaetrena Davis. "The Low Morale Experience of Academic Librarians: A Phenomenological Study." *Journal of Library Administration* 57, no. 8 (November 17, 2017): 846–78. https://doi.org/10.1080/01930826.2017.1368325.

Matz, Chris. "Libraries and the USA PATRIOT Act: Values in Conflict." *Journal of Library Administration* 47, no. 3–4 (May 2008): 69–87. https://doi.org/10.1080/01930820802186399.

Michalak, Russell, and Monica D. T. Rysavy. "Data Privacy and Academic Libraries: Non-PII, PII, and Librarians' Reflections (Part 2)." *Journal of Library Administration* 59, no. 7 (October 2019): 768–85. https://doi.org/10.1080/01930826.2019.1649969.

Montana State University, Scott W. H. Young, Jason A. Clark, Sara Mannheimer, Lisa Janicke Hinchliffe, and University of Illinois at Urbana-Champaign. "A National Forum on Web Privacy and Web Analytics: Action Handbook." Montana State University. April 30, 2019. https://doi.org/10.15788/20190416.15446.

Nichols Hess, Amanda, Rachelle LaPorte-Fiori, and Keith Engwall. "Preserving Patron Privacy in the 21st Century Academic Library." *The Journal of Academic Librarianship* 41, no. 1 (January 1, 2015): 105–14. https://doi.org/10.1016/j.acalib.2014.10.010.

OpenAthens. "About Reports and Privacy." OpenAthens Documentation. Accessed January 14, 2022. https://docs.openathens.net/libraries/about-reports-and-privacy.

Singley, Emily. "A Holistic Approach to User Privacy in Academic Libraries." *The Journal of Academic Librarianship* 46, no. 3 (May 1, 2020): 102151. https://doi.org/10.1016/j.acalib.2020.102151.

Voeller, Stacy. "Privacy Policy Assessment for the Livingston Lord Library at Minnesota State University Moorhead." *Library Philosophy & Practice* (November 2007): 1–29.

Young, Scott W. H., Paige Walker, Shea Swauger, Michelle J. Gibeault, Sara Mannheimer, and Jason A. Clark. "Participatory Approaches for Designing and Sustaining Privacy-Oriented Library Services." *Journal of Intellectual Freedom & Privacy* 4, no. 4 (July 31, 2020): 3–18. https://doi.org/10.5860/jifp.v4i4.7134.

Zimmer, Michael. "Librarians' Attitudes Regarding Information and Internet Privacy." *The Library Quarterly: Information, Community, Policy* 84, no. 2 (2014): 123–51. https://doi.org/10.1086/675329.