Technologies of Surveillance Group Advocacy Action Plan

Eliza Bettinger, Mahrya Burnett, Michelle Gibeault,
Yasmeen Shorish, Paige Walker

September 2019

DOI 10.17605/OSF.IO/J5K8S

Digital Library Federation (DLF)
https://diglib.org

DLF is a program of the
Council on Library and Information Resources
2221 South Clark Street
Alexandria, VA 22202
https://clir.org

Introduction

A lack of privacy inhibits intellectual freedom. According to research, human behavior changes when an individual thinks that their activities might be surveilled, even when the avoided behavior is legal.[1]

Privacy is foundational to intellectual freedom, to the right to explore and experiment with information, ideas, and creative expression.[2] It is also foundational to a free society, like other civil liberties such as freedom of speech, religion, and assembly. Although you may personally may feel that you have "nothing to hide," perhaps you do value living in a society that produces a wide variety of new ideas, new science, new political arguments, and new creative arts. Similarly, although you may feel that you have nothing controversial to say, you may value living in a society where freedom of speech is protected.[3] In short, the benefit to society of a right to privacy is much greater than the benefit to any one individual.

This document will assist librarians who want to communicate about the sensitivities of library patron data with those serving in decision-making roles. As librarians discuss how patron data is used and shared in wider institutional and societal contexts, it is essential to understand why librarians choose to share and analyze some patron data, while at other times choose to protect, limit the collection of, and purge that data. In many cases, libraries may be mandated by their governing bodies (i.e., university administrators, city councils, boards) to provide data related to the use of the library

1 There has been much research in this area. The following is a small sampling: Melissa Bateson, Daniel Nettle, and Gilbert Roberts, "Cues of Being Watched Enhance Cooperation in a Real-World Setting," *Biology Letters* 2, no. 3 (2006): 412-414 https://doi.org/10.1098/rsbl.2006.0509; Pierrick Bourrat, Nicolas Baumard, and Ryan McKay, "Surveillance Cues Enhance Moral Condemnation," *Evolutionary Psychology* 9, no. 2 (2011):193-199 https://doi.org/10.1177/147470491100900206; Kevin J. Haley and Daniel M. T. Fessler, "Nobody's Watching?: Subtle Cues Affect Generosity in an Anonymous Economic Game," *Evolution and Human Behavior* 26, no. 3 (2005): 245-256 https://doi.org/10.1016/j.evolhumbehav.2005.01.002; and Costas Panagopoulos, "Watchful Eyes: Implicit Observability Cues and Voting," *Evolution and Human Behavior* 35, no. 4 (2014): 279-284.

2 For a thorough treatment of the interplay between intellectual privacy and free speech and how they might be treated in our digital age, see Neil Richards, *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age* (Oxford, UK: Oxford University Press, 2017).

3 Daniel J. Solove, "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy," San Diego Law Review 44 (2007): 745; GWU Law School Public Law Research Paper No. 289. Available at SSRN: https://ssrn.com/abstract=998565.

and its systems and content. Librarians may struggle to balance the potential usefulness of patron data as it relates to student success, library funding, advocacy, and assessment with concerns over patron privacy.[4]

This document aims to identify these potential areas of tension. In addition, it calls for more exploration and rigorous study of ambiguities and emerging trends. Finally, the document makes some tentative suggestions for those who find themselves in the position of wanting to advocate for patron privacy, while balancing the need to collect data for legitimate purposes. Since the authors all work in academic libraries, use of student data for the purposes of learning analytics research is a point of focus.

It is the authors' hope that others who are interested in articulating privacy concerns in the wake of big data collection and learning analytics will add to this document as well as use it to frame research inquiries and conversations. In this time of unprecedented technological development, the professional practices cultivated over time by librarians have the potential to be miscast as a "culture of resistance," when in truth these professional values are rooted in sustaining the personal freedoms of individuals and their agency within open democratic societies. As a profession, we are well suited to use our values and expertise to help shape the conversation surrounding data collection and privacy.

Ethical Frameworks for Data Privacy

Ethical use of online user data is a topic that is important not only to librarians, but also to educators, programmers, database managers, business leaders, and citizens.[5] Like librarians, other internet privacy stakeholders are also articulating principles to guide the ethical use of data. These frameworks and guidelines might be of use when addressing particular needs or circumstances.

eCenter International Data Privacy Principles. eCenter is a European group that advises on e-commerce and internet law. Although these data privacy principles are meant to guide use of personal data in a business setting, this document might help guide a university or library in its data collection policies.

---

4 Scott W. H. Young, Sara Mannheimer, Jason A. Clark, and Lisa Janicke Hinchliffe, *A Roadmap for Achieving Privacy in the Age of Analytics: A White Paper from A National Forum on Web Privacy and Web Analytics* (May 2019) http://dx.doi.org/10.15788/20190416.15445

5 In a 2019 interview with ARL, EDUCAUSE president and CEO John O'Brien tried to identify the educational leaders who have responsibility relative to privacy questions: "librarians, information security officers, privacy officers, HR officers, safety/police officers, compliance officers, registrars, internal auditors, faculty, research administrators, and staff from government relations, records management, risk management, and other areas. I wonder if the list of who probably doesn't have responsibility would be shorter?"

JISC Code of Practice for Learning Analytics. JISC is a British nonprofit that supports universities' digital infrastructure. This document contains eight core principles that make up a set of guidelines for groups working with learning analytics.

National Forum on Education Statistics–The Forum Guide to Data Ethics. These principles come from the Data Ethics Task Force of the National Forum on Education Statistics. They might be particularly relevant when discussing data use in American educational settings.

Setting the Table: Responsible Use of Student Data in Higher Education (*EDUCAUSE Review*). This article culminates with a set of principles for responsible use (shared understanding, transparency, informed improvement, open futures).

ALA Code of Ethics. While our profession's ethical framework encompasses more than user data, it is still largely applicable.

General Library Data Protection

It has become increasingly clear that the security measures of even the largest corporations are inadequate against determined bad actors. Collecting and retaining the least amount of data about our communities is not just a good practice of librarianship, it is a practical measure to protect the library from those who would access the data and use it in a malicious manner.

Libraries can work to address the new risks in several ways.

Inward-facing actions:

- Develop and implement a privacy policy.
- Collect and retain the least amount of data necessary to fulfill the function of the library.
- Articulate privacy as a core value of the library in the strategic plan.

Outward-facing actions:

- Incorporate privacy literacy in all aspects of information literacy instruction.
- Provide consulting services for library patrons who have special risk profiles to help them understand and mitigate their risks.
- Inform patrons about the types and amount of data that each vendor collects about them, and offer alternatives when possible.
- Create an information-seeking space that in all aspects collects and stores as little patron data as possible, and clearly informs the user when and how it does collect such data.

By building these practices and providing these services and instruction, the library can help support a culture of privacy awareness in the community. Moreover, with policies and practices in place, the library is better positioned to respond to requests for data from other constituents.

Library Data and Learning Analytics

Libraries make significant contributions to institutions of higher learning. These contributions must balance with the trust that is expected of librarians who work with students and researchers. The recent IMLS-funded projects LIILA and Data Doubles provide deeper research into the area of learning analytics and student success.

Libraries can engage with learning analytics conversations on campus by:

- being engaged in early analytics conversations
- sharing and centering professional ethics in conversations and learning analytics decision-making processes
- advocating for centering student agency in the learning analytics landscape

When asked for library data to be incorporated into analytics, we recommend asking the following questions:

1. What question are we trying to answer with this data?
2. What confidence do we have that these data are significant in answering that question?
3. What data protections are in place?
4. What agency do constituents have in limiting their engagement with these systems?

The increased focus on learning analytics in K-12 and higher education can present an opportunity for librarians to advocate for privacy-protective practices whenever possible, to center the agency and privacy of the user in community discussions, and to engage with the analytics systems in ways that adhere to professional ethics and values.

Responsible Web Analytics for Library Websites

Privacy-aware implementations of web analytics for library websites involve limiting data collection about user behavior. The guiding rationale is that once created, data about our users' browsing and reading behaviors will exist forever, and can be used, recombined with other data, and mined for insights that are difficult to comprehend or predict.

A National Forum on Web Privacy and Web Analytics: Action Handbook. This document provides guidance and best practices for libraries implementing privacy-focused web analytics. Page 5 of the document summarizes five suggested indicators:

> *Indicator 1:* Collect only the data needed for your use case.
>
> *Indicator 2:* Support analytics tools that allow retention and downloading of your own data in open formats.
>
> *Indicator 3:* Support analytics tools that allow the setting of a data retention strategy and enable the complete removal of data.
>
> *Indicator 4:* Implement analytics tools that allow for deidentification or pseudonymization, or both, and the removal of personally identifiable information (PII).
>
> *Indicator 5:* Implement analytics tools that have support for emerging international privacy standards.

Privacy "Nutrition" Labels

Since privacy policies are notoriously lengthy and opaque, legal scholars have noted that they fall short of normative standards of "morally transformative consent."[6] For this reason, seeking to communicate privacy terms through standardized and legible methods is necessary. Since at least 2009, projects out of Carnegie Mellon, UC Berkeley, Stanford University, and other institutions have explored the prospect of "privacy nutrition labels" and the idea is slowly gaining traction. In 2018, groups within the data industry developed a data transparency label for the purposes of buying and selling data (see: DataLabel.org) but so far, no similar standards have been developed for citizens/consumers. According to its website, IMS Global Learning Consortium[7] is seeking to develop a standard label for educational technologies that identifies the following:

- What information is collected
- How your information is used
- How and with whom your information is shared

As transparency labels and other codified methods develop for communicating data sharing, libraries can be at the forefront of adopting them and integrating them into information literacy education.

---

6 Elizabeth Edenberg and Meg Leta Jones. Jones, "Analyzing the Legal Roots and Moral Core of Digital Consent," *New Media & Society* 21, no. 8 (2019): 1804-1823. https://doi.org/10.1177/1461444819831321.

7 IMS Global Learning Consortium also developed the Learning Tools Interoperability (LTI) standard that governs data flows between learning management systems and third parties. Credo's suite of information literacy modules, "Instruct," is one example of a learning tool that has adopted the LTI standard.

Biometric and Image Technologies

Biometric data collection at library entries/exits or platforms, which includes facial recognition technologies, might be considered for purposes involving safety, community security, and efficiency. The broader implications of identifying patrons at library entries and exits are likely to have chilling effects that undermine the broader purposes of libraries and the professional responsibilities of librarians. The 2019 amendment to the American Library Association's privacy interpretation of the Library Bill of Rights states: "Emerging biometric technologies, such as facial recognition, are inconsistent with the mission of facilitating access to library resources free from any unreasonable intrusion or surveillance."

- Biometric data cannot be changed, unlike passwords. If biometric data is stolen (which it may be, because it has to be stored somewhere in order to function as authentication), it is much more difficult to create new credentials. Stolen biometric data is also much easier to reuse across platforms, given the unique nature of the data.
- As the law stands now, most law enforcement agencies do not need a court order to compel biometric data from a patron. This can disproportionately affect marginalized groups.

Conclusion

The data privacy landscape is a dynamic and evolving space. These resources and practical steps help provide a strong foundation, despite the pace of change. Building shared understanding of these principles and actions across the profession will help inform how libraries evolve with technology, while continuing to hold our professional ethics at the fore. This document represents a starting place for library workers looking for direct and actionable paths to becoming more privacy-aware. While libraries may belong to larger organizations that will require data for myriad purposes, being present at the decision-making table and speaking from an informed and practiced position is a critical function of advocacy.

Privacy Resources and Advocates

- The SPEC Survey on Learning Analytics (ARL, September 2018)
- The Library Freedom Project—"We provide librarians with the skills necessary to turn their ideals into action"
- ALA Privacy Toolkit
- DLF Technologies of Surveillance Working Group: Ethics in Research Use of Library Patron Data: Glossary and Explainer