

Academic Platforms & Your Privacy

Briefing for Library Workers

Invasive tracking that would be unthinkable in a physical library setting now routinely occurs through publisher platforms.^{1,2} As library workers have moved from buying physical materials to licensing platforms, increased harvesting and exploitation of patron data by these platforms risks collapsing the ability of library workers to provide meaningful privacy to faculty, staff, and students. There are a variety of shorter and longer term options for library workers to take action in addressing these risks to privacy. These actions will be essential to maintain library workers' professional commitment to privacy in the future.

Key Privacy Concerns

- The academic platforms libraries subscribe to are collecting much more data about our patrons than we may realize or should be comfortable with.^{2,3,4} This is occurring because vendors are incentivized to monetize the data they can collect, and some have shifted their focus beyond publishing to research analytics products.²
- We could be failing to properly protect the privacy of our patrons (and their families / friends / affiliates) from the potential for harmful actions downstream due to the data collection practices of some library vendors.^{3,4}
- Surveillance has a disparate impact on and imposes increased risks to minoritized communities as they are subjected to greater policing and socio-economical hardship. This can translate to greater reliance on public resources and may lead to increased surveillance exposure due to the lack of economic resources to protect privacy.⁵
- The parent companies of some of our largest vendors are deeply involved in data brokering and surveillance activities that undermine library privacy values.^{1,2,3,4,19} Library workers can be in a position to prevent increased surveillance, as technology allows more intrusive data collection, and send a clear message that this is unacceptable.^{6,7}

What You Can Do

- Library workers are uniquely positioned to be knowledgeable about vendor practices and concerned about patron privacy. We can become experts in this area by educating ourselves and our patrons about:
 - What identifying data may be collected about patrons while they use vendor products. Transparency is key.⁸
 - How patrons may be able to limit this data collection (e.g., by not creating personal accounts or not logging in when not necessary).⁹
- Library workers should consider including data privacy knowledge, skills, and abilities in new hire job descriptions and rewriting current job descriptions to include this language.¹⁰

- Library workers, especially acquisitions experts, can consider negotiating strong privacy requirements in licensing agreements. These protections, such as data processing agreements or addenda, can be used to address and limit what data the vendors we subscribe to can collect about our patrons and how such data can be used.^{3,6,9, 11,12}
- Library acquisitions should require privacy reviews before committing to purchasing a resource:
 - Does the vendor have a privacy policy that provides meaningful protections?
 - Does the resource address minimum technical privacy requirements?^{13,14}
- Library workers, supported by administration, may reconsider purchasing decisions with vendors that do not take sufficient steps to protect user privacy.^{15,16}
 - This could include considering competitor products with superior privacy practices.
 - Depending on local context, some libraries may consider discontinuing contracts if there are sufficient concerns, including doing so as a negotiation strategy to improve privacy terms.^{16,17,18}

References

1. [Physical-equivalent privacy](#) by Dorothea Salo.
2. [Navigating risk in vendor data privacy practices: An analysis of Elsevier's ScienceDirect](#) by Becky Yoose and Nick Shockey.
3. [Addressing the alarming systems of surveillance built by library vendors](#) by SPARC.
4. [Data cartels: The companies that control and monopolize our information](#) by Sarah Lamdan.
5. [Unsettling knowledge inequities podcast with Chris Gilliard](#) by the Knowledge Equity Lab (Season 3, Episode 5).
6. [Intellectual freedom principles for academic libraries](#) by the Association of College & Research Libraries (ACRL) (article 2 on privacy).
7. [Resolution on the misuse of behavioral data surveillance in libraries](#) by the American Library Association (ALA).
8. [Transparency and consent: Student perspectives on educational data analytics scenarios](#) by Kyle M. L. Jones, Abigail Goben, Michael R. Perry, Mariana Regalado, Dorothea Salo, Andrew D. Asher, Maura A. Smale, and Kristin A. Briney.
9. [Managing data for patron privacy: Strategies for libraries](#) by Kristin Briney and Becky Yoose.
10. [Disrupting the digital status quo: Why and how to staff for privacy in academic libraries](#) by Eliza Bettinger, Meryl Bursic, and Adam Chandler.
11. [Privacy field guides – Vendors and privacy](#) by the American Library Association (ALA).
12. [Data processing agreement](#) by University of Washington Privacy Office.
13. [Licensing privacy - Vendor contract and policy rubric](#) by the University of Illinois [Licensing Privacy Project](#).
14. [Library freedom vendor scorecard](#) by the Library Freedom Project.
15. [Negotiation community of practice](#) by SPARC.
16. [Denver Public Library cancels Lynda courses over privacy concerns](#) by John Bear.
17. [Big deal cancellation tracking](#) by SPARC.
18. [Exit Interviews: Leaving Big Deals & Proprietary Products](#) by SPARC.
19. [Data Brokers, Legal Platforms, and ICE: Questions on the Canadian Context](#) by Lisa Levesque

About the Campus Briefings on Privacy & Academic Platforms

- This briefing was authored by the Resource Library Working Group of SPARC's Privacy & Surveillance Community of Practice which seeks to ensure privacy is fundamental to the future of research & education.
- See additional briefings and a glossary of terms at sparcopen.org/our-work/privacy-briefing-documents