Academic Platforms & Your Privacy

Introduction to Campus Briefing Documents

Online platforms are increasingly central to university research and teaching activities. Courses are now frequently taught online and managed using courseware systems. Academic research is primarily accessed online through publisher platforms—not through local, physical copies.

Most of these systems are owned by large commercial vendors which are strongly incentivized to monetize the personal data they can collect. Some are expanding into analytics products that could directly leverage user-collected information, sometimes in ways that could be concerning to the average faculty member or student.

As a result, instructors, students, and all college and university community members who must use these digital systems can face significant privacy risks.

This series of briefing documents seeks to better educate members of the campus community about these risks and actions that can be taken to mitigate them.

Key Privacy Concerns

When patrons use academic platforms owned by third parties, libraries and institutions have less control over whether and what use is tracked, who is allowed to collect that information, and how that information may be later used.[1] In some cases, data collected in an academic context may be combined with external data sources (e.g. from data brokers) to create a more comprehensive profile of a user.

This is a major challenge for academic librarians as these vendor data practices can directly conflict with a core value of librarianship to protect patron privacy as outlined in privacy standards and guidelines including the American Library Association (ALA) Code of Ethics,[2] the Library Bill of Rights,[3] and the International Federation of Library Associations and Institutions (IFLA) Statement on Privacy in the Library Environment.[4]

Data brokers aggregate and resell data about individuals gathered from credit bureaus, social media platforms, web trackers, marketers, public information sources, government service providers, and other sources.[5, 6, 7, 12] The relationship between some publishers and third-party partners and data brokers raises questions about the possibility of academically-derived data ending up in this broader data brokering ecosystem.[8] This raises ethical concerns. For instance:

- The parent companies of two leading academic vendors have contracted with the US Department of Homeland Security (DHS) and Immigrations and Customs Enforcement (ICE) during a period with frequent reports of human rights violations [9, 10, 11]
- These companies can extract a concerning amount of data from the academic publishing process, which could then influence research communication toward commercial interests.[13]

- Surveillance via user tracking conducted by library content and service providers may create a chilling effect that constrains the scope of inquiry, research, and writing that scholars and students are willing to explore.[14, 15, 16, 17]

What You Can Do

Libraries are in a strong position to evaluate and address potential privacy risks; nevertheless, protecting privacy requires campus community support and resources. These briefing documents for faculty, administrators, students, and other campus groups seek to better educate key groups on campus about the potential impact of these privacy risks and how we can take action.

References

1. Physical-Equivalent Privacy by Dorothea Salo.
2. Professional Ethics by the American Library Association (ALA).
3. Library Bill of Rights by the American Library Association (ALA).
4. Statement on Privacy in the Library Environment by the International Federation of Library Associations and Institutions.
5. *Data Cartels*: The companies that control and monopolize our information by Sarah Lamdan.
6. Corporate Surveillance in Everyday Life by Wolfie Christl.
7. Tracking the Surveillance and Information Practices of Data Brokers: A Report by Centre for Access to Information and Justice, Rahul Kanwal, and Kevin Walby.
8. Navigating Risk in Vendor Data Privacy Practices: An Analysis of Elsevier's ScienceDirect by Becky Yoose and Nick Shockey.
9. The Legal Tech Giants Powering ICE, Part 1 — How Thomson Reuters and LexisNexis Helped Support America's Immigration Surveillance Machine by Bob Ambrogi.
10. LexisNexis to Provide Giant Database of Personal Information to ICE by Sam Biddle.
11. She Raised Concerns About Her Company's Contracts With ICE. Then She Lost Her Job by Jude Joffe-Block.
12. Profits Over Privacy: Investigating the Under-Regulated Business Practices of the Global Data Brokerage Industry in Canada by Mackenzie Porter.
13. The Scholarly Fingerprinting Industry by Jefferson Pooley.
14. Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor by Pen America.
15. Fear, Risk and the First Amendment: Unraveling the Chilling Effect by Frederick Schauer.
16. Privacy: An Interpretation of the Library Bill of Rights by the American Library Association (ALA).
17. Data tracking in research: aggregation and use or sale of usage data by academic publishers by Deutsche Forschungsgemeinschaft (DFG, German Research Foundation).

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