

Academic Platforms & Your Privacy

Briefing for Administrators

Many academic publishers and educational technology vendors are increasingly focused on personal data collection and data analytics.¹ While universities and colleges are already sensitive to the issue of protecting Personally Identifiable Information (PII) in student records, legal compliance often does not go far enough in ensuring that these academic platforms sufficiently protect student and researcher privacy.^{2,3} This protection is particularly important in the case of academic platforms owned by corporations that are also data brokers, which may sell access to personal data and/or analytics products to insurance companies, employers, and law enforcement.^{1,4} When working with these kinds of third parties, administrators will be well-served by considering the privacy risks and liabilities they may present, now and in the future.^{5,6}

Key Privacy Concerns

- The increased collection and use of institutional and patron data may endanger academic and research freedoms, or could shift knowledge production away from public interest and toward privatization.^{7,8} For instance, faculty data collected by these platforms may be used to guide the decisions around what research is funded^{1,7} and who gets published.^{1,7,9}
- Institutions can have little control over student and research data once it is collected or aggregated by platforms, which may lead to increased risks for data misuse and breaches.^{10,11} If a vendor or platform's system is breached and sensitive student or research data is exposed, for example, the institution can face possible reputational harm and legal liability.^{12,13}
- Institutional practices and limited privacy laws can cause harm to student privacy (through data surveillance) and ultimately to institutional reputations.^{3,14,15}

What You Can Do

- Support campus units to negotiate contracts that better protect privacy.^{16,17,18,19,20,21,22}
- Evaluate new technologies against privacy risks and liability they may create.²³
- Avoid over-reliance on proprietary metrics and analytics products to track student success or faculty productivity. Engage with proprietary data carefully and critically.²⁴
- Support institutional data governance stakeholders, such as the library, campus IT, and offices of teaching and learning, in tightening up data collection and retention policies.^{5,25,26,27}
- Collaborate with the library and draw on their expertise in patron privacy and vendor practices.
- Encourage a culture on campus of educating students, faculty, and staff to be their own privacy advocates.²⁸
- Include data privacy knowledge, skills, and abilities in new hire job descriptions and rewrite current job descriptions to include this language.

References

1. [Data cartels: The companies that control and monopolize our information](#) by Sarah Lamdan.
2. [Student privacy principles for the age of big data: Moving beyond FERPA and FIPPS](#) by Elana Zeide.
3. [He wanted privacy. His college gave him none](#) by Tara García Mathewson.
4. [Data is a toxic asset](#) by Bruce Schneier.
5. [US library survey 2022: Navigating the new normal](#) by Ioana G. Hulbert.
6. [Open data, grey data, and stewardship: Universities at the privacy frontier](#) by Christine L. Borgman.
7. [Elsevier's acquisition of Interfolio: Risks and responses](#) by SPARC.
8. [RE: Advanced notice of proposed rulemaking: Commercial surveillance and data security](#) by SPARC.
9. [The perils of artificial intelligence in academic publishing](#) by Yves Gendron, Jane Andrew, and Christine Cooper.
10. [Data breaches in higher education institutions](#) by Samantha Mello.
11. [US schools leaked 37.6 million records in 3,713 data breaches](#) by Sam Cook.
12. [AG Nessel Re-Issues Data Breach Alert Following University of Michigan Network Infiltration](#) by Michigan Department of Attorney General.
13. [Predominantly Black college to shut down after Covid-19 and cyberattack burdens](#) by Omar Jimenez and Sean Lyngaas.
14. [The absurd proposal to put bodycams on teachers is ... feasible?](#) by Sidney Fussell.
15. [The failure of FERPA](#) by Sarah Hartman-Caverly.
16. [Library privacy guidelines for vendors](#) by the American Library Association (ALA).
17. [Licensing privacy: Views from library leadership](#) by Danielle Cooper.
18. [Navigating risk in vendor data privacy practices: An analysis of Elsevier's ScienceDirect](#) by Becky Yoose and Nick Shockey.
19. [Intellectual freedom principles for academic libraries: An interpretation of the Library Bill of Rights](#) by the Association of College and Research Libraries (ACRL).
20. [Privacy field guides for libraries: Vendors and privacy](#) by the American Library Association (ALA).
21. [Privacy](#) by the University of Washington Privacy Office.
22. [Managing data for patron privacy: Comprehensive strategies for libraries](#) by Kristin Briney and Becky Yoose.
23. [On the necessity \(or lack thereof\) of digital proctoring: Drawbacks, perceptions, and alternatives](#) by Alex Duncan and David Joyner.
24. [Barcelona Declaration on Open Research Information](#)
25. [Measuring library vendor cyber security: Seven easy questions every librarian can ask](#) by Alex Caro and Chris Markman.
26. [Setting the table: Responsible use of student data in higher education](#) by Martin Kurzweil and Mitchell Stevens.
27. [Customer data: Designing for transparency and trust](#) by Timothy Morey, Theodore Forbath, and Allison Schoop.
28. [Data defense: Privacy protection actions](#) by Melissa Ezarik.

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