

Academic Platforms & Your Privacy

Briefing for Faculty

Online tools have become central to conducting research and building an academic career. As many parts of the research process have shifted online, serious questions related to privacy and control of data have followed. Leading academic publishers have evolved into data analytics businesses that own widely adopted products across the research lifecycle—including the tools faculty use to search across library resources, disseminate research, and for promotion and tenure evaluation. These companies are incentivized to monetize personal information, including in ways that may make faculty uncomfortable. As a leading research foundation has noted, these platforms and the tracking they enable can contradict academic freedom.¹ There are a variety of actions that faculty can take to mitigate these risks, for themselves and their students.

Key Privacy Concerns

- Academic platforms, such as faculty information systems, can collect extensive personal data about individual faculty, including demographic information, evaluations, external reviews, and other career history data (including publications and research funding).^{2,3} This data can be combined with data from additional vendor platforms, allowing companies to create detailed faculty member profiles and to potentially develop new metrics for productivity.^{1,2,3,4,5}
- Educational technology platforms, such as learning management and homework systems, can collect personally identifying information from both students and faculty that could be sold or shared with third parties, including data brokers.⁶ Existing federal laws like the U.S. *Family Educational Rights and Privacy Act* (FERPA) and the Canadian *Personal Information Protection and Electronic Documents Act* (PIPEDA) do not fully protect student data.^{7,8,21} This can create risks for both students and faculty.
- Some publishers are building platforms that span the entire research process from application, hiring, discovery, collecting and analyzing data, publishing, evaluation, and academic career management. This has the potential to create platform lock-in and commercially influence what research is valued and supported.^{1,9}
- Many academic platforms are also incorporating Artificial Intelligence (AI), often without transparency or clear external review. This may create or reinforce biases in the academic publication process.¹⁰

What You Can Do

- Faculty can consider what tools they use and pedagogical choices that may put their or students' privacy at risk, choose privacy-respecting alternatives, and educate colleagues on these risks.^{11,12}
- Faculty can consider privacy practices and risks when selecting journals and publishing venues.
- Faculty can look for opportunities to educate students regarding data privacy and surveillance issues (e.g., library instruction session or materials chosen to embed into the course).^{13,14,15}

- Faculty can pass resolutions within academic senates, such as these examples from Portland State University,¹⁶ City University of New York,¹⁷ University of Colorado Boulder,¹⁸ and University of Washington.¹⁹
- Faculty can request or support representation on campus data governance and IT committees.
- Faculty can contact their professional associations, ask about their data practices, and where needed, encourage the adoption of stronger data protections internally and by vendors the association engages with (e.g. publishers of association-owned journals).
- Faculty can support the library in negotiating for contract terms that limit invasive data collection practices that could harm faculty and students. Vendors know libraries focus on supporting faculty needs, so faculty advocacy for stronger privacy protections may increase the likelihood of reaching favorable terms.^{9,16,20}

References

1. [Data tracking in research: aggregation and use or sale of usage data by academic publishers](#) by Deutsche Forschungsgemeinschaft (DFG, German Research Foundation).
2. [Elsevier's acquisition of Interfolio: Risks and responses](#) by SPARC.
3. [Welcome to Hotel Elsevier: you can check-out any time you like ... not](#) by E. Fried.
4. [Data Cartels: The companies that control and monopolize our information](#) by Sarah Lamdan.
5. [The Scholarly Fingerprinting Industry](#) by Jefferson Pooley.
6. [Paying Twice to Learn: How Higher Education Students May be Forced to Sacrifice Privacy for Digital Learning Tools](#) by Ariel Fox Johnson.
7. [Beyond compliance: Students and FERPA in the age of big data](#) by Cecelia Parks.
8. [The Application of PIPEDA to Municipalities, Universities, Schools, and Hospitals](#) by the Office of the Privacy Commissioner of Canada.
9. [Navigating Risk in Vendor Data Privacy Practices: An Analysis of Elsevier's ScienceDirect](#) by Becky Yoose and Nick Shockey.
10. [The perils of artificial intelligence in academic publishing](#) by Y. Gendron, J. Andrew and C. Cooper.
11. [The ethics of student privacy: Building trust for ed tech](#) by Jules Polonetsky and Omer Tene.
12. [Transparency and consent: Student perspectives on educational data analytics scenarios](#) by Kyle M. L. Jones, A. Goben, M. R. Perry, M. Regalado, D. Salo, A. D. Asher, M. A. Smale, and K. A. Briney.
13. [Why students should be involved in data privacy conversations](#) by Pegah Parsi.
14. [Data privacy in higher education: Yes, students care](#) by Jasmine Park and Amelia Vance.
15. [Data defense: Privacy protection actions](#) by Melissa Ezarik.
16. [Library faculty position statement on vendor surveillance](#) by Jill Emery and Portland State University.
17. [Resolution affirming the privacy of learning data and principles for working with third-party vendors](#) by the University Faculty Senate of The City University of New York.
18. [Resolution in Support of Libraries Licensing Priorities](#) by the Boulder Faculty Assembly of the University of Colorado Boulder.
19. [Resolution regarding support for the UW Libraries' principles in licensing scholarly resources](#) by University Libraries, University of Washington.
20. [Negotiating with scholarly journal publishers](#) a toolkit by the University of California
21. [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