

Academic Platforms & Your Privacy

Briefing for Unions

Privacy protection for campus employees is a union concern. Employees may face surveillance by third-party vendors, and data uses by their institutions that may raise concerns, including around union activities. Federal and state law and campus policy frequently provide insufficient protection. Addressing surveillance is an investment in the membership's rights, including intellectual property rights, freedom of expression, and academic freedom.

Key Privacy Concerns

- Academic platforms, from those of academic publishers^{17,18} to faculty information systems used in evaluation processes,¹⁹ collect detailed user data that could pose risks to researchers. They can provide data insights on readers and researchers that could be uncritically used in ways that cause potential harm.^{1,2}
- Institutionally provided software has the potential to collect or share individuals' private data in damaging ways. Data can be quite granular, including such data points as screen time, application usage, website visits, email communications, and document access.³
- Data which might seem insignificant, such as the times a document was viewed, can be used to infer traits about an individual. Data brokers can sell this data as comprehensive dossiers of individuals.^{4,22} This is why *all* data collection and its use by institutional parties or sale to third parties should be carefully considered.
- In public academic institutions, work devices and communication tools may be subject to public records requests, including informal tools like Slack.^{5,6} *Freedom of Information Act* (FOIA) requests overall have been on the rise, requesting information like course materials and faculty syllabi.⁷

What You Can Do

- Create and publish union statements on member privacy rights in the workplace. The Canadian Association of University Teachers statement can serve as a template.⁸
- Include privacy protections in collective agreements, empowering librarians, IT purchasers, and procurement professionals to negotiate for privacy-respecting contracts with data vendors. Empower union members to uphold and enforce the provisions in the collective agreement.^{9,10}
- Share information within the union. Members from different departments may have information on institutional privacy risks and risks posed by third-party vendors. Specifically, librarians have expertise on patron privacy and library resources, including vendor practices.
- Find out whether your pension fund invests in data broker firms like RELX or Thomson Reuters, whose contracts with US Immigration and Customs Enforcement (ICE) have been widely reported.^{4,11,12,13} Pension funds may wish to assess the alignment between any such investments and their members' values. Leveraging its pension fund, the British Columbia General Employees'

Union (BCGEU) has been at the forefront of raising scrutiny around these issues and pressuring these companies around what it describes as the human rights risk posed by their products.²¹

- Advocate for implementing more equitable assessment practices to be used on your campus, moving away from proprietary metrics. Examples include the Leiden Manifesto,¹⁴ the San Francisco Declaration on Research Assessment (SF DORA),¹⁵ the Coalition for Advancing Research Assessment (CoARA),¹⁶ and HELIOS Open.²⁰
- Support contract amendments that guarantee privacy for all workers, including the privacy of researchers, instructors, and student workers.

References

1. [Surveillance and digital control at work](#) by Wolfie Christl.
2. [Proposal to install spyware in university libraries to protect copyrights shocks academics](#) by Gautama Mehta.
3. [Inside the invasive, secretive "bossware" tracking workers](#) by Bennett Cyphers and Karen Gullo.
4. [Data cartels: The companies that control and monopolize our information](#) by Sarah Lamdan.
5. [SACUA talks Slack usage among students, faculty](#) by Samantha Rich.
6. [Information disclosure requirements and issues for universities in the United States: Letting sunshine into the ivory tower](#) by Jamie P. Horsley and Can Sun.
7. [UNC Campuses Split on Whether Syllabi Are Public Documents](#) by Emma Whitford.
8. [Confidentiality of personal information](#) by the Canadian Association of University Teachers.
9. [Privacy in the workplace: Are collective bargaining agreements a place to start formulating more uniform standards?](#) By Karen Mika.
10. [Carpe diem: Privacy protection in employment act](#) by Ariana Levinson.
11. [Union investor successfully pushes Toronto's Thomson Reuters to prioritize human rights and re-evaluate ICE contracts](#) by BC General Employees' Union (BCGEU).
12. [Thomson Reuters commits to human rights assessment of ICE contracts after union investor push](#) by Corin Faife.
13. [CAUT panel discussion: academic publishing, data surveillance and human rights - May 17, 2022](#) by Sarah Lamdan, Emma Pullman, and Cinthya Rodriguez.
14. [Bibliometrics: The Leiden Manifesto for Research Metrics](#) by Diana Hicks, Paul Wouters, Ludo Waltman, Sarah de Rijcke, and Ismael Rafols.
15. [San Francisco Declaration on Research Assessment \(SFDORA\)](#).
16. [Coalition for Advancing Research Assessment \(CoARA\)](#).
17. [Navigating Risk in Vendor Data Privacy Practices: An Analysis of Elsevier's ScienceDirect](#) by Becky Yoose and Nick Shockey.
18. [Navigating Risk in Vendor Data Privacy Practices: An Analysis of Springer Nature's SpringerLink](#) by Becky Yoose and Nick Shockey.
19. [Elsevier's acquisition of Interfolio: Risks and responses](#) by SPARC.
20. [HELIOS Open](#).
21. [Thomson Reuters Is Profiting Off of ICE'S Reign of Terror](#) by Carl Ginsburg.
22. [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