

Academic Platforms & Your Privacy

Briefing for Students

Although laws like FERPA protect core academic records, they often fail to cover the vast personal data harvested by modern educational technology (e.g. platforms that provide courseware and access to academic publications). Many vendors now operate like big tech firms, collecting and sharing student data—often feeding it into data brokerage ecosystems. For example, student data could be used to assess job candidates for employment or evaluate future creditworthiness.² Students have the power to demand transparency and drive institutional change; by understanding how their data is collected and used, they can lead initiatives to secure better privacy protections across campus.

Key Privacy Concerns

- Third-party technology companies can collect a significant amount of student data.^{3,4} In class and beyond, students deserve to be assessed on their academic achievements, not vendor-collected behavioral data.
- Student data is not guaranteed to be vetted, error free, or free of bias.⁵
- Third-party vendors may be amassing even more student data. This can add to concerns of this data ending up in unanticipated places such as with employers, immigration agencies, and law enforcement.^{2,6,7} In many instances, for-profit data companies lack meaningful regulation that fully protects students in this context.
- Without intentional safeguards, university-licensed systems can collect and use data in ways that could negatively impact students. This can include surveillance systems that allow for the monitoring of individuals^{4,5} and student protests.⁸ Surveillance systems that are not transparent and do not obtain student consent can diminish student trust in higher education institutions.⁹

What You Can Do

- Student awareness and activism can motivate change—it already has.^{10,11,12}
- Students can demand transparency by pushing to understand what personal data is collected, shared, and used by the university and vendors.
- Students can request representation on campus committees related to student data and data governance.
- Student groups can create complementary resources for this document based on the specifics of their campus environment. This could include localized lists covering opportunities for students to engage with relevant stakeholders.
- Student governments can pass resolutions in favor of privacy.^{13, 14,15,16}
- Students can consult library workers to understand their personal privacy risks, mitigation strategies, and the vendor landscape. Librarians can also be important allies in strengthening privacy protections, particularly in collaboration with the broader campus community.

- Students can limit data collection by actively managing privacy settings and opting out of personal accounts when possible.¹⁷

References

1. In the USA student data is protected at the federal level by the [Family Educational Rights and Privacy Act](#) (FERPA); in Canada provincial legislation is relevant for student privacy concerns and protection varies widely between provinces and territories. See the [Provincial and Territorial Privacy Laws and Oversight](#) by the Office of the Privacy Commissioner of Canada.
2. [Ethical Issues Regarding the Use of AI Profiling Services for Recruiting: The Japanese Rikunabi Data Scandal](#) by Fumiko Kudo, Hiromi Arai, and Arisa Ema.
3. [Meet the software company tracking college students' behavior](#) by Margaret Peppiatt.
4. [Understanding student monitoring](#) by Future of Privacy Forum.
5. [A data collection effort at GW leads to privacy questions](#) by Suzanne Smalley.
6. [Law students protest research database contracts with ICE](#) by Josh Moody.
7. [Law students demand Seattle University cut ties with data companies working with ICE](#) by Bunthay Cheam.
8. [Tracked: How colleges use AI to monitor student protests](#) by Arijit Douglas Sen and Derêka Bennett; an update is provided in [Universities and students investigate use of AI surveillance tool in response to grantee's reporting](#) by Sarah Swan, Arijit Douglas Sen, and Derêka Bennett.
9. [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.
10. [How a facial recognition error on a Waterloo vending machine led to an international debate on privacy](#) by Robert Williams; [Meet the students who broke the vending machine story](#) by Regina Ashna Singh.
11. [Education officials urged to curb student snoopware](#) by Thomas Claburn.
12. [Piazza makes three significant changes to deal with privacy issues](#) by Phil Hill.
13. [S.A. Resolution underscores privacy concerns over Cornell's use of Zoom](#) by Sean O'Connell.
14. [Resolution 16: GPSA R16: Demanding Cornell fight for fair terms for the remote services its community is required to use](#) by Cornell Graduate and Professional Student Assembly.
15. [BOD 2022-23 – 1R Resolution in support of the removal of webcam proctoring](#) by Cal State East Bay Associated Students Inc.
16. [S.R. 59.2-8, Resolution to discourage the use of Respondus Lockdown Browser and other proctoring programs requiring the use of audio/visual recording](#) by University of North Carolina at Charlotte Student Senate.
17. [Your Data Isn't a Tuition Fee. Protect Your Intellectual Freedom](#) by Library Freedom Project.

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