

Academic Platforms & Your Privacy

Briefing for IT

For IT experts, security vulnerabilities are top of mind—but privacy vulnerabilities should be an equal concern. IT manages systems, from research data management tools to research portals, that contain sensitive data. There have been incidents of academic privacy breaches related to campus IT-managed platforms. To avoid this situation, libraries can be a helpful collaborator with campus IT offices, based on their expertise in privacy, patron data, and university research needs.

Key Privacy Concerns

- Several prominent academic institutions have faced scrutiny and backlash related to student monitoring and surveillance. In particular, institutions have faced scrutiny for facial recognition software,¹ tracking students and faculty,^{2,3} and proctoring software such as ProctorU and Proctorio.^{4,5}
- Students are concerned about requirements to share their sensitive health information and biometric information⁶ with school courseware, a trend exacerbated by pandemic remote learning and increasingly common throughout their academic lives.⁷ Students have objected and even filed a lawsuit in response,^{8,9} with one student summarizing the outrage: “You’re paying so much to be at school and to be protected, and you’re forced to use a program that you don’t even feel safe with.”¹⁰
- Faculty are concerned about privacy for themselves, their disciplines, and their students,¹¹ and an education technology expert faced legal ramifications after speaking out.¹²

What You Can Do

- IT organizations should work together with campus librarians to make informed decisions when purchasing library technology. Together, we can build stronger protections for patron data and ensure that external vendors comply with rigorous privacy standards and data collection and use limits.
- IT organizations should share information with library colleagues concerning contract language. Specifically, vendor contracts should explicitly state data collection, use, and retention limitations, refer to relevant statutory requirements, and include language addressing risky vendor data practices.
- IT organizations that regularly attend privacy courses can actively respond to risk and build trust on campus by sharing their expertise and collaborating to define best practices. Resources are available on retaining student trust.¹³
- Guidance and advice on data processing and privacy practices are available from leading universities including the University of Washington¹⁴ and UC Berkeley.¹⁵
- Privacy is a complex topic. Technology companies use increasingly sophisticated data collection practices, and the legal landscape is evolving and unsettled.¹⁶ Privacy issues require continual improvement and proactive, rather than reactive, actions.

References

1. [UCLA cancels on campus facial recognition program after backlash](#) by Laura Hautala.
2. [George Washington University apologizes for tracking locations of students, faculty](#) by Monique Beals.
3. [Glasgow University staff apologise after 'tracking students'](#) by Catriona Stewart.
4. [How it feels when software watches you take tests](#) by Anushka Patil and Jonah Engel Bromwich.
5. [Cheating-detection companies made millions during the pandemic. Now students are fighting back](#) by Drew Harwell.
6. [Invasive remote learning tech scans my retina, records voiceprints and gobbles up my data](#) by Anjali Chakradhar.
7. [Cradle-to-grave surveillance of our children now begins in school](#) by Massachusetts ACLU.
8. [Tech companies promised schools an easy way to detect cheaters during the pandemic](#) by Tyler Sonnemaker.
9. [Federal court deems university's use of room scans within the home unconstitutional](#) by Lauren Merk.
10. [Poor security at online proctoring company may have put student data at risk](#) by Thomas Germain.
11. [When your journal reads you](#) by Renke Siems.
12. [An ed-tech specialist spoke out about remote testing software — and now he's being sued](#) by Monica Chin.
13. [Keeping student trust](#) by Jill Dunlap, Iris Palmer, and Alexa Wesley.
14. [Data processing agreement](#) by University of Washington Privacy Office.
15. [Privacy at UC Berkeley](#) by UC Berkeley Office of Ethics, Risk and Compliance Services.
16. [Industry unbound](#) by Ari Ezra Waldman.

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