

Academic Platforms & Your Privacy

Briefing for Collective Governance Bodies

Data analytics can be used to monitor students^{1,2} and employees,³ can impact research directions,¹ and can have a chilling effect on academic freedom and freedom of inquiry.⁴ Moreover, surveillance through data collection can affect tenure and promotion opportunities,⁵ student success,⁶ or in some cases may risk disclosure to law enforcement agencies.⁷

Collective governance structures, including faculty councils, librarian councils, boards, senates, and committees, shape institutional policies with the best interests of the community at heart. However, the rise of institutional data surveillance has introduced a concerning power imbalance where data analytics, and those that manage them, may influence or undermine traditional forms of governance.⁸ Collective governance bodies can take action to safeguard the individuals they represent. Investing in campus privacy is a critical investment in the fundamental rights of the campus community.

Key Privacy Concerns

- Digital monitoring and surveillance by vendors, and possibly governments, is increasingly a risk within many university processes, including those that are traditionally expected to be private, such as accessing library resources and in faculty information systems. This growing intrusion raises concerns for faculty governance bodies as it impacts the privacy and autonomy of faculty and students, and has the potential to compromise academic freedom and the free exchange of ideas within the university community.^{9,10}
- Institutional data surveillance is frequently imperceptible by its targets. For example, surveillance through vending machines at one institution was only noticed due to an error message.¹¹
- Standard licensing and procurement processes do not fully prevent surveillance.¹²
- Governance bodies have been effective in drawing attention to data collection and expressing commitments to protect against surveillance, for example through senate resolutions.¹³
- Without opposition, data collection risks concentrating more power under the control of private companies that operate outside the supervision of institutional oversight. In the broader societal context, a rise of corporate power that may operate outside the bounds of state rules has been termed a system of "surveillance capitalism".¹⁴

What You Can Do

- Introduce and advocate for resolutions to block indiscriminate campus video surveillance, unnecessary remote proctoring, and privacy-violating contracts if you are a member of a collective governance body.
- Partner with unions, boards of trustees, and other stakeholders in advocating for institutional policies that limit data collection and surveillance practices.

- Bring any potentially harmful campus surveillance practices to the attention of your local collective governance body. Learn more about the scope and agency of these bodies.¹⁵
- Review governance resolutions from peer institutions and adapt them to address specific concerns at your local institution.¹³
- Reach out to members of the campus community who are knowledgeable about harmful surveillance practices and ways to mitigate harms. This includes librarians with expertise in patron privacy and information resources.

References

1. [Understanding student monitoring](#) by Future of Privacy Forum.
2. [Cheating-detection companies made millions during the pandemic. Now students are fighting back](#) by Drew Harwell.
3. [‘Bossware is coming for almost every worker’: the software you might not realize is watching you](#) by Zoë Corbyn.
4. [Not-so-SMART: Why new platform and surveillance technologies are bad news for science and understanding](#) by Bram Büscher.
5. [Academic analytics, Big data, and the tenure track](#) by Mike Nietzel; [University of Missouri faculty members upset about use of data in promotion and tenure](#) by Roger McKinney.
6. [A comprehensive primer to library learning analytics practices, Initiatives, and privacy Issues](#) by Kyle M.L. Jones, Kristin A. Briney, Abigail Goben, Dorothea Salo, Andrew Asher, Michael R. Perry.
7. [Librarianship at the crossroads of ICE surveillance](#) by Sarah Lamdan; [LexisNexis to Provide Giant Database of Personal Information to ICE](#) by Sam Biddle.
8. [Digital education governance: data visualization, predictive analytics, and ‘real-time’ policy instruments](#) by Ben Williamson.
9. [The “Academicon”: AI and surveillance in higher education](#) by Mark Swartz and Kelly McElroy.
10. [What the vendor saw: Digital surveillance in libraries](#) by Emily Cukier.
11. [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
12. [Navigating Risk in Vendor Data Privacy Practices: An Analysis of Elsevier's ScienceDirect](#) by Becky Yoose and Nick Shockey.
13. Senate resolutions include: [Faculty Senate debates expansion of video surveillance](#) by Cassidy Dalva; [Resolution supporting learning data privacy principles and practices](#), University of Hawai‘i Manoa Faculty Senate; [Revision of AP 6520 – security of district property](#) [about video surveillance on campus], College of Marin Academic Senate; [On the use of remote proctoring software for assessment](#), California State University Academic Senate; [Resolution affirming the privacy of learning data and principles for working with third-party vendors](#), City University of New York University Faculty Senate.
14. [The age of surveillance capitalism : The fight for a human future at the new frontier of power](#) by Shoshana Zuboff.
15. Canadian primers include: [University governance in Canada : Navigating complexity](#) by Julie Eastman, Glen A. Jones, Claude R. Trottier, Olivier Bégin-Caouette; [An introduction to university governance](#) by Cheryl Foy; The American Association of University Professors provides numerous [Resources on Shared Governance](#).

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