

Academic Platforms & Your Privacy

Briefing for the Office of Research

As the Office of Research is well aware, attention to data privacy and confidentiality in Institutional Review Boards and Research Ethics Boards (IRB and REB) and grant applications is vitally important. Similarly, ensuring data privacy throughout campus requires ethical and legal frameworks that balance the interests and rights of all parties involved. Campus affiliates' data privacy is an important consideration when procuring research analytics tools. In an environment where research-tracking systems and their vendors routinely require or ask users to sign away data privacy rights, the Office of Research may want to consider how vendors access, use, share, and sell information from or about faculty, staff, and students. The risk of privacy violations has increased as vendors have reimagined themselves as data analytics businesses and are increasingly engaged in data brokering.^{1, 2, 3, 19} Risks of data collection and surveillance on campus include: loss of privacy in research and scholarship and sharing of sensitive information⁵ and undermining free speech and academic freedom.^{6, 7, 8}

Key Privacy Concerns

- Research data integrity and confidentiality can be threatened by software and service vendors. Specifically, vendors and additional third parties may be able to reidentify data which had been deidentified by researchers, exposing researchers and participants. Responsible and ethical data management methods can mitigate these risks.^{11, 12, 13, 14}
- Proper support for campus activities should include policies and procedures for ensuring data privacy for institutional data, including assessment data.
- For research data, research data management plans should be developed and used for data collection, documentation, storage, preservation, sharing, and compliance.¹⁵
- The increasing use of AI by research infrastructure providers (e.g. through faculty information systems) could enable vendors to extract and monetize institutional data (such as faculty activity statements) in ways that have not previously been feasible.

What You Can Do

- The Office of Research's functionality within a university already includes internal research security expertise focused on campus data-governance and privacy efforts, including both research data security and research security and integrity,^{9, 10} that can be helpful in addressing privacy risks.
- The Office of Research can consider including contractual privacy terms in contracts for vendor products such as IRB/REB and grant application software, research information systems, and faculty information systems.³
- Focus on privacy. Documentation coming out of federal agencies encourages the Office of Research to strengthen support for faculty compliance with privacy and security measures.¹⁶ The Office of Research could also consider incorporating privacy as a focus in job descriptions for both current and prospective employees.¹⁷

- IRB/REB processes for confidentiality, security, and ethical data practices are rigorous; these same rigorous standards can be applied to institutional practices that protect faculty, student, and staff privacy. Some IRB or REB-reviewed terms may warrant additional reviews of privacy protocols.¹⁸
- Partner with the library or allies in data governance and privacy, both inside and outside research contexts.
- The Office of Research can leverage its expertise to shape campus data governance and privacy policies, ensuring robust protection of both research and personal data. This includes implementing responsible data management practices, assessing vendor risks, and addressing emerging threats from AI and other technologies to safeguard institutional data.

References

1. [Data cartels](#) by Sarah Lamdan.
2. [Surveillance publishing](#) by Jefferson Pooley.
3. [Elsevier's acquisition of Interfolio: Risks and responses](#) by SPARC.
4. [Library patron privacy in jeopardy: An analysis of the privacy policies of digital content vendors](#) by A. D. Lambert, M. Parker, and M. Bashir.
5. [Navigating risk in vendor data privacy practices: An analysis of Elsevier's ScienceDirect](#) by Becky Yoose and Nick Shockey.
6. [Academic Freedom and Electronic Communications](#) by the American Association of University Professors (AAUP).
7. [Data tracking in research: Aggregation and use or sale of usage data by academic publishers](#) by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation).
8. [PI's submission to the UN Special Rapporteur on the right to education's report on academic freedom](#) by Privacy International.
9. [Research misconduct and its federal regulation: The origin and history of the Office of Research Integrity—with personal views by ORI's former associate director for investigative oversight](#) by Alan R. Price.
10. [Establishing and maintaining research integrity at academic institutions: Challenges and opportunities](#) by Janet D. Robishaw, David L. DeMets, Sarah K. Wood, Phillip M. Boiselle, and Charles H. Hennekens.
11. [The Office of Research Integrity](#) by the U.S. Department of Health and Human Services.
12. [Ensuring research integrity: The role of data management in current crises](#) by Heather Coates.
13. [Ensuring the integrity, accessibility, and stewardship of research data in the digital age](#) by the National Academy of Sciences (US), National Academy of Engineering (US) and Institute of Medicine (US) Committee on Ensuring the Utility and Integrity of Research Data in a Digital Age.
14. [Strengthening research integrity: Which topic areas should organisations focus on?](#) by Mads P. Sørensen, Tine Ravn, Ana Marušić, Andrea Reyes Elizondo, Panagiotis Kavouras, Joeri K. Tjeldink, and Anna-Kathrine Bendtsen.
15. [Guide to preparing a data management plan](#) by Social Sciences and Humanities Research Council
16. For examples, see the [Tri-agency guidance on research security](#) and their resource portal or the [NIH principles and best practices for protecting participant privacy](#).
17. [Disrupting the digital status quo: Why and how to staff for privacy in academic libraries](#) by Eliza Bettinger, Adam Chandler, and Meryl Bursic.
18. [Research privacy: Why IRB reviews aren't always sufficient](#) by Pegah Parsi and Isaac Straley.
19. [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