2021 EDUCAUSE Horizon Action Plan: Privacy

EDUCAUSE

2021 EDUCAUSE Horizon Action Plan: Privacy

Mark McCormack, D. Christopher Brooks, and Jamie Reeves, *2021 EDUCAUSE Horizon Action Plan: Privacy* (Boulder, CO: EDUCAUSE, 2021).

© 2021 EDUCAUSE

This report is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.

Learn More

Read additional materials on the 2021 Horizon Report research hub, https://www.educause.edu/horizon-report-infosec-2021.

EDUCAUSE

EDUCAUSE is a higher education technology association and the largest community of IT leaders and professionals committed to advancing higher education. Technology, IT roles and responsibilities, and higher education are dynamically changing. Formed in 1998, EDUCAUSE supports those who lead, manage, and use information technology to anticipate and adapt to these changes, advancing strategic IT decision-making at every level within higher education. EDUCAUSE is a global nonprofit organization whose members include US and international higher education institutions, corporations, not-for-profit organizations, and K–12 institutions. With a community of more than 100,000 individuals at member organizations located around the world, EDUCAUSE encourages diversity in perspective, opinion, and representation. For more information, please visit educause.edu.

Introduction

We live in a digital era of near-constant risks and threats to our personal privacy. News headlines routinely remind us that our personal and professional data are vulnerable to attack, and technological innovations continuously introduce new ways for us to be watched and heard and tracked, with or without our knowledge, inside our homes and out in our communities.

These present-day realities are being felt more and more profoundly within higher education as well—particularly with the rise of remote and hybrid models of work and education—and are shaping the lived experiences of our students, faculty, and staff. Indeed, higher education might very well be at an inflection point in its orientation to privacy, and bold new visions may be needed now for what the future of higher education privacy can and should be.

As we imagine together what the future of higher education might look like, there is power in highlighting positive, generative visions that can help inspire us to plan and take steps toward a more desirable future state. As dire as things may seem at times, despair may ultimately fail us as an orientation to professional practice, leading to resignation and inaction. On the other hand, with grounded and reasoned hope in the ways in which we might build a better future, we may yet find the will to act and move the higher education privacy profession—and our institutions—forward.

Drawing on the insights of a small panel of higher education privacy experts and building on work previously done in the *2021 EDUCAUSE Horizon Report | Information Security Edition*, this resource is offered to the privacy and higher education communities as an actionable tool to help guide our thinking about tomorrow and to help inspire us to plan and take action today.

Contents

Goals for Our Future State

Asked to imagine what their institutions could look like in the future if they were to begin implementing effective privacy strategies today, our Privacy Action Plan panelists offered a hopeful vision for their institutions; for their staff, faculty, and students; and even for our local and global communities.

Institutions

Institutions are safer, more connected, and more strategic. Perhaps most obvious, improving privacy at the institution will lead to a safer institution with a lower risk profile. Though obvious, this hope for our shared future should not be overlooked and cannot be overstated—our institutions need to be well protected and less at risk, a critical goal for present-day planning and action.

Privacy professionals are just one part of an institutional ecosystem devoted to building safer institutions. The ideal institution of the future will have a shared understanding of and commitment to privacy across the whole institution, from institutional leaders down through each individual and all functional and academic units. This collaborative and holistic approach to privacy will extend even beyond the individual institution to a more connected global institutional network of shared privacy knowledge, practices, and policies.

Our privacy houses *will* be put in order. The ideal institution of the future will have an established privacy governance structure and oversight function, as well as established data management and governance capabilities, to guide the ethical and consistent use of student and institutional data (e.g., data mapping). These enhanced capabilities at the institution will no doubt necessitate investments in privacy staffing and infrastructure, resulting in fully staffed and resourced privacy units within the institution.

Students, Faculty, and Staff

Students, faculty, staff, and leadership understand and are invested in privacy. In some respects, privacy at the institution ultimately depends on the extent to which end users are informed and committed to it. In our ideal institutional future, end users (students, faculty, and staff) are routinely and consistently educated and trained in their institution's privacy policies and practices. The institution's privacy unit is highly visible and engaged in the life of the institution, and key stakeholders at every level of the institution are involved in helping shape and support their privacy program.

Robust privacy programs strengthen student experiences and outcomes. As informed and engaged stakeholders, students understand how and why their institutions use academic and personal data. A more visible and collaborative privacy function, along with more systematic and robust data governance structures, will have instilled in students a greater sense of trust in the use of their data and, subsequently, a greater sense of trust and investment in the institution overall.

Communities

Our local communities and global society are digitally safer and more informed. As individuals educated and profoundly shaped and developed by their higher education experiences, students have the potential to carry an awareness and appreciation for privacy with them into their post-college lives and into other private and professional sectors of society, expanding their influence for better, privacy-focused decision-making.

Higher education is a privacy leader on the global stage. Institutions themselves, as they build global networks for sharing privacy knowledge and practice and engage in policy discussions with national and international leaders, have seized opportunities to help shape public discourse and awareness of privacy issues. Higher education, in general, has claimed its seat at the global privacy table and is viewed as a leading partner in advancing privacy across all sectors of our global community.

Actions

With the future states for higher education institutions in mind, what actions did our panelists identify that might help privacy professionals and their institutions begin to make progress in those directions? If we tie a thread from the desired future states to our present-day planning and practice, we can begin to take the important step of converting our future hopes into current actions. It is to this critical step in our thinking that we now turn.

SHORT-TERM ACTIONS

Easier

- **Refine current definitions and terminology around privacy.** Efforts to clarify and disseminate the differences between "privacy as advocacy" (e.g., privacy is a fundamental right; privacy is an ethical norm) and "privacy as compliance" (e.g., ensuring privacy policies and laws are followed; privacy programs train, monitor, and measure adherence to rules) help frame conversations and set expectations.
- **Establish inter-institution information sharing and collaboration.** The issues confronting higher education privacy officers are similar across institutions. Sharing and collaboration avoid each institution's having to "reinvent the wheel" in efforts to enforce privacy regulations and promote privacy awareness and may also encourage creative problem-solving on privacy-related issues.

MID-TERM ACTIONS

Easier

- **Increase privacy awareness/knowledge across the institution.** Comprehensive and sustained privacy awareness campaigns (beyond Data Privacy Day) that target leadership, staff, faculty, and students can encourage greater compliance with rules and policies related to privacy while nudging people to be more attentive to the ways in which their own (and others') privacy can be jeopardized.
- **Integrate privacy risk analysis into third-party reviews and other projects.** A comprehensive privacy risk analysis baked into procurement and continuous review processes with third-party vendors puts privacy considerations at the center of conversations instead of treating them as afterthoughts or nice-to-haves. Recommendations based on risk analyses, however, need to have the backing of leadership to be effective.
- **Establish a privacy governance board.** Composed of existing leadership positions on matters of privacy, information security, ethics, compliance, and human resources, privacy governance boards provide executive institutional leadership with confidential consultation and greater collaboration on matters of data privacy.
- **Establish benchmarks for standardized privacy controls, practices, and policies across institutions.** Absent a federal initiative to create national standards, institutions would benefit from a coordinated standard for how higher education institutions comply with data privacy issues. Using established standards and resources such as the National Institute of Standards and Technology (NIST) Privacy Framework could reduce the burden of the creation of such benchmarks for institutions, especially those with limited resources.

More Difficult

- **Drive the ethics conversation through the creation of an ethics board or similar body.** While many institutions already have IRBs and data governance policies, "a data ethics board could support a continuous systematic review of management practices, technology purchases, and data governance and use."[1] Ethics boards would be charged with reviewing policies and procedures to ensure best data practices are followed when making decisions about what data to collect, how to store those data, and when and how to use them.
- **Have early input in open access (research data) implementation.** Whether required by grant conditions or desired for the sake of knowledge exchange, the open-access publishing of research data requires thoughtful and early consideration of which data can and should be made available. The creation of a data management plan that establishes the criteria for data de-identification, anonymization, and minimization protects the research subjects beyond the IRB by providing the primary investigators a roadmap for how to share their data widely.
- **Dedicate a person, team, and/or office to data privacy.** Institutions that are going to get serious about protecting data privacy need to invest sufficient financial and human resources to meet institutional needs and empower those in authority to implement policies and enforce compliance. The issue is not whether your institution can afford to dedicate resources to defending privacy; the issue is whether it can afford not to.
- **Develop a process to ensure privacy is a consideration in student analytics and institutional research.** Unfortunately, concerns about student data privacy have been minimal since the earliest days of the student success movement. Retroactively bringing these tools into compliance may be difficult to impossible, but implementing robust processes—similar to those of an institutional review board (IRB) review—for the use of student analytics and institutional research data going forward may shape choices about future uses of personal student data to promote student success.

LONG-TERM ACTIONS

More Difficult

- **Embrace data minimization at the point of collection.** No longer should higher education institutions collect all of the data they possibly can, in hopes that they might someday be useful. Instead, the principle of data minimization demands that data collection is limited to only those data that are necessary to complete a specific task. Furthermore, those data should not be used for any other purpose without obtaining the consent of the person from whom the data were collected. Retroactively, this may require institutions to de-identify, redact, and delete superfluous data and seek permissions for data currently in use.
- **Educate legislative bodies and advocate for higher education privacy laws.** Because the constitutional right to privacy in the United States is an implied one, the legal approaches to protecting privacy tend to vary by state, with some exceptions, such as FERPA and HIPAA. What higher education needs is a consistent and unified approach to privacy regulation spearheaded by privacy advocates in legislative bodies. Privacy laws that establish uniform rules for handling personally identifiable information in postsecondary settings eliminate the need to reconcile varying and often conflicting requirements.

1. Charles Mathies, "The Ethical Use of Data," *New Directions for Institutional Research*, no. 178 (November 23, 2018), 94.

Planning for the Road Ahead

Many of our institutions share similar experiences with the privacy challenges and opportunities highlighted throughout this report, enabling us to find a common ground and dream together about our collective futures. And yet our paths forward are wholly unique to each particular constellation of institutional contexts, goals, and resources, and it's up to each of us to determine whether and how our own institution will respond and adapt to those possible futures.

Your path from here may begin from a very personal place as you reflect on your own orientation to privacy at your institution and as you consider the role you might play in supporting your institution's privacy capabilities. As a next step, then, you might consider the following questions and document your responses to them:

- How does my role intersect with issues of privacy?
- Does my institution have a privacy policy? If so, have I reviewed it?
- How does my work intersect with my institution's privacy program?
- How can I stay current on news and issues related to privacy in higher education?

Alternatively, your path might begin by considering your institutional context and capabilities and reflecting on where your institution is on its journey and where it needs to go from here. Questions such as those listed below, or exploratory activities like the "Understand Your Institution's Policies" activity (see sidebar), might help you determine where to get started at your institution.

- Does your institution have a dedicated chief privacy officer and/or privacy team?
- Is your institution's privacy policy up to date and made available to all staff and students?
- How much of your institution's data are filtered through third-party tools and services? What are the implications of using third-party vendors?
- What level of visibility and support does your privacy program receive across the institution?

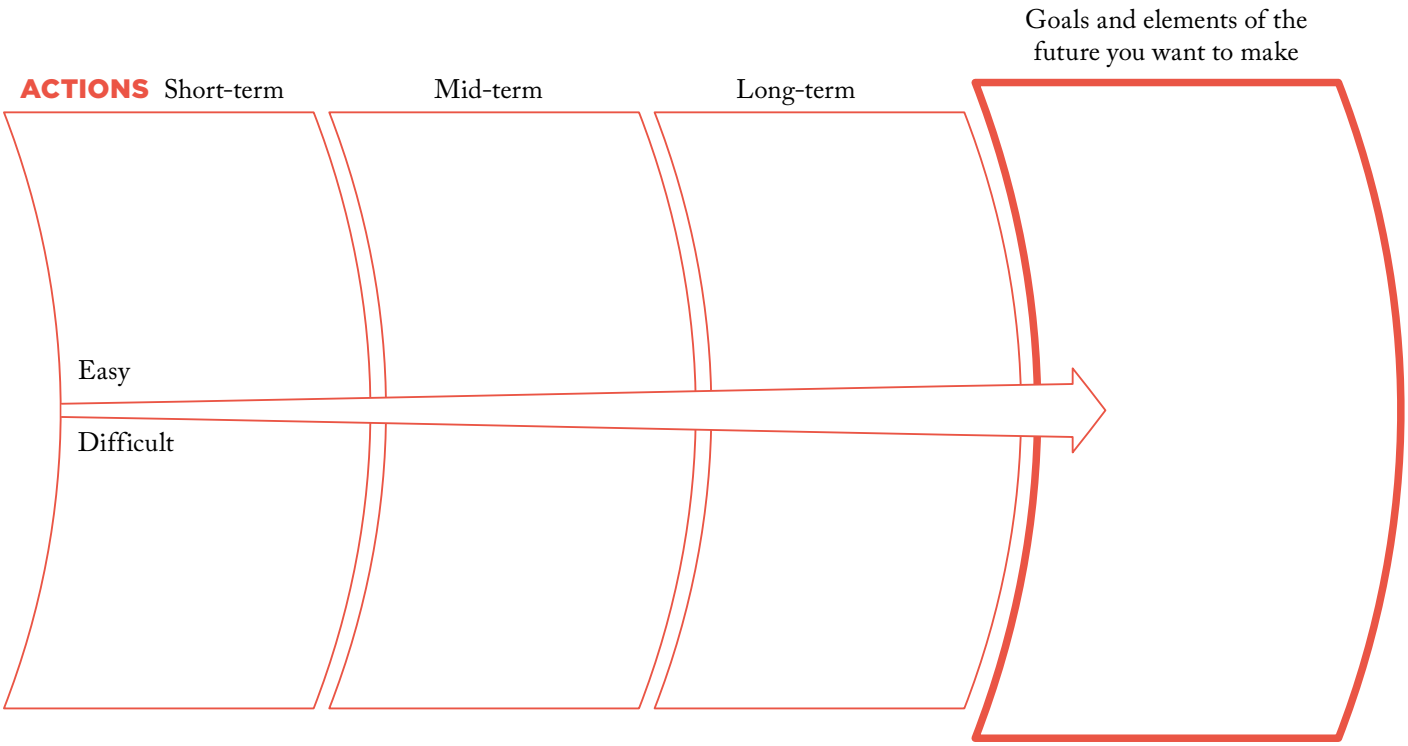
Activity: Understand Your Institution's Policies

It's important to understand how privacy regulations and best practices are managed at your institution. In this activity, you will research your institution's approach to privacy and begin to reflect on possible improvements for your institution.

- Identify who has responsibility at your institution for privacy policies. Some institutions have a chief privacy officer. If yours does, that's the best place to start. If it doesn't, then start by asking the senior leader for IT for advice on whom you should talk to.
- Once you identify a contact person, talk with that person about the following questions:
  - » What privacy policies or practices exist for the institution?
  - » Where are the institution's policies or practices around privacy posted or maintained?
  - » How is this information shared with the rest of the institution?
  - » What challenges are associated with policy communication, implementation, and compliance?
- Write a short (two pages or less) summary of your interview. Document whom you spoke to, their role in the institution, their responses to your questions, and any additional items you discussed. Also include references and links to any publicly available institutional policies or practices.
- Reflect on the interview and existing policies at your institution. Are any privacy policies or practices missing at your institution, or do any need to be strengthened? How would improvements be made in these areas, and how might your current role help support those improvements?
- Make a plan for whom you're going to share the results of your research with. You might want to discuss the results with your supervisor and consider together any direct actions you may be able to take. Or, if you're in a position of influence, you might want to assemble a team of stakeholders to discuss how you can move your institution forward together.

With a clearer sense of your own role in relation to privacy, and a broader understanding of your own institutional context, needs, and opportunities, you might then be in a better position to begin setting goals and charting your institution's path of short-, mid-, and long-term actions toward your ideal future state. To help you structure these goal-setting and action-planning activities, the Action Roadmap tool below (adapted from the Institution for the Future toolkit) provides you and your team with a framework for identifying where you want your institution to be and what you may need to do today and in the months and years ahead to get from here to there.

BUILD AN ACTION ROADMAP



© 2018 Institute for the Future. All rights reserved. SR-2012 | CC BY-NC-ND 4.0

Methodology

The *EDUCAUSE Horizon Action Plan: Privacy* is grounded in the perspectives and knowledge of an expert panel of practitioners and thought leaders from the United States who represent the higher education privacy community. The members of this group were sought out for their unique viewpoints, as well as their contributions and leadership within their domain. The panel reflects the current state of the higher education privacy profession, with most members representing larger, research-oriented institutions. Dependent as the *Horizon Report* efforts are on the voices of its panel, every effort was made to ensure those voices represented diverse perspectives and that each could uniquely enrich the group's work.

For the Privacy Action Plan, we adopted and adapted different components of the Institute for the Future (IFTF) foresight methodology. First, we asked panelists to review the trends, technologies and practices, and scenarios from the *2021 EDUCAUSE Horizon Report: Information Security Edition* and to individually brainstorm threats and opportunities that might emerge from them. Second, smaller groups of panelists were directed to review the threats and opportunities they identified, elevate the ones they deemed the most important and/or interesting, and brainstorm possible actions in response to those threats and opportunities. Third, panelists were asked to collaboratively rate the actions on the continuums of effort and impact (high to low for each). Fourth, panelists were asked to list milestones for change that they would like or expect to see at their institutions if the actions they identified were implemented. Finally, panelists were asked to vote on the time frame (short, medium, or long term) and level of difficulty (easier or more difficult) for each high-impact action. The data produced as a result of these efforts have been used to create the action plan featured in this report.

EDUCAUSE staff provided group facilitation and technical support but minimal influence on the content of the panel's inputs and discussions. This was done to reduce the potential introduction of bias into the results and to allow for this organized group of experts themselves to discuss and converge on a set of actions for the future, based on their own expertise and knowledge.

The panel discussions were held remotely on July 29, 2021, and August 4, 2021, by Zoom.

Expert Panel Roster

We would like to acknowledge and express our deepest gratitude to the panel of privacy experts listed below, who were responsible for generating all of the big ideas summarized throughout this resource. Their brilliant thinking and rich discussions were the foundation of this work, and this resource simply would not exist had it not been for their dedication to this project and their passion for serving the larger higher education privacy profession.

Mark Cather
Chief Privacy Officer
University of Maryland, Baltimore County

Holly Drake
Chief Privacy Officer
The Ohio State University

Jan Kiehne
Data Privacy Officer
Connecticut State Colleges and Universities

Dan LoPresto
Privacy Compliance Director & Data Protection Officer (DPO)
University of Central Florida

Pegah Parsi
Campus Privacy Officer
University of California, San Diego

Shannon Sinclair
Director of Privacy Compliance
Colorado School of Mines

Holly Swires
Chief Privacy Officer
The Pennsylvania State University

Kent Wada
Chief Privacy Officer
University of California, Los Angeles

Brian Kelly
Director of the Cybersecurity Program
EDUCAUSE

Mark McCormack
Senior Director of Analytics and Research
EDUCAUSE

D. Christopher Brooks
Director of Research
EDUCAUSE

Jenay Robert
Researcher
EDUCAUSE

Jamie Reeves
Product and Portfolio Senior Manager, Communities and Research
EDUCAUSE

Nichole Arbino
Communities Program Manager
EDUCAUSE

Emily Kendall
Communities Program Manager
EDUCAUSE