

The Role of the CPO

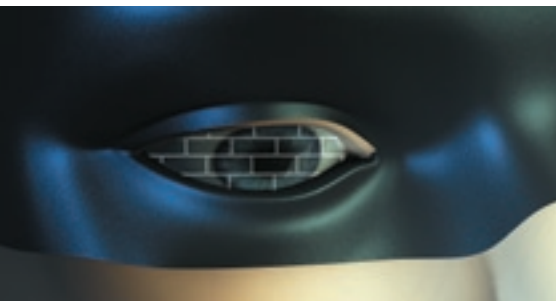
By Lauren Steinfeld and Kathleen Sutherland Archuleta

Privacy—and the loss of it—attracts attention. Few issues enjoy a higher national profile. And in the growing list of data breaches reported over the last year, the leading industry sector has been higher education.¹ Colleges and universities now find themselves in the spotlight as they grapple with an increasingly complex legal and regulatory environment relating to information privacy and security. It is not surprising, then, that a recent survey of college and university attorneys identified the proliferation of privacy regulations and technology to be among the most important issues and trends emerging for higher education in the next five to ten years.²

Lauren Steinfeld serves as Chief Privacy Officer at the University of Pennsylvania and was formerly Associate Chief Counselor for Privacy at the Office of Management and Budget. She sits on the Board of Directors of the International Association of Privacy Professionals. Kathleen Sutherland Archuleta is the former Assistant Vice President and Chief Privacy Officer for the University of Colorado system. Currently, she serves as special advisor to the University of Colorado and is the Membership Networking Director for the International Association of Privacy Professionals.

Failure to implement an effective strategy to ensure compliance with sweeping new laws poses significant financial and reputational risk—inviting additional scrutiny from privacy advocates, the plaintiffs’ bar, and government enforcement agencies. To address this challenge, institutions of higher education have begun to look to the private sector for lessons on creating comprehensive data privacy programs that mitigate risk while building trust with key stakeholders.

One fundamental lesson involves leadership of institutional privacy initiatives. In 2001, the *Wall Street Journal*



reported that the new position of Chief Privacy Officer, or CPO, was finding its way into Fortune 500 companies.³ IBM, American Express, General Motors, Eastman Kodak, Procter & Gamble, and many other household corporate names were beginning to focus on privacy and to designate senior-level personnel to champion and direct that focus.⁴ At the time, the International Association of Privacy Professionals (IAPP) had just been formed to represent the emerging profession. Today, the IAPP has 2,600 members, of whom 60–70 percent are practicing privacy professionals. According to Trevor Hughes, the executive director of the IAPP: “Our membership has grown so substantially because of the public demands for strong privacy protection and because of the demonstrated progress Chief Privacy Officers are making in meeting those demands consistent with their institutional priorities.”⁵

As more organizations have recognized the value of consolidating responsibility for privacy in a single “point-person,”⁶ certain themes can be gleaned about the role of the CPO in any sort of organization:

- The CPO champions the issue of privacy within the organization.
- The CPO leads or monitors major compliance initiatives around global, federal, and local privacy laws.
- The CPO assists in assessing privacy-related risks throughout the organization and promotes strategies to mitigate these risks through the development and implementation of infrastructure, standards for the collection, use, and sharing of personal information, vendor requirements, training, and other appropriate mechanisms.
- The CPO participates as a key team member in responding to and managing incidents resulting in the loss or potential compromise of personal data by the organization or its service providers.
- The CPO serves as the organizational point of contact for individuals, internally and externally, who have questions about privacy policies and practices, ranging from how to incorporate appropriate privacy considerations into new systems, programs, contracts, and other initiatives, to how to opt out of a certain program, to what the organization’s position is on marketing uses of data.

The CPO in Higher Education

The robust privacy agenda being pursued in the corporate arena and, more recently, in government⁷ is gradually finding its way into the higher education sector. With the growth of legislative and stakeholder demands for responsible information management, more colleges and universities are appointing CPOs to coordinate and guide privacy initiatives across the institution. Some would say that it’s about time.⁸ The ethical obligation of colleges and universities to protect the personal information of their many constituencies is no less than that of any other business or governmental entity, and campus privacy practices should be as thoughtful and rigorous as those in business and government.

Yet several distinctive features make coordinated privacy protection particularly challenging for the higher education sector and create additional risk. First, the types of constituents whose data are

collected go well beyond customers and employees. Colleges and universities collect data about students, faculty, staff, alumni, research subjects, donors, library patrons, retail customers, parents, board members, patients, online visitors, conference attendees, and others. Further, in operating campus “micro-communities,” colleges and universities provide a wide variety of services including housing, food, parking, retail stores, healthcare, IT and telecommunications infrastructure, legal, public safety, financial, construction, and cultural and athletic events—in addition to the actual educational services that are central to their mission. Each of these functions carries with it particular privacy risks, including compliance risks associated with the numerous privacy regulations that apply to specific activities or data.⁹ When this volatile mixture is placed in an environment characterized by decentralized governance, independent academic and research pursuits, and distributed business processes, the potential for significant risk to the enterprise is all too apparent.

Traditionally, higher education has attempted to manage these risks through targeted mitigation and compliance initiatives. However, as institutions have begun to adopt a “unified approach” to information security,¹⁰ they are also recognizing the value of an integrated program around privacy protection with a CPO at the helm. A number of organizations are adopting a comprehensive privacy strategy based on long-recognized fair information practices.¹¹ Regardless of the particular framework, a coordinated approach to privacy protection helps avoid duplication of effort, inconsistent policy, inefficient deployment of technology, and compliance gaps that can arise from a more distributed and reactive model.

Although the specific responsibilities of each CPO vary by institution, the role itself, properly designed, is critical. An informal survey reveals the following types of initiatives in which college and university CPOs have played a leadership role:

- Addressing compliance activities around the Family Educational Rights

and Privacy Act (FERPA), including notifying students of FERPA rights, training faculty and staff on the appropriate uses of student records, and providing tools for students to consent online and offline to sharing records and to opting-out of sharing directory information

- Addressing compliance activities around the Health Insurance Portability and Accountability Act (HIPAA), including developing policies and procedures and related training for handling information about patients and research subjects
- Developing strategies for reducing reputational, operational, and other risks related to the continued collection and use of Social Security numbers
- Educating students about how to use credit responsibly and to minimize the risk of identity theft, as well as about the safety and professional risks associated with certain online activities, such as posting to blogs and social networking sites like Facebook and MySpace.com
- Developing consensus on the types of faculty and staff contact information that should be made available within

stitution may monitor and/or access the documents, e-mail, and voicemail messages of faculty, staff, and students

- Developing procedures for the appropriate use of alumni data, including the process for selecting and administering partnerships with outside organizations offering services to alumni
- Creating a process and tool to facilitate the posting of privacy policies on all institutionally controlled Web sites
- Adopting a policy for the use of closed-circuit television cameras to record activities of members of the community for public-safety purposes

Key Elements for Success

The CPO cannot work alone to undertake the kind of cross-functional initiatives and activities described above. The nature, reach, and overall effectiveness of any privacy program are influenced by certain critical elements. An institution's willingness to provide key "ingredients" will make the difference between a successful privacy program and a well-intentioned but ultimately feckless effort.

The first key ingredient for success is, not surprisingly, visible and sustained

and of the creation of an institution-wide privacy program. Public, senior-level support can ensure strong credibility for the initiative from the outset and can energize the campus community to actively participate in the effort. Institutional support can also be reflected in the allocation of organizational resources to the privacy program. Even the most earnest public statement of support for the initiative will ring hollow if the CPO has no budget at his or her disposal to carry out the necessary work.

A second important ingredient for success is a CPO who possesses the necessary skill set. Most CPOs have backgrounds in privacy-related functions, such as legal, public, or government affairs, marketing, or information technology.¹² A solid grasp of the laws that affect the institution's operations is certainly necessary. In late 2004, the IAPP established the Certified Information Privacy Professional (CIPP) credential, which many in the field have obtained by participating in the training and testing process administered by the IAPP. According to the AICPA/CICA "Roadmap for Protecting Privacy of Personal Information," the privacy officer's effectiveness will depend largely on: (1) a

Even the most earnest public statement of support for the initiative will ring hollow if the CPO has no budget at his or her disposal to carry out the necessary work.

the institution and to the public and incorporating these decisions into an online directory project

- Creating a methodology for "building privacy" into new IT applications and databases
- Leading a compliance program regarding the Payment Card Industry Data Security Standard (PCIDSS) to protect sensitive cardholder data and avoid significant monetary penalties for noncompliance
- Collaborating with other operational units such as information security, procurement, and legal counsel in establishing vendor management programs and appropriate language for contracts involving confidential data
- Creating policies and procedures regarding whether and when the in-

support from the top. As required for any effective compliance initiative, executive management—from the governing board to the president and chancellors—must have a clear understanding of the program's ultimate goals and must stand behind them. Independent-minded, busy people from academic or business units may not be willing to set time aside to reexamine privacy controls if the senior leadership fails to demonstrate a firm institutional commitment to responsible information management and the value of safeguarding individual privacy. This support can take form in a variety of ways. One example is a governing board resolution recognizing the importance of information privacy and security. Another example is a media campaign for public awareness of the appointment of the CPO

broad understanding of how the organization works and its organizational culture, (2) a positive track record of working with cross-functional teams, (3) strong interpersonal, communications, and leadership skills, and (4) technical savvy about data management and computer systems.¹³

In addition, the CPO should be placed appropriately in the organizational structure so that his or her scope of authority is sufficiently strong and broad in reach to allow the CPO to be effective.¹⁴ According to one study, 82 percent of privacy officers report directly to senior officials. A more recent benchmark study indicates that almost half of appointed privacy leaders report to senior executives at the C-level (e.g., CEO, COO, CFO, CRO).¹⁵ In higher education, CPOs tend to report to the

legal, internal audit, compliance, provost, or risk-management functions.

Perhaps the most significant success factor for a CPO is effective outreach and collaboration, on several fronts. Strategic partnerships are important to understanding and prioritizing issues for the institutional privacy initiative. Key partners include the following:

- System and campus compliance and information security officers
- Campus and unit-based privacy coordinators
- Legal counsel
- Internal audit department
- IT services units
- Provost's office
- Registrar's office
- Government relations
- Law enforcement
- Human resources
- Communications/public relations
- Facilities and emergency management operations
- Marketing and alumni relations/development
- Procurement services
- Members of the executive management team

In addition to setting the privacy agenda, collaboration is necessary for implementation activities. New privacy-

answer to the challenge of one centrally placed individual or office attempting to “make privacy protection happen” throughout the institution. In fact, a recent benchmark study of corporate privacy practices revealed that 93 percent of respondents have a cross-functional committee to manage privacy initiatives, with 70 percent of these companies appointing their designated privacy leader (CPO) to chair this committee.¹⁶

One collaborative relationship is so important that it deserves special attention: the partnership between the CPO and the Chief Security Officer (CSO). A brief discussion of the relationship between “privacy” and “security” is warranted here. The terms are often used interchangeably in discussions of data protection, and some say that you can't have the former without the latter. However, there is a distinction between the two frequently complementary, interdependent principles. For organizations like colleges and universities, privacy involves the policies, procedures, and other controls that determine which personal information is collected, how it is used, with whom it is shared, and how individuals who are the subject of that information are informed and involved in this process. These are the fundamental privacy principles that a robust privacy program should be designed to

following: conducting inventories and mapping personal information data flows; educating the community about appropriate steps to safeguard confidential data; developing a risk-assessment process to determine the adequacy of administrative, technical, and physical data-protection measures; and adopting and applying incident-response procedures when personal data are involved. The collaboration is equally important when privacy and security interests are at odds, such as in programs designed to collect sensitive personal data in the name of public safety or information security. In these cases, “bringing privacy in” can help identify opportunities to be less intrusive, to orient communications to address privacy concerns, or to otherwise reflect privacy values in a program designed to meet broader institutional interests.

Conclusion

Privacy management is an essential component in any organization's overall effort to manage information responsibly. In higher education, that effort is uniquely challenging. The success of an institution's privacy program depends on senior management support, the skill set and organizational placement of the CPO or other privacy professional, strategic partnerships, and collaboration.

The success of an institution's privacy program depends on senior management support, the skill set and organizational placement of the CPO or other privacy professional, strategic partnerships, and collaboration.

driven information systems will not get built without the participation of the IT organization. Notices of FERPA rights will not be distributed without the engagement of the registrar. Contracts will not include necessary language concerning the privacy and security of sensitive information without the assistance of legal counsel and procurement services. The list goes on.

Collaboration is also necessary to implement certain initiatives, such as training and awareness or risk-assessment programs, that must be carried out at a local level. Establishing a distributed network of privacy liaisons in major organizational units can provide an effective

address, under the direction of the CPO.

Information security, on the other hand, includes the process of protecting data from accidental or intentional misuse by people inside or outside the organization. Although information security is by no means strictly a technical problem, its technical aspects (e.g., firewalls, encryption) are important. Accordingly, an organization's CSO is charged with establishing standards to ensure the integrity and security of sensitive data, at rest and in transit.

The relationship between the CPO and the CSO is critical when privacy and security initiatives reinforce one another. Examples are abundant and include the

With these in place, colleges and universities can align the value of responsible privacy protection with other institutional priorities.

A privacy program can be based merely on complying with applicable laws, but such a compliance model is the least mature in the range of privacy program models.¹⁷ To be sure, achieving and maintaining such compliance is no small feat, especially in the diverse, decentralized higher education environment. But colleges and universities owe more to their constituents—many of whom are particularly vulnerable due to their youth or health status and many of whom have little choice but to

entrust the institution with their most sensitive personal information. Indeed, college and university constituents are demanding more every day. The case for the appointment of the Chief Privacy Officer to meet these demands in higher education has never been stronger than it is today. *e*

Notes

1. See, e.g., "A Chronology of Data Breaches Reported since the ChoicePoint Incident," Privacy Rights Clearinghouse Web site, <<http://www.privacyrights.org/ar/ChronDataBreaches.htm>>. See also Lynn Doan, "College Door Ajar for Online Criminals," *Los Angeles Times* (May 30, 2006).
2. National Association of College and University Attorneys (NACUA) Survey Report: Summary of Responses to the Survey of NACUA Committee Members and Higher Education Associations (March 21, 2006).
3. Kemba J. Dunham, "Your Career Matters—Hot Titles: The Jungle," *Wall Street Journal*, February 20, 2001, p. B14.
4. Jennifer Bresnahan, "The Business Case for Privacy," *CIO Enterprise Magazine*, March 15, 1998.
5. Author interview with J. Trevor Hughes, Executive Director, International Association of Privacy Professionals, July 7, 2006.
6. Steve Ulfelder, "Oh No, Not Another OI?" *CIO*, January 15, 2001, <<http://www.cio.com/archive/011501/ohno.html>>; Edward Hurley, "CPO: An Enterprise Point-Person for Privacy," *Search Security.com*, January 27, 2003, <http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci876634,00.html>.
7. See David Perera, "The Need for Privacy: Should Every Agency Have a Chief Privacy Officer?" *FCW.com*, April 11, 2005, <<http://www.fcw.com/article88549>>; Judi Hasson, "3 Principles for Chief Privacy Officers," *FCW.com*, September 5, 2005, <<http://www.fcw.com/article90645-09-05-05-Print>>.
8. See Fred H. Cate, "The Privacy and Security Policy Vacuum in Higher Education," in this issue of *EDUCAUSE Review*; Dan Carnevale, "Colleges' Online Records Are Treasure to Hackers, Cybersecurity Expert Warns," *Chronicle of Higher Education*, May 12, 2006. See also Eric J. Sinrod, "Perspectives: Universities Need a Privacy Refresher Course," *CNET News.com*, April 26, 2006, <http://news.com.com/Universities+need+a+privacy+refresher+course/2010-1029_3-6065085.html>.
9. For example, at the federal level, healthcare activities are regulated by HIPAA, financial services activities by the FTC safeguards of the GLBA, student-related activities by FERPA, certain e-mail messages by the CAN-SPAM Act, and credit reports and background checks by the FACTA information disposal standards. This list does not even take into account applicable international and state laws or industry requirements such as the PCIDSS. See M. Peter Adler, "A Unified Approach to Information Security Compliance," in this issue of *EDUCAUSE Review*.
10. See *ibid.* This approach is based on established national and international standards such as ISO 17799 or the NIST framework.
11. These practices form the underpinning of many U.S. and international privacy laws and emerging privacy frameworks. See Section III, "Fair Information Practice Principles," in Federal Trade Commission, *Privacy Online: A Report to Congress*, June 1998, <<http://www.ftc.gov/reports/privacy3/toc.htm>>. For an example of a unified privacy framework, see the AICPA/CICA Privacy Framework (November 15, 2003; revised March 22, 2004), <http://www.aicpa.org/download/innovation/baas/ewp/privacy_framework.pdf>.
12. Elizabeth Clampet and Gabe Armstrong, "CPOs Confront Business Reality," *Inside 1to1 Privacy*, September 8, 2005, <<http://1to1media.com/view.aspx?DocID=29113>>.
13. American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA), *Privacy Matters: An Introduction to Personal Information Protection* (2003), 12–13. See also Don Peppers and Martha Rogers, "Have You Got What It Takes to Be a CPO?" *Inside 1to1 Privacy*, September 8, 2005.
14. Jay Cline, "So You Want to Be a Privacy Pro," *Computerworld*, November 11, 2005, <<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=105986>>.
15. Joint study by Privacy & American Business and the Association of Corporate Privacy Officers, cited in AICPA/CICA, *Privacy Matters*, 13. See also Ponemon Institute, "2005 Benchmark Study of Corporate Privacy Practices," July 11, 2005, <http://www.vontu.com/uploadedFiles/global/2005_Benchmark_Study.pdf>.
16. Ponemon Institute, "2005 Benchmark Study."
17. *Ibid.*