Information privacy is not a technology concept. Long before there were Chief Privacy Officers working to address practical information privacy problems, lawyers and academics studied and worked on privacy issues. The majority of people who enter the still-nascent information privacy profession come from non-technical fields including legal, compliance, marketing, and risk management. In 2012, the annual Privacy Professionals Role, Function, and Salary Survey from the International Association of Privacy Professionals (IAPP) found that the majority of privacy offices—59 percent—report through legal (30%) and compliance (29%) departments, with only 9 percent reporting through information security and only 5 percent through information technology. So why is information privacy the focus of this issue of EDUCAUSE Review and EDUCAUSE Review Online? The IAPP survey contains the answer: “Meeting regulatory compliance requirements continues to be the top perceived driver of privacy office funding, while concern about required data breach notifications and the bad publicity that such announcements entail grew in importance among survey respondents, with almost nine in every 10 listing it as a concern.”
It's all about the data. Regardless of which office oversees privacy or who causes data breaches, protecting privacy is inescapably tied to technology, due to the almost universal use of technology to collect, store, process, and utilize personal information in the pursuit of organizational goals. It is thus important that all IT professionals have the intelligence they need to embrace their role as participants in, or even as leaders of, institutional information privacy efforts. IT senior leaders and IT staff should learn what privacy is, why it is important in higher education today, and how they can identify and address privacy risks. CIOs in particular can then respond positively to institutional efforts to assign responsibility for privacy—or even better, to spearhead such an effort.

**Definition and History**

Although there is no universally accepted definition of “information privacy,” the following definitions represent three major perspectives:

- **“Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.”**

- **“[Privacy is] the appropriate use of personal information under the circumstances. What is appropriate will depend on context, law, and the individual's expectations; also, [privacy is] the right of an individual to control the collection, use, and disclosure of personal information.”**

- **“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.”**

Notice that the word “privacy” is usually by itself, without the clarifying “information” preceding it. However, the term “information privacy” is more accurate because it rarely covers activities such as designing facilities, furniture, and workplaces in ways that enhance physical privacy. Information privacy focuses on anything that leaves an information trail, whether or not that trail is digital. IT professionals should be prepared to advise and assist with privacy issues concerning oral, paper-based, and digital information, including images and video.

Privacy is not security. Although it is possible to have security without privacy (e.g., system administrators can view any data they please, due to their legitimate full-access rights, though administrative policies and personal ethics would normally prevent such behavior), it is not possible to have privacy without security. Typically, security professionals are very comfortable deploying physical and technical safeguards such as installing locks, deploying access control, avoiding viruses, patching vulnerabilities, and implementing encryption, but many are less comfortable working on administrative controls such as policies, awareness and training, on-screen wording that clearly describes to end users how applications work, appropriate use agreements, and contracts. Privacy augments strong physical and technical controls with correspondingly strong administrative controls.

**How Did We Get Here?**

Information privacy became the subject of attention several times in the eighteenth and nineteenth centuries. For example, the British Parliament passed the 1710 Post Office Act to protect the confidentiality of letters in the North American colonies, and the U.S. Congress passed “An Ordinance for Regulating the Post-Office of the United States of America” in 1782. The U.S. Census, containing citizens’ personal information collected by the government, prompted privacy concerns that resulted, by 1840, in promises of confidentiality of the information and also, by 1889, in a law that significantly fined census officials for disclosing confidential information. The introduction of the telegraph led to laws in the late 1800s to keep the contents of telegraphs confidential. The now-famous 1890 *Harvard Law Review* article “The Right to Privacy,” by Samuel Warren and Louis Brandeis, was inspired by the authors’ concern with protecting Americans from the intrusiveness of photography and the press, a concern generated by the new Kodak camera, a general-consumer camera placed on the market that year.

None of these developments generated enough activity to cause the creation of a privacy profession. Americans were not quite ready. As the Irish dramatist George Bernard Shaw noted when giving a speech in New York in 1933: “An American has no sense of privacy. He does not know what it means. There is no such thing in the country.” Not until the technology called “computing” entered the scene do we see another flurry of attention to privacy issues in the United States. Yet if we claim the year 1951, with the introduction of the UNIVAC, as the start of the computing technolog-
ogy revolution, it still took nearly fifty more years for information privacy to become a profession—and even longer for higher education to take notice.

Technology innovation and privacy law practically danced around each other during those fifty years. In 1970, the Fair Credit Reporting Act (FCRA) required credit agencies to allow consumers access to their credit records to review and correct mistakes. The Privacy Act of 1974 regulated the type of personal information the federal government can collect about private individuals and how that information can be used. The 1974 Family Educational Rights and Privacy Act (FERPA) is designed to protect the privacy of education records, to establish the right of students to inspect and review their records, and to provide guidelines for the correction of inaccurate data. Meanwhile, technology innovations added confusion around how to apply these laws. In 1969, the ARPANET connected four research centers, and in 1971, Ray Tomlinson sent the world’s first e-mail communication. Tomlinson later claimed that the contents were “entirely forgettable” and that he had, therefore, forgotten them.11 By 1973, e-mail constituted 75 percent of ARPANET traffic.12

Technology innovations continued: by 1976, several personal computers for consumers were available; in 1986, the NSFNET launched, incorporating ARPANET connections into its broad reach and eventually becoming the Internet. The legislative process responded in 1986 with the Electronic Communications Privacy Act (ECPA), which extended restrictions on wiretaps from telephone calls to transmissions of electronic data by computer and prohibited both the interception of electronic communications and access to stored electronic communications. In 1990, the first commercial provider of dial-up access offered its services, and in 1991, the first World Wide Web server appeared on the network. Maybe that web server was the last straw: also in 1991, Acxiom Corporation, a data broker, became one of the first organizations on record to appoint a Chief Privacy Officer, or CPO.

The pace of the dance picked up. In 1995, the Internet went commercial, and law enforcement took advantage of the change: the first official Internet wiretap was successful in helping the Secret Service apprehend three people who were illegally manufacturing and selling cell phone cloning equipment. In 1996, the Health Insurance Portability and Accountability Act (HIPAA) applied privacy requirements to health care, covering a small part of overall college and university operations. In 1999, the Financial Services Modernization Act, also known as the Gramm-Leach-Bliley Act (GLBA), established guidelines for the collection of personal data in the banking and insurance sectors and also covered a small part of college and university operations. That same year, the Federal Trade Commission (FTC) took its first Internet privacy enforcement action against Geocities, for deceptively collecting personal information.

Some of the laws, most notably HIPAA, require accountability through the assignment of a person to manage an organization’s efforts to comply. The IAPP was founded in 2000 to provide a professional community and certification for these individuals, and in 2001, the Wall Street Journal reported that the new position of CPO was finding its way into Fortune 500 companies.13 Finally, in January 2002, the University of Pennsylvania named Lauren Steinfeld as CPO—the first recorded instance of that position in higher education—and in September 2002, the University of Florida named Susan Blair as CPO. Interestingly, in that same year, the Department of Homeland Security was the first federal agency required by statute to appoint a CPO.

Higher education had not ignored privacy prior to this time, especially as it related to compliance with the law, but colleges and universities handled privacy in silos. Legal counsel monitored legislation, highlighted the need for compliance, and ensured that an office took on the day-to-day responsibilities, whereas registrars typically dealt with FERPA compliance, health science or research staff dealt with HIPAA compliance, and financial staff dealt with GLBA compliance. Higher education (and indeed, all other sectors) did not realize what was about to hit them.

The Tipping Point
The tipping point that pushed all organizations past the comfortable privacy-by-silo model and into the uncomfortable realization that privacy required more organization-wide attention and coordination was California’s SB 1386, introduced in February 2002 and effective on July 1, 2003.

SB 1386, a personal-data-protection statute, covers information such as Social Security numbers (SSNs) and outlines data breach notification requirements. It was the beginning of a new breed of privacy law. Over the next three to five years, nearly every state passed similar legislation. Just what was so different about SB 1386 and its copycats that caused organizations to realize they needed more integrated information privacy management?

- Notification: Prior to SB 1386, data-protection laws did not require notification to affected individuals. The notification requirement introduced significant costs and negative publicity in the event of a breach.
- Commonly Used Data: No universally used data, such as SSNs, had
been covered by previous laws—and SSNs were handled by nearly everyone working in higher education before the mid-2000s, since institutions were required to collect them both for employees and for student financial aid. Historically, SSNs had been the unique identifier.

- **Enforcement:** In general, prior to SB 1386, privacy laws were not enforced routinely through sanctions. For example, there had been no FERPA enforcement actions, even though FERPA had been in place since 1974. However, California and other state attorneys general were now enforcing these new laws, causing increased attention to many of the other privacy laws by their enforcing authorities.

- **Private Right of Action:** Older laws did not usually allow a private right of action, whereas many of the state data-protection laws now did. This increased the risk of legal action against the business or organization.

- **Criminalization:** Older laws did not make mishandling of protected data a crime, whereas many of the state data-protection laws now did. This was a game-changer for higher education: individual employees were now accountable for any data breaches they might cause—for example, due to negligence. Even if an institution had an indemnification policy and chose to cover the legal costs of defending an employee charged with the crime, the employee could go to jail if the defense was unsuccessful.

**Implications for Higher Education**

In 2005, the Privacy Rights Clearinghouse began its “Chronology of Data Breaches.” The first three listings in that year highlighted higher education breaches. In 2006, the “Chronology” reported that 52 percent of breaches involving outside hackers were in the higher education sector. In 2007, the total number of breach incidents reported by institutions of higher education rose 67.5 percent—to 139 incidents. In 2008, the number of data breach

---

**PRIVACY RESOURCE RECOMMENDATIONS FROM THE HIGHER EDUCATION CHIEF PRIVACY OFFICERS (HE-CPO)**

Freely available mailing lists, newsletters, and blogs:
- IAPP Daily Dashboard
  https://www.privacyassociation.org/publications/daily_dashboard
- IAPP Inside 1to1: Privacy
  https://www.privacyassociation.org/publications/inside_1to1_privacy/
- Privacy and Information Security Law Blog from Hunton & Williams
  http://www.huntonprivacyblog.com/
- Privacy Rights Clearinghouse
  https://www.privacyrights.org
- Electronic Privacy Information Center (EPIC)
  http://epic.org/alert/

Basic standards on which most privacy programs and legislation are based:
- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
  http://www.oecd.org/document/18/0,3746,en_2649_34223_1815186_1_1_1_1,00.html
- Generally Accepted Privacy Principles (GAPP), American Institute of Certified Public Accountants Inc. and Canadian Institute of Chartered Accountants
  http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples
- Security and Privacy Controls for Federal Information Systems and Organizations, Special Publication (SP) 800-53, Revision 4 (Initial Public Draft)
  http://www.nist.gov/itl/csd/sp800-022812.cfm

Seminal works:

Professional groups:
- International Association of Privacy Professionals (IAPP)
  https://www.privacyassociation.org/
- Higher Education Chief Privacy Officers (HE-CPO)
  Contact Valerie Vogel at EDUCAUSE: vvogel@educause.edu

Certification:
- Certified Information Privacy Professional (CIPP) and specialized certifications for the United States, Canada, Europe, the U.S. government, and information technology
  https://www.privacyassociation.org/certification
incidents and profiles compromised by all education-related organizations was found to be “disproportionately high compared to the total of all other U.S. enterprises that reported data breach incidents.”

However, by 2009, the “Chronology” had turned its attention from higher education to health care. Clearly, someone in higher education institutions was—and is—working on privacy issues. But who? Higher education institutions typically do not have large enterprise-wide legal and compliance offices and typically do not assign many C-level titles such as CEO, CFO, CTO, CCO, and CPO. More likely, privacy duties in colleges and universities are being shared by the information security office, the data management group, the compliance silos mentioned previously, university counsel, and various others. Current financial pressures can preclude assigning even one full-time person the singular title of Chief Privacy Officer. Instead, additional duties are likely assigned to staff holding other titles, or—a favorite solution—one person is given multiple titles (and corresponding duties). The most important action that higher education institutions can take is to assign overarching privacy coordination duties to someone—no matter his or her title or where the person is organizationally situated—and enable that person to work cooperatively with other areas to achieve objectives.

As of fall 2012, IAPP membership included 246 individual members (out of 11,138) from higher education institutions; 121 of those held at least one privacy certification. Although that number includes academics, the number of practitioners was high enough to cause the formation of a Higher Education Chief Privacy Officers group (HE-CPO) in 2012, which brought together approximately 34 self-identified individuals who have been assigned lead information privacy responsibilities by their institutions. However, only 3 in the group have the title Chief Privacy Officer with no additional titles, and 10 do not even have the word “privacy” in their titles.

What Do Higher Education Privacy People Do?
CPOs or individuals who are assigned lead privacy duties take a risk-based approach to privacy and focus on strengthening administrative controls, working in partnership with security professionals on physical and technical controls and with data management professionals on data classification. Activities include the following:

• Creating and overseeing an Information Privacy Program for the institution (often in coordination with the Information Security Program), with an appropriate governance structure
• Managing privacy and security breach incidents
• Developing privacy policies or working with others to incorporate privacy into other policies (e.g., employee, student, and visitor electronic data; website privacy notices; customer relationship management; human subjects research; video surveillance)
• Assessing the privacy impact of business processes, services, and projects and providing guidance on how to reduce identified privacy risks
• Crafting language for documentation such as privacy notices, forms requesting personal information, user help screens, and appropriate-use agreements
• Advising decision-makers on privacy risks so that they can make prudent decisions—for example, when determining whether or not to implement a technology option or to contract with a third party
• Reviewing contracts with third parties to include wording that ensures the proper handling of institutional data shared with that party
• Coordinating with information security, data management, legal counsel, internal audit, compliance, risk management, and others
• Providing awareness and training and teaching others how to “think privacy” so that privacy becomes part of the day-to-day thinking of all employees
• Maintaining knowledge of privacy law and generally accepted best practices

Overview of Privacy Harms and Principles
Even if an institution has a CPO, all of those who are working to provide the infrastructure to collect, store, process, and utilize personal information in pursuit of the organization’s goals need to continually evaluate how their service affects privacy and need to take action to reduce any identified privacy risks.

Privacy Harms
How can an institution determine whether a business process, service, or project is going to be or already has been implemented in a way that might cause a privacy risk? The following list of privacy harms, based on the work of Alan F. Westin and Daniel J. Solove, includes questions particularly related to interactions with users whose information is being collected, used, disclosed, and retained.

Information Collection. Is the institution collecting information about users or
watching what users are doing, more than it should? Examples include surveillance (watching, listening to, or recording a user’s activities); interrogation (inappropriately probing for information); visual monitoring (viewing private activities without the user’s knowledge); communications (wired tapping phones or viewing e-mail or Internet transactions); and “too much information” (unnecessarily asking for what the user thinks is “private” information or collecting information not really needed for the transaction). Whether or not someone at the institution actually looks at the information does not even matter; the fact that the information is being collected will concern people.

Information Processing. Is the institution storing, manipulating, and using users’ data in a way that they might not like or expect? Examples include data mining that makes assumptions about patterns (deciding if users are good students based on how many times they accessed an online textbook); aggregation (combining pieces of users’ information collected from different sources); identification (linking unidentified information elements to particular users, perhaps to learn about “anonymous” actions); insecurity (failing to protect information from leaks and unauthorized access); secondary use (using collected information for a purpose different from the use for which it was collected, without users’ consent); and exclusion (using data to exclude a user, especially if the data was incorrect or interpreted incorrectly). Information processing can be helpful when it “personalizes” and gives better service. However, it can invade privacy when it goes too far or is used in unexpected ways. Does the institution keep information long after it is finished with the data? This can make the information vulnerable to processing harms. Privacy is a balancing act: users are going to balance the gains from using a service against the potential privacy harms. Some may choose not to use a service because they do not know how the institution will process their information.

Information Dissemination. Is the institution planning to spread or transfer information about users, more than they might like or expect? Examples include breach of confidentiality (breaking an agreement to keep information confidential); disclosure (sharing data with or transferring data to unexpected persons or entities); exposure (revealing intimate information, and many users consider any personal picture to be intimate); increased accessibility (making information more accessible, for instance by putting paper records online and indexing by search engines); blackmail (threatening to disclose personal information); appropriation (using a user’s identity, such as a name or picture, without permission); and distortion (disseminating false or misleading information about users). Information dissemination is one of the most commonly performed harmful activities—every time a cloud service or third party is used.

Invasion. Will the institution go into users’ spaces and contact them or tell them what to do? Examples include invasions into private affairs; invasive acts that disturb users’ tranquility or solitude; decisional interference (entering into users’ decisions regarding private affairs); unwanted e-mail (many people consider e-mail to be a personal space, which is why they become upset when colleges or universities e-mail unwanted communications); unwanted phone calls (most users consider phone numbers, especially cell phone numbers, to be personal space); and entering a room without knocking.

Privacy Principles

Once the privacy risks are understood, the institution must take steps to address them. Information privacy is enhanced through the application of the Fair Information Practice Principles (FIPPs), through principles outlined in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, and through the Generally Accepted Privacy Principles. In nearly every situation, an institution should be able to identify one or more actions it can take to address any privacy issues, while still achieving its business goal.

Notice. Identifying a way to inform users of institutional practices around the data collected from them is usually the easiest way to address most privacy harms. Posting a privacy policy on the institutional website or explaining on a form or login screen the plans for the data that users will enter is a way to provide notice. Institutions should explain who will be collecting the data, how the data will be used, who will receive it, and the steps that will be taken to preserve the confidentiality, integrity, and quality of the data. Any automatic collection of data—such as log files and
data collected by web analytics engines—should be described as well.

Choice and Consent. Can the institution identify a way to obtain implicit or explicit consent from individuals with respect to the collection, use, disclosure, and retention of their information? Choice may apply to “secondary uses”—that is, uses beyond the original reasons for which the data was provided. Sometimes choice is “opt in” (the institution will not share the data without agreement), and sometimes choice is “opt out” (the institution can share the data or contact users, but users have a way to stop the sharing or contact). Can the institution give options, perhaps by providing checkboxes to indicate consent to various uses?

Collection Limitation. Can the institution review what data it is collecting with the business process owner and ensure that it is collecting only the information needed to achieve the purposes identified by the business unit in support of the university’s mission and as outlined in the notice? Especially critical here are very sensitive or risky pieces of data such as SSNs and birthdates, which need to have a significant business purpose for collection. “Because we’ve always done it that way” is not an excuse in this post-SB 1386 world.

Use and Retention. Can the institution ensure that the collected information will be used only as outlined in its notice, with no unexpected “secondary uses”? Can it ensure that it is keeping the information only as long as necessary to fulfill the stated purposes? Once the data is collected, an institution can be compelled to reveal it through certain legal orders. But if an institution does not have the data, it cannot be compelled to provide the data. On the other hand, if a law or business practices require the institution to retain the data for a set period of time, it must be retained for that long—and must be protected appropriately while being retained.

Disclosure Limitation. Can the institution review with the business process owner what it is disclosing to whom and ensure that it is disclosing information to others only as outlined in the notice and only as consented to—either implicitly or explicitly? Contracts should be reviewed regularly with third parties, to ensure up-to-date and appropriate data-protection language.

Access. Can the institution provide access to users to review and update or correct their own information? This should be possible, especially when decisions will be made based on that data. In fact, FERPA outlines the right of students to petition for correction of errors in their student records. The Privacy Act outlines the right of individuals to see records about them that are held by the federal government. The Fair Credit Reporting Act was enacted because consumers with errors on their credit reports had no way to correct them. This process need not include a beautifully designed online form; it can be manual.

Institutions should explain who will be collecting the data, how the data will be used, who will receive it, and the steps that will be taken to preserve the confidentiality, integrity, and quality of the data.

Integrity and Security. Is the institution applying reasonable technical, physical, and administrative measures to secure its systems and data and to ensure data integrity? Incorrect data is as bad as, if not worse than, missing data, since incorrect decisions can adversely affect individuals.

Enforcement and Redress. Does the institution provide a way for users to complain—for example, to report issues to the institution or to a central Incident Response unit? Are reported issues investigated? Are dispute-resolution mechanisms in place? At its simplest, redress should include a righting of the wrong; when issues are reported, does the institution correct misinformation or cease the harmful practice? Does it post easy-to-find information for users to learn about enforcement and redress procedures?

Reflections

From the 1710 Post Office Act of the British Parliament to SB 1386 in 2003, laws have progressed to protect the privacy of individuals at the same time that technology innovations have continually pushed our understanding of how to apply those laws. Although the dance between law and technology in the quest to protect privacy is never-ending, the information privacy profession already has a foothold in institutions of higher education. Now is the time for every institution to assign an individual to coordinate privacy activities and to infuse the college and university community with basic awareness. Colleges and universities may not yet—or indeed ever—be able to support large numbers of Chief Privacy Officers, but they can create privacy-intelligent enterprises by coordinating privacy activities, revealing the basics of information privacy, and encouraging the application of these basics to day-to-day activities, especially those related to the collection, storage, processing, and utilization of data.
Notes
4. In fact, the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act (ARRA) in 2009, added notification requirements for personal health information in order to update the “older” HIPAA law from 1996.
6. I have been fortunate to be able to provide input on physical privacy issues at my institution (e.g., placement of bathrooms, use of privacy panels below conference room tables, and provision of private space for nursing mothers and self-administered medical care needs), but this is not common.
14. In fact, the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act (ARRA) in 2009, added notification requirements for personal health information in order to update the “older” HIPAA law from 1996.
19. A list of members is available at http://www .educause.edu/policy/be-cpo.
20. Many theorists have worked to identify and classify privacy harms. One of the first was Alan F. Westin, in his classic book Privacy and Freedom. Westin’s work and that of Daniel J. Solove, in “A Taxonomy of Privacy”—described in his book Understanding Privacy (Cambridge: Harvard University Press, 2008)—are the sources for the list of privacy harms described here.
© 2013 Merri Beth Lavagnino. The text of this article is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Unported License (http://creativecommons.org/licenses/by-nc-nd/3.0/).