



The Privacy and Security Policy Vacuum in Higher Education

By Fred H. Cate

Colleges and universities possess an exceptional volume and variety of personal information. Given this fact—along with their wide range of activities, the often decentralized nature of their operations, and their growing reliance on technologies that collect and centrally store data—these institutions face significant privacy and security challenges. Unfortunately, to date, most colleges and universities in the United States have failed to live up to these challenges. Their stewardship of personal, even sensitive, information is frequently governed by inconsistent and inadequate policies. Higher education institutions often implement new technologies and systems while paying little attention to privacy and security implications. They lag far behind industry in appointing privacy and security officers. Although colleges and universities accounted for more than one-third of the publicly reported information security breaches in 2005 and the first half of 2006, they provide scant training in privacy and security issues, especially outside of the technological arena, and rarely audit for compliance. Perhaps most important, colleges and universities have failed to exercise leadership in the expanding national debate about the appropriate protection for personal data and the proper limits of government access.

Fred H. Cate is Distinguished Professor and Director of the Center for Applied Cybersecurity Research at Indiana University and Senior Policy Advisor in the Center for Information Policy Leadership at Hunton & Williams.

Equally as important as the volume and sensitivity of this information is the fact that many institutional data systems overlap and the data interconnect.

To be sure, those of us in higher education face a dizzying array of demands for our attention and scarce resources. But industry and government face similar problems, and somehow they have responded to the growing concerns about privacy and security. Moreover, colleges and universities in Canada, the European Union, and elsewhere are dealing with privacy and security issues under national data-protection laws. Those of us in U.S. higher education can no longer ignore our privacy and security policy responsibilities, especially given the growing demands for the personal data we possess, the special nature of our mission, the relationships we have with our students and supporters, and the likelihood that our continued failure to voluntarily protect personal information will lead to more burdensome legal obligations.

The Volume and Variety of Personal Information

As noted, colleges and universities possess an enormous and growing volume and variety of information about students, employees, applicants, alumni, and their families. Consider just a sample of what campuses routinely collect and retain:

- Every indicator of students' academic lives, including applications, letters of reference, transcripts, grades, and records of disciplinary actions
- Extensive financial information about students and their parents, including financial aid applications, income tax returns, employment history, salary, work schedules, loans, bursar accounts, records of purchases charged to campus accounts, and insurance claims
- Health information that campus health centers, athletic programs, and campus-provided insurance services collect on students, employees, and their families
- Broad financial and other personal information about employees' payroll, insurance, benefits, retirement, research accounts, travel reimbursements, and vehicles

- Student, faculty, and staff e-mail (sent or received), centrally stored or accessed documents, backup files, Internet-browsing records, telecommunications and Internet use patterns, voicemail, and billing records
- Location information on students, faculty, and staff as they swipe parking passes and magnetic key cards (or use passwords or biometric identification devices) in their dorm rooms, dining rooms, and offices and as they log on to wireless Internet nodes
- Videotapes and files from the increasingly ubiquitous cameras installed in libraries, parking lots, office buildings, dorms, campus stores, cashier offices, athletics facilities, and hundreds of other locations on campus
- The titles of all books and articles checked out of the library, accessed via electronic reserves, bought at the campus bookstore, or paid for using institutional charge or debit cards
- Extensive financial and other data on alumni and donor prospects, including their assets, salaries, past gifts, employment records, achievements, family members, wills, and bequests
- Health, financial, and/or behavioral data on the patients treated at college/university hospitals, the clients served at student legal services and law school clinics, the subjects chosen for research studies, and the children cared for in campus day-care centers
- Data about vehicles that access and park on campus, even temporarily
- Data accessed from external sources for background checks, references, debt collection, litigation, and other uses (e.g., institutions are increasingly using sources like Facebook.com to monitor students' online activity)

These data concern not only students, alumni, and employees but also people less directly associated with the institution—people such as family members, donors, and others who take advantage of campus services, including hospitals, theaters, sporting events, and Web sites.

In addition, equally as important as the volume and sensitivity of this information is the fact that many institutional data systems overlap and the data interconnect. For example, the same swipe cards are used to check books out of the library, enter dorm rooms and offices, and charge purchases.¹ Such indiscriminate centralization and the fact that data are often subject to inconsistent policies not only make privacy and security easier to compromise but also increase the scope of the resulting injury.

The Pressure to Disclose

Colleges and universities also face growing pressure to use and share the information they hold. Among the sources of heightened pressure to provide data are the following:

- The U.S. Department of Homeland Security (DHS) requires the reporting of granular data on students and others, especially non-U.S. students and visitors, for national security reasons—for example, the Student and Exchange Visitor Information System (SEVIS).² The FBI has routine access to these data.³
- DHS, the Department of the Treasury, the Internal Revenue Service, and the Department of Labor require the reporting of data on employees' citizenship, work eligibility, salary and benefits, and withholding and on students' loan eligibility and repayment.
- The Department of Education (DOE) seeks increasingly detailed data on students for accountability and compliance programs. DOE's proposed "unit record" system would require colleges and universities to report, for each student enrolled, the following: Social Security number, name, birthday, race, gender, citizenship, courses completed, grades received, financial aid, tuition and fees paid, attendance record, degrees completed, and even participation in varsity sports. Although not yet adopted by Congress, the proposal was recently endorsed by

Most colleges and universities devote insufficient resources to assessing the risks to, and systematically protecting the privacy and ensuring the security of, personal information.

the National Commission on Accountability in Higher Education.⁴

- The Department of Defense collects information not only on students' draft registration status but also on their interests, grades, and likely value as military recruits.
- National and local law enforcement agencies, often without compliance with applicable laws, seek access to e-mail, Internet browsing records, and other information concerning students, faculty, and staff suspected of wrongdoing.⁵ The Federal Communications Commission has issued regulations requiring higher education institutions to install and maintain taps into their telecommunications and Internet systems to comply with the Communications Assistance for Law Enforcement Act (CALEA).⁶
- Attorneys and courts demand personal data for civil litigation, disciplinary proceedings, divorces, and other actions involving students, employees, donors, and their families.
- Legislators, the press, interest groups, aggrieved students and employees, and others seek records for myriad purposes, especially in public colleges and universities subject to open records laws.

Adding to these and other external pressures for access to personal information, colleges and universities face significant internal pressures for the increased collection, centralization, and use of personal information to generate revenue, control costs, and improve accountability. For example, many institutions have financial deals with credit card companies, student loan companies, travel and telecommunications providers, and other institutions that share revenue based on the business referred. These deals almost always involve the transfer of personal information both out of the institution (e.g., referring names for affinity credit cards) and back into the institution (e.g., calculating usage-based proceeds and auditing those calculations).

In addition, colleges and universities are deploying application-through-alumni lifecycle tracking of students and are implementing systems to integrate data about faculty, staff, and students. They are using new surveillance and identification technologies to prevent the theft of lab equipment, to ensure students' safety, and to stop students from sharing meal plans. And they are deploying plagiarism-detection programs that require students to submit their work electronically and then upload that work into national databases (often without the students' consent) and are monitoring students' access to school and Web resources.⁷

These and other data-based innovations have many positive aspects, but they raise critical privacy and security issues.

Higher Education Privacy and Security Policy Resources

As the range, volume, and accessibility of personal data held by colleges and universities expand, and as the demand for these data grows, are campus privacy and security policies and oversight mechanisms keeping up? The available evidence suggests that the answer is no: most colleges and universities devote insufficient resources to assessing the risks to, and systematically protecting the privacy and ensuring the security of, personal information.

To help determine the adequacy of their own institution's preparedness and response, college and university leaders might ask themselves the following questions:

- Does the institution have system-wide privacy policies that extend beyond medical centers and student records (where they are legally required)? Are the policies consistent across schools, units, campuses, technological media, and settings? Most institutions do not have such policies. In 2006, Bentley-Watchfire completed a study of the Web sites at the top 236 U.S. doctoral universities and liberal arts colleges as ranked in the 2004 *U.S. News & World Report* list of "best colleges." The

researchers found that 100 percent of the institutions had pages without a privacy notice, 100 percent had pages that were not secure and on which personal information was collected, and 99 percent had pages on which personal information from visitors was collected without providing a privacy notice.⁸

- Does the institution routinely consider the privacy and security implications before buying or deploying new systems? Does it have a policy requiring this consideration? Does it ever reject an otherwise feasible new technology or new system because of its privacy or security implications?
- Does the institution have a chief privacy officer (CPO) and a chief security officer (CSO), outside of medical centers (where these positions are legally required)? If so, do those officers have policymaking authority? Do they report to the governing board or chief executive officer? When the University of Pennsylvania appointed the academic community's first CPO (to my knowledge) in 2002, hundreds of companies already had CPOs in place.⁹ Today, the membership of the International Association of Privacy Professionals (IAPP) is around 2,300, of which only about 30 have any connection to a college or university.¹⁰
- Does the institution audit for compliance with privacy and security policies and procedures?
- Does the institution train its faculty and staff in privacy and security policies and procedures? Does it educate its students about these issues? Does it comment, directly or through higher education groups such as EDUCAUSE, on pending legislation and regulations affecting privacy and security within higher education?
- Has the institution suffered a major privacy or security incident within the past year? A majority of publicly reported information security breaches have involved colleges or universities.¹¹

Fair Information Practices

Less than one-third of America's leading colleges and universities have a privacy notice accessible from their home page, and . . . many of these notices fail to include the core elements of fair information practices. . . .

Fair information practices are procedures that provide individuals with control over the disclosure and subsequent use of their personal information. They balance the competing organizational and consumer interests around the use of the consumer's personal information and serve as the basis for privacy laws in the U.S. and elsewhere. . . .

Currently, the most widely accepted U.S. definition of fair information practices . . . is based on four elements: Notice, choice, access and security.

- **Notice** means that when individuals provide personal information, they have the right to know what, if any, information is being collected and how it will be used;
- **Choice** means that individuals should have the right to object when personal information is collected for one purpose and will be used for other unrelated purposes or shared with third parties, unless this sharing is required by law;
- **Access** means that individuals should have the right to see their information and correct errors; and
- **Security** means that organizations should be good stewards of personal information by ensuring data integrity and that data are secure from unauthorized access during both transmission and storage.

In addition, organizations should develop a reliable mechanism to ensure they abide by these principles.

Excerpted from Mary J. Culnan, Thomas J. Carlin, and Traci A. Logan, *Bentley-Watchfire Survey of Online Privacy Practices in Higher Education: Final Report* (April 1, 2006), <http://www.bentley.edu/news-events/pdf/Final_Report_040610.pdf>.

Surveys and anecdotal evidence suggest that colleges and universities lag far behind industry and government agencies in taking up these issues, even though higher education institutions tend to possess a greater volume and range of sensitive personal information.

Recommendations

Five steps can help colleges and universities turn this situation around and begin treating personal information more responsibly.

First, colleges and universities need to make an institutional commitment to taking privacy and security seriously. This requires more than adopting a simplistic, “yes-or-no” approach to collection and disclosure, and it certainly requires more than just papering the campus with privacy notices. It requires thinking broadly and sensitively about the wide range of privacy and security issues, including the need for the information, limitations on its use, minimization and retention policies, authorization requirements, and auditing. The goal is not just to address these issues but to do so systematically, consistently, and predictably.

Second, colleges and universities need to put in place practical tools to help achieve this goal and to ensure that protecting privacy is an integral consideration in all activities. One practical example is the privacy impact assessment (PIA) that federal agencies are required to perform before buying or implementing new data-based systems. A PIA requires proponents of new systems to articulate

- what information will be collected (e.g., nature and source);
- why the information will be collected (e.g., to determine eligibility);
- what the information will be used for;
- with whom the information will be shared;
- what opportunities individuals will have to decline to provide information or to consent to particular uses of the information, and how individuals will be able to grant consent;
- how the information will be secured (e.g., administrative and technological controls); and
- what risks the data will present.¹²

Government privacy officers have found that PIAs, when taken seriously, are useful in anticipating privacy and security risks from the start. PIAs not only help provoke useful dialogue about privacy and security issues but also serve to dampen the gee-whiz mentality that can lead to pursuing new technologies without adequate forethought and planning.¹³ Colleges and universities should consider instituting a similar requirement. If instituted in higher education, PIAs could help colleges and universities accomplish individually the important mission that EDUCAUSE promotes collaboratively: “to advance higher education by promoting the intelligent use of information technology” (<http://www.educause.edu>).

Third, colleges and universities need to collect, use, share, and retain personal data only with a clear purpose and only subject to consistent or uniform institutional policies. Higher education institutions have long operated under a laissez-faire approach to data collection and retention. Each

unit tends to collect and store whatever data it wants, whatever data it can, and/or whatever data it finds itself stuck with because deciding which data to discard—subject to inconsistent policies or, more commonly, no policies at all—is too expensive or time-consuming. Colleges and universities must move to more of a “need-to-have, need-to-know, need-to-share, need-to-retain” system. This not only will help protect privacy and ensure security but also will likely improve the quality of the data generated and the efficiency with which the data are managed. It also will provide those of us in higher education with an effective response to government and industry demands for campus personal information: if we do not have it, we cannot share it.

Fourth, all colleges and universities need to designate CPOs and CSOs with appropriate staffing and resources, policy-level responsibilities, and direct reporting lines to governing boards and presidents. At Indiana University, information security improved

The public holds colleges and universities to a higher standard and expects them to behave more responsibly and more transparently than businesses or government agencies.

considerably when Chief Information Officer (now Interim Provost) Michael McRobbie was given a direct reporting line to the board of trustees. Such an approach is essential to higher education leaders' ability to execute their fiduciary duties. Moreover, giving CPOs and CSOs policy-level responsibilities and high-level reporting lines recognizes that these jobs are only partly regulatory or compliance-oriented in nature. The primary function of these jobs is to prompt people throughout the institution to think intelligently about privacy and security issues and to provide them with the education and resources to do so. The high-level placement of CPOs and CSOs also enhances their ability to help the institution play a leadership role in addressing privacy and security issues outside of the institution—for example, in Congress and in state legislatures.

Finally, colleges and universities need to exercise leadership in the national debate over government and industry access to personal data. Figuring out the rules for who should be able to obtain access to which information and for what uses is a difficult and important task. Those of us in higher education are well positioned to help legislatures and policymakers make wise rules and decisions and to require that entities desiring access to our data comply with those rules. If we do not stand up for our students, employees, alumni, and donors, who will?

Conclusion

Colleges and universities face heightened responsibilities. They possess a large volume and variety of sensitive information on a wide range of individuals, and demands for this information are growing. The students that are educated,

housed, and/or employed by colleges and universities tend to be in a vulnerable age cohort: eighteen- to twenty-nine-year-olds are the most likely segment of the population to be victimized by identity theft—three times more likely than senior adults.¹⁴ Colleges and universities also have unique responsibilities to parents and to donors, for whom these institutions act as trustees not only of their money but also of their personal data. Moreover, in part because of these special considerations, the public holds colleges and universities to a higher standard and expects them to behave more responsibly and more transparently than businesses or government agencies.

In view of these increased expectations and responsibilities, higher education institutions need to take the five steps outlined above. These steps can help campuses guard against the practi-

cal, financial, legal, and reputational risks of not treating privacy and security seriously. In short, by taking these five steps and implementing a policy-level approach to privacy and security, an institution is acting in its own self-interest.

Campuses are already subject to a broad array of privacy and security laws and regulations. Student records are subject to the Family Educational Rights and Privacy Act (FERPA).¹⁵ Health-related activities are subject to regulations under the Health Insurance Portability and Accountability Act (HIPAA).¹⁶ The security of many institutional financial records is subject to the Federal Trade Commission (FTC) Safeguards Rule.¹⁷ E-mail marketing practices are subject to the CAN-SPAM Act,¹⁸ and telephone marketing is subject to federal and state do-not-call laws.¹⁹ Finally, those colleges and universities in the thirty-three states with security breach notification laws are subject to those laws for improperly accessed personal data.²⁰ Although ensuring compliance with these and myriad other state

and federal enactments concerning privacy and security may ultimately be the responsibility of the campus counsel's office, bringing consistency to practices in the face of such disparate requirements requires a system-wide educational and policy-level approach to privacy and security. Moreover, recent breach notification and Social Security number disclosure laws impose very tight notification deadlines and therefore require extensive internal reporting and response systems that many in-house counsel's offices may not be staffed to provide. In the absence of such a broad-based approach, colleges and universities run the serious risk of failing to comply with their legal obligations as personal data move across the many campus operations or are combined in data warehouses, and they run the risk of overwhelming or misapplying scarce counsel's office resources. Colleges and universities thus need to build appropriate infrastructures that include heightened awareness to privacy and security issues throughout the institution.

Doing so is in an institution's self-interest for a second reason as well. Despite the broad range of privacy and security laws and regulations to which colleges and universities are already subject, the higher education community has mostly avoided especially onerous regulatory obligations. To date, the burdens faced by those of us in higher education have been, on the whole, modest when compared with the federal and state privacy and security regulations, security statutes, enforcement actions, and tort lawsuits emerging in other sectors. Legislators, regulators, state attorneys general, and private litigators have not yet gotten around to us as they work their way through other information-intensive enterprises. But our days out of the spotlight are numbered. In fact, they may already be ending. And if we do not figure out how to behave responsibly toward personal data, and how to demonstrate that fact convincingly and publicly, the government is likely to do the job for us. *e*

Notes

I am grateful for the helpful suggestions of Beth Cate and Lauren Steinfeld.

1. Avi Salzman, "On Campus, a Security Card and More," *New York Times*, October 5, 2003.
2. See "SEVIS Database Tracks Every Move of Foreign Students, Visitors," *EPIC Spotlight on Surveillance* (September 2005), <<http://www.epic.org/privacy/surveillance/spotlight/0905/>>. When SEVIS was hacked at the University of Nevada at Las Vegas in 2005, records on 5,000 current and former international students and scholars were accessed (Sara Lipka, "Hacker Breaks into Database for Tracking International Students," *Chronicle of Higher Education*, April 1, 2005). In its first year of operation, SEVIS detected more than 36,000 potential visa violations, of which only 1,600 were investigated by the government, leading to 155 arrests (Brad Heath, "Students Slip Past Visa Check," *Detroit News*, September 19, 2005).
3. Kelly Field, "FBI Gets Access to Student Databases," *Chronicle of Higher Education*, September 24, 2004.
4. Miles Benson, "Student Information Bank Considered," *New Orleans Times-Picayune*, March 31, 2005; "Come Here Often?" *Baltimore Sun*, December 6, 2004.
5. The U.S. attorney in Iowa used a subpoena, issued under a gag order, to seek information from Drake University about the participants in an antiwar conference organized by the National Lawyers Guild. Apparently in response to protests, the U.S. attorney withdrew the subpoena. See Sharon Walsh, "Government Withdraws Subpoena for Records of Antiwar Meeting at Drake U.," *Chronicle of Higher Education*, February 20, 2004.
6. See Andrea L. Foster, "FCC Brief on Electronic Surveillance Calms Colleges' Fears about Costs," *Chronicle of Higher Education*, March 10, 2006.
7. See, for example, Jim Buckell: "Ethical Query in Online Check," *The Australian*, October 22, 2003; and "Plagiarism Programs Hit Glitch," *The Australian*, October 15, 2003.
8. Mary J. Culnan, Thomas J. Carlin, and Traci A. Logan, *Bentley-Watchfire Survey of Online Privacy Practices in Higher Education: Final Report* (April 1, 2006), <http://www.bentley.edu/news-events/pdf/Final_Report_040610.pdf>.
9. Lauren Steinfeld was appointed Chief Privacy Officer at the University of Pennsylvania in January 2002 (*University of Pennsylvania Almanac*, February 26, 2002, <<http://www.upenn.edu/almanac/v48/n24/Steinfeld.html>>).
10. Communication from Trevor Hughes, executive director of the International Association of Privacy Professionals, to the author, April 27, 2006.
11. See "A Chronology of Data Breaches Reported since the ChoicePoint Incident," updated July 17, 2006, <<http://www.privacyrights.org/ar/ChronDataBreaches.htm>>.
12. E-Government Act of 2002, Pub. L. No. 107-347, § 208.
13. Institutions that have installed biometric identification systems have discovered the need to maintain redundant swipe or password systems to deal with anomalies such as "weak fingerprints," hand sanitizers, and every-fifteen-minutes cleaning of sensors (to deal with the problem of disease transmission). See Vincent Kiernan, "Show Your Hand, Not Your ID," *Chronicle of Higher Education*, December 2, 2005.
14. Identity Theft Data Clearinghouse, "Identity Theft Complaints by Victim Age, January 1–December 31, 2005," *Consumer Fraud and Identity Theft Complaint Data* (Federal Trade Commission, January 2006), <<http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf>>.
15. 20 U.S.C. § 1232g.
16. Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 43,181 (2002) (HHS, final rule) (codified at 45 C.F.R. pt. 160, §§ 164.502, 164.506); Health Insurance Reform: Security Standards, 68 Fed. Reg. 8,333 (2003) (HHS, final rule) (codified at 45 C.F.R. pts. 160, 162, 164).
17. Standards for Safeguarding Customer Information, 67 Fed. Reg. 36,483 (2002) (FTC, final rule) (codified at 16 C.F.R. § 314).
18. Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (codified at 15 U.S.C. §§ 7703-13).
19. The following states have do-not-call laws: Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Kansas, Kentucky, Louisiana, Maine, Massachusetts, Michigan, Minnesota, Missouri, Nebraska, New York, North Carolina, Oklahoma, Oregon, Pennsylvania, Tennessee, Texas, Vermont, Virginia, Wisconsin, and Wyoming.
20. Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Kansas, Louisiana, Maine, Minnesota, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New York, North Carolina, North Dakota, Ohio, Oklahoma, Pennsylvania, Rhode Island, Tennessee, Texas, Utah, Washington, and Wisconsin.