Why IT Matters to Higher Education

EDUCAUSE REVIEW
JANUARY/FEBRUARY 2013

Information Privacy Revealed

Merri Beth Lavagnino

Privacy, Security, and Compliance
Michael Corn and Jane Rosenthal

Mentoring, Self-Awareness, and Collaboration
Melissa Woo, David G. Swartz, and Earving L. Blythe

PLUS
EDUCAUSE Values: Community
activate learning.

An integrated collection of classroom furniture, Verb™ is designed to support a full range of teaching and learning styles on demand.

www.steelcase.com/Verb
4 EDUCAUSE Values: Community

FEATURES

10 Information Privacy Revealed
Merri Beth Lavagnino

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.

24 Privacy, Security, and Compliance: Strange Bedfellows or a Marriage Made in Heaven?
Michael Corn and Jane Rosenthal

The authors examine several campus issues lying at the intersection of privacy, security, and compliance and provide insight for institutional leaders planning strategic directions.

36 Mentoring, Self-Awareness, and Collaboration: The 2012 EDUCAUSE Award Winners
Melissa Woo, David G. Swartz, and Earving L. Blythe

The 2012 EDUCAUSE Award winners talk about the higher education IT profession and about how their particular interests have influenced and guided their leadership roles.

48 Analytics: Changing the Conversation
Diana G. Oblinger

The third in a three-article EDUCAUSE Review series exploring analytics.
8 Leadership

[Views from the Top]
Helping to Take the Disruptive out of MOOCs
Michael Reilly and Jeffrey von Munkwitz-Smith

52 E-Content

[All Things Digital]
Is Linking Thinking? Addressing and Assessing Scholarship in a Digital Era
Michael Roy

54 New Horizons

[The Technologies Ahead]
ds106: Not a Course, Not Like Any MOOC
Alan Levine

56 Policy Matters

[Campus Environment & Political Context]
Amassing Student Data and Dissipating Privacy Rights
Marc Rotenberg and Khaliah Barnes

58 Viewpoints

[Today’s Hot Topics]
MOOCs: Get in the Game
Brian D. Voss
Old cars are classics. Old SIS are obsolete.

If your SIS vendor built its system before the Internet, it’s not vintage — it’s a liability. With the right innovations for higher education engineered into CampusVue® Student, institutions are winning the hearts and minds of constituents on a more efficient centralized system. So, before overhauling your old system again, test drive the most proven brand in the industry. Experience the Student Information System that’s serving leaders in higher education worldwide.

www.campusmanagement.com/vue
The values of the higher education IT community shape the strategic directions and actions of EDUCAUSE. In consultation with EDUCAUSE members and community leaders, the EDUCAUSE executive staff continues to develop a series of value statements. Each statement will provide a brief overview of what the value means, why our community considers it to be important, and how the value guides EDUCAUSE in its service to association members and to higher education. The list of values, which will change over time and should not be considered exhaustive, is posted on the EDUCAUSE website: http://www.educause.edu/stratdir#values.

“EDUCAUSE values community for the relationships, commitment, and collective action it catalyzes, and EDUCAUSE thus supports the development and adoption of technologies, applications, and approaches to foster community.”

A community is “a group or society, helping each other.” A strong community nurtures the development of relationships and fosters mutual commitment, respect, responsibility, understanding, and participation among its members.

The college/university is the very essence of community—a place where people gather together to explore ideas and to expand the boundaries of knowledge. The community acts as a springboard to discovery, encouraging individuals to expand their worldviews and remain open to a wide range of ideas and possibilities. EDUCAUSE values this type of community.

Technological innovations, however, have created, changed, and in some cases, challenged our notions of community. Anyone and anything can be connected. Communities can appear and disappear spontaneously or can be long-lived. Technology enables the formation of
Thousands of students plus an entire faculty equals a whole lot of data. Certainly more information than one IT person can handle. That’s why we’ve partnered with Riverbed to provide you the extra power you need. Our solution architects will make sure you find the right technology for your data center.

The extra bandwidth you need is at CDWG.com/datacenter
communities of any size, on topics general or specialized, and without limitations of geography or time. Wikipedia, Facebook, and Twitter, for example, have catalyzed communities never before imagined. Technology-enabled communities can be social, scientific, political, or about collective action. They can have great power.

EDUCAUSE too is a community, comprising institutions and individuals who are committed to the free flow of information and ideas through the use of technology. EDUCAUSE manifests the value of community in the ways it promotes the association’s other values: innovation, openness, collaboration, and working toward the common good. Interaction among the members of our community opens us up to the experiences of others, gives us an awareness, deeper understanding, and appreciation for the common challenges faced at institutions large and small, and helps bring into focus possible approaches and solutions.

The EDUCAUSE community is not limited to IT practitioners. Our community is enriched by connections with international colleagues, the broader world of higher education, and corporate and government organizations. As expressed in our motto—“uncommon thinking for the common good”—our community values opportunities to consider a diversity of perspectives, to think imaginatively, and to embrace innovation. EDUCAUSE cultivates strategic relationships with other professional associations to enhance our community’s work.

EDUCAUSE strives to foster a community of higher education IT professionals who can engage with colleagues, contribute their expertise, and grow in the profession. Our members can find others with similar interests and can follow, share, and expand professional networks through social media. The ability to share lessons learned and leverage effective practices allows the entire community to progress more rapidly.

As the higher education technology association, EDUCAUSE embraces the values of collaboration, the common good, innovation, openness, and community. A spirit of community is central to EDUCAUSE and our service to higher education.

You walked across campus on the coldest day in January to make sure Ashley’s financial aid form made it to the Registrar’s Office by the 10:00 a.m. deadline. But when her mom called later with a question, you didn’t have the answer because Ashley’s form is across campus … and you’re not.

It’s time to rewrite this story.
Perceptive Software process and content management solutions close information gaps and eliminate workflow bottlenecks in every department, to make staff and students’ lives easier. No matter what host application you use or how your staff interacts with data, Perceptive gives you more choices and greater flexibility – end of story.

Read success stories from real customers at www.perceptivesoftware.com/highered
From serving as a trusted liaison with your preferred Epson dealer to providing product demos, training, and answers to your planning and technical questions, the Epson team will come to your campus to help you take full advantage of our exclusive Brighter Futures education programs and pricing.

We’re a whole team of professionals focused on creating great relationships with the higher education community.

Epson Has a Team on Campus.
Visit epson.com/higherEd

Thomas Hines
Austin, TX

Kristan Kuykendall
Lakewood, CA

Gerry Campana
Ellicott City, MD

Barry Sugarman
Weston, FL

PowerLite® Pro Z Large Venue Installation Projectors
Offering low cost of ownership and liquid cooling technology, all Pro Z projectors also feature dual lamps that are ideal for use in large auditoriums and performance venues.
Helping to Take the Disruptive out of MOOCs

Those of us who have found our way into the enrollment and academic services professions in higher education have become accustomed to the somewhat familiar refrain that colleges and universities are slow to change. The recent attention given to MOOCs (Massive Open Online Courses) has often included the descriptor “disruptive” (meaning: “to throw into confusion or disorder”) partly because this characterization of resistance to change suggests that higher education institutions could not possibly address this phenomenon in an orderly fashion.

We—the authors of this article—think that change, particularly change around the technology that makes it easier for students to enroll and complete their degrees and that helps faculty focus their time and energy on their teaching and research, is instead part of the fabric of higher education and is actually more characteristic of our profession than is any notion of our resistance to change. We have both been in higher education for long enough to have witnessed change that would make our offices and processes unrecognizable to those who were in the business twenty years ago. We believe that the same measured approach that we have taken to apply emerging technologies to current business processes in order to make them more student-centered can be used to navigate the MOOC phenomenon in order to make it more “productive” than “disruptive.”

To understand higher education’s ability to “roll with the changes” from the academic and enrollment services perspective, think of how students applied for admission or registered for classes, or how faculty submitted grades or advised their students, thirty years ago. Applying to college involved completing a paper application and tracking down transcripts to mail to the admissions office. A bank of staff hand-keyed these applications and records into the “system” (usually a legacy system built on COBOL code). Registering for classes was a massive manual exercise involving 80-column punch cards, paper forms, and miles logged walking around campus tracking down signatures. Faculty advised students by comparing transcripts against the degree requirements in the institution catalog. Grades were rushed to the Registrar’s Office at the end of each term and were hand-keyed into the system so that grade reports could be mailed to students.

Today, web-based services have made nearly all academic and enrollment processes available to students and faculty through their computers and, increasingly, through mobile applications on their phones. The vast majority of students apply for admission through a web-based application (many institutions accept only electronic applications). Transcripts can be requested via a website and delivered electronically to the college or university of choice. Transcripts can be uploaded into a degree audit system that shows a student’s progress toward degree requirements and is updated each term. These degree audits allow faculty advisors to spend more time talking with students about research interests or career plans and less time making sure students’ course choices are meeting degree requirements. Students register for classes, pay their bills, order their textbooks, request transcripts, change their major, and handle many other processes via the web.

The embracing of emerging technologies has made many of these improvements in student services possible. Verification of enrollment for financial aid purposes is now easily done through the National Student Clearinghouse. Document imaging has made it easier to share records with faculty and to store records in digital files rather than in the bulging file cabinets that cluttered offices. Most students get their questions answered or their needs met through websites, allowing institutions to close the banks of windows that often characterized student services offices. Many students attend institutions only through web-based instruction and never even see the inside of campus offices.

So what does AACRAO and what do academic and enrollment service professionals have to contribute to the discussion of MOOCs? Academic leaders at our institutions are already beginning work to address student assessment and learning outcomes issues. The areas where AACRAO members have expertise are in ensuring identity management, in transcripting, and in recording and verifying credentials. A degree from an accredited institution of higher education in the United States has substantial value in part because rigorous quality controls have been applied to the process of obtaining that degree. These include not only institutional and program
accreditation, faculty credentials, and other academic quality metrics but also procedures ensuring that an applicant's academic preparation for study has been thoroughly evaluated, that prior credit applied to the degree was earned at legitimate institutions, that transcripts reflect the achievement earned by the student in the course and assessed by faculty, that a prescribed course of study was completed, that the record is stored in a secured environment, and that student privacy is protected. Call us old-fashioned, but we think these sets of quality assurances have served U.S. higher education well.

MOOCs create challenges to this quality-assurance regimen—challenges that will require some thought. How do we know who is taking a course when the course is “open” to anyone who wants to take it? Does this matter only if someone is interested in earning course credit to apply toward a degree or credential? Promising technologies are emerging in identity management, including through Internet2 and the Common Identity and Trust Collaborative (CommIT), which present some opportunities for better authentication of the participants. A variety of strategies is available for transcripting or awarding credit for MOOC courses. The American Council of Education (ACE) and others are beginning work in this area.

At the AACRAO annual meeting in San Francisco in April 2013, we are planning to hold a robust discussion of the role of enrollment and academic services in contributing to the success of MOOCs. We anticipate that our members and partners will have a number of creative ideas to offer. Hopefully we can one day look back to the beginnings of the MOOC phenomenon as just another of the many challenges we have tackled as part of the ever-evolving enterprise known as higher education.

Michael Reilly (reillym@aacrao.org) is Executive Director for the American Association of Collegiate Registrars and Admissions Officers (AACRAO). Jeffrey von Munkwitz-Smith (jvon@bu.edu) is President of the American Association of Collegiate Registrars and Admissions Officers (AACRAO) and is Assistant Vice-President and University Registrar at Boston University.

© 2013 Michael Reilly and Jeffrey von Munkwitz-Smith. The text of this article is licensed under the Creative Commons Attribution 3.0 Unported License (http://creativecommons.org/licenses/by/3.0/).
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.”

By Merri Beth Lavagnino
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 workspaces 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 technol-
The Enterprise Cloud for HR and Finance

Intuitive, insightful, and innovative, Workday provides best-in-class applications for higher education institutions.

Workday customers:
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. By 1973, e-mail constituted 75 percent of ARPANET traffic.

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. 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
Overseeing district purchasing requires a lot of effort and planning. The Cooperative Purchasing Network (TCPN) helps simplify your steps and reduce your costs. TCPN’s contracts leverage the purchasing power of over 30,000 actively engaged government entities. All contracts are competitively bid and awarded by a single governmental entity – Region 4 Education Service Center. An industry giant with ISO certified processes; TCPN monitors contracts through third-party audits and regular reviews to ensure vendor accountability. You can rely on TCPN’s 100+ combined years of government purchasing experience and 50+ combined years of auditing experience – we know what it takes to keep a school running.

Keep your school purchasing on time, and on budget. Go to www.tcpn.org and sign up today.
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 (wiretapping 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
Mediasite gives us a more global reach, sharing our courses locally, nationally and internationally.

It’s invaluable for our distance learning and part-time students, who can now enjoy the experience of a more traditional face-to-face lecture. Plus working with Sonic Foundry, the best global practitioners of lecture capture technology, we’ve been able to learn from both the company and their global user community, which means we don’t have to reinvent the wheel.

Sean Faughnan
Deputy Director, Department for Continuing Education
Oxford University

Learn more about Oxford’s Mediasite success
Sonicfoundry.com/OxfordUniversity
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.
AN OPEN LETTER TO APOGEE
RE: MOVE-IN

We are nearing the end of move-in week for our freshmen class and it couldn’t have gone smoother.

Typically at this time of year, our network and help desk teams are scurrying in and out of dorms troubleshooting network connectivity for our students. With Apogee now in place, those calls for help have simply stopped, allowing HSU personnel to focus on the multitude of other tasks necessary to begin the academic year. Even better than that, our students absolutely love the new wireless connectivity and the ability to choose the service plan that best meets their needs.

While Apogee’s customer support has been outstanding, I think it is important to note that move-in week has been so successful in large part because of the meticulous project organization that we have experienced from the very start. Throughout the entire process, Apogee made us feel comfortable because it was clear they had walked this road before and were on point. From the initial discovery, to the network engineering, to the installation, this project has run beautifully. Each Apogee representative that has been on our campus was respectful, competent, and efficient. Move-in week has been wonderful, but the foundation that was laid throughout the preceding five month should not be ignored.

From top to bottom, you have an organization of which you can be proud. We look forward to many years of successful partnership with Apogee.

- TRAVIS P. SEEKINS
ASSOCIATE VICE PRESIDENT FOR TECHNOLOGY SERVICES
HARDIN-SIMMONS UNIVERSITY
Notes

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.
10. The speech, an address to the Academy of Political Science on April 11, 1911 at the Metropolitan Opera House in New York, was published as: George Bernard Shaw, “The Future of Political Science in America,” *Political Quarterly*, vol. 4 (July–September 1913), pp. 313–340.
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/he-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.
22. 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.
24. 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/).
Pushback has always been the great destroyer of initiatives to institute enterprise-wide automation of administrative processes—until now.

Find out how colleges and universities like The Texas A&M University System are achieving the seemingly impossible: enterprise-wide automation initiatives that departments and business units are racing to embrace.

laserfiche.com/tamu
Where does privacy belong in the college/university ecosystem, and what should its relationship be with security and compliance? Are the three areas best kept separate and distinct? Should there be some overlap? Or would a single office, officer, and/or reporting line enable a big picture of the whole? This article examines several of the campus issues lying at the intersection of privacy, security, and compliance and provides some insight for institutional leaders as they plan strategic directions.
Privacy, Security, and Compliance: Strange Bedfellows or a Marriage Made in Heaven?

There are probably as many organizational variations to the areas of privacy, security, and compliance as there are organizations. The authors’ home institutions (the Universities of Kansas and Illinois) exemplify this. The University of Kansas positioned the privacy officer within a compliance office answering to the provost’s office, with IT security included in the information technology structure through another reporting line to the provost.2 The University of Illinois has combined privacy and security under the CIO on the information technology side of the house. Both institutions have considerable compliance activity vested within and outside of their respective areas.

Not surprisingly, there is not a common organizational design for these functions across higher education. Privacy as an institutional concern is relatively new within colleges and universities, and even though security and compliance are arguably older, the rapid transformation that technology has wrought on information ecosystems has imposed a similarly aggressive evolution in these two areas.

The recognition of privacy as a distinct field in the United States began around the year 2000, with the founding of the International Association of Privacy Professionals, or IAPP (https://www.privacyassociation.org/). In just over a decade, the IAPP has increased in size to more than 9,000 members in some 70 countries worldwide and now has certifications across jurisdictions (the United States, Canada, Europe), as well as across areas of expertise (government, corporate, information technology).3 Security

How is the privacy office function shaped by the legal office, or in a reporting structure

Privacy (noun)

1 a: the quality or state of being apart from company or observation: seclusion
b: freedom from unauthorized intrusion <one’s right to privacy>

Security (noun)

1: the quality or state of being secure: as
a: freedom from danger: safety
b: freedom from fear or anxiety
c: freedom from the prospect of being laid off <job security>
2 a: something given, deposited, or pledged to make certain the fulfillment of an obligation

Compliance (noun)

1 a: the act or process of complying to a desire, demand, proposal, or regimen or to coercion
b: conformity in fulfilling official requirements
2: a disposition to yield to others

compromise of personal data by the organization or its service providers.

- Serves as the organizational point of contact for individuals, internally and externally, who have questions about privacy policies and practices.9

Further, “privacy is essential to establishing and maintaining trust. If customers, clients, or employees believe that their personal information will be handled respectfully, in an open and transparent manner, with strong, reasonable safeguards, and made accessible to them at their request, this fosters trust and a continued positive relationship can be expected. If customers are typically considered a business’ greatest asset, then their personal information must be considered one as well. Organizations will want to build and protect their assets, and personal information, as an asset, is no different. An accountable organization can demonstrate to customers, employees, shareholders, regulators, and competitors that it values privacy, not only for compliance reasons, but also because privacy makes good business sense.”9

Privacy as a Security or Compliance Function

Increasingly, privacy officers today hold a law degree (JD) and thus are able to understand and apply the patchwork of laws and regulations to information management. Privacy officers are champions for the protection of individual privacy; they act as advocates for the inclusion of privacy as a critical facet when designing and advising on digital identity within the campus ecosystem. Other privacy professionals view their position as one of regulatory compliance, strongly defining the contours of the privacy domain.6

Additional data provided by the IAPP confirms that regulatory compliance is a dominant driver in organizations that are increasingly funding a privacy role within an institution. A close second is the organizational effort to avoid data breach and the expensive and time-driven notification process of the affected individuals and government oversight agencies. On the other hand, it is easy to see these two drivers as variations of one another.7

How is the privacy office function shaped by the decision to place it in the compliance office, in the legal office, or in a reporting structure combined with information security? There are many able and enthusiastic advocates for placing personal privacy in both the compliance and the legal offices of higher education institutions, yet it is easy to imagine this having a limiting (or chilling) effect on the scope of the privacy function. This is particularly true within U.S. institutions, since the United States lacks a mature, contemporary regulatory framework for privacy and since the legal structure is long engrained in the organization. Ensuring compliance within the patchwork of federal, state, and accompanying regulations or standards pertaining to security benefits the individual. Nevertheless, based on the IAPP 2012 survey, the role of the privacy officer has increasingly moved toward avoiding liability, rather than focusing on the individual or on the larger community desires.

IP Address Tracking and Web Browsing

As techniques for monitoring networks, workstations, and campus activities have become more sophisticated, the quandary of the privacy/security/compliance position requires reassessment. In one simple example, over the last six years at the University of Illinois, we have observed that malware has shifted from relying on e-mail as the dominant method of distribution to utilizing web-based attacks. Users are often innocent victims: they are not clicking foolishly on e-mailed phishing links but, rather, are clicking on ads or links on major news and sporting outlets that have been compromised. To better forensically understand these attacks, we increasingly collect—either from intrusion-detection systems or system-management agents—the web-browsing history of our users. Obviously, this information is treated with the utmost confidence and security. Only authorized staff who are researching specific incidents may access it. Nevertheless, the reality is that such information can lead to the feeling that both institutional privacy and personal privacy have been breached. This is true even in the context of policies stating that campus equipment and services are involved and that no privacy is guaranteed when working to maintain the overall system security. Yet for example, the data gathered and accessed may reveal the ratio of visits to Democratic or Republican websites from an administrative building or may reveal which personnel are visiting sites indicative of certain medical conditions or sexual orientation—data that most would agree is universally private or personal information.

As our work and our lives are thoroughly mediated by technology, the
invisible breach of this personal space, albeit done with good intentions, must raise concerns. The security professional might rightfully argue that this information is increasingly essential to fulfilling professional responsibilities. Although academia frowns on the idea of intruding into personal space and filtering or collecting information from these resources, in the security environment the methods may be necessary to gather information to fend off current and future attack vectors. The compliance officer might well acknowledge that these resources are legal and even necessary to maintain the requirements for an institution. Only the privacy officer, in his or her role as advocate, might actively challenge the use of these tools as being too invasive to personal freedoms and might recognize the risk to the level of trust or transparency that the institution provides to the community. Does this conflict of interest or duality of roles prevent someone who is vested with the role of privacy and security or the role of privacy and compliance from succeeding in this role?

Mobile Device/Application Management Technologies
Although the world of laptops has long challenged higher education institutions, that challenge has migrated to smaller mobile devices with greater computing power. There is exponential growth in these devices with the Android, Symbian, Windows, and other operating systems prevalent on smart phones and tablets. Colleges and universities face the challenge of containing and retaining information within their sphere of control while employees clamor for their own device of choice—known as “BYOD” or the “consumerization of devices.”

Mobile device management (MDM) and mobile application management (MAM) technologies entered the playing field as another compliance solution to reduce the inevitable data and device loss. These program consoles or applications provide the institution with a picture into the life of the device owner/user, with access to review the location of the device (or the holder), the application inventory (e.g., Mobile Application Inventory from MobileIron, http://www.mobileiron.com/), and restrictions on travel (e.g., Geo-Fencing from Zenprise, http://www.zenprise.com) and content (e.g., Mobile Content Management from AirWatch, http://www.air-watch.com/). The issue becomes the necessity of the institution to employ reasonable and available tools to track not only the devices but also the device applications that are plac-
MDM technologies can literally view every application on an enrolled device and wipe (“brick”) the device if it is reported missing by the owner or the assigned guardian of the device. MAM technologies are not device-centric but are based on a restriction of applications for the security of institutional data on a mobile device. How does an institution balance the privacy right of the individual against the use of such invasive tools, especially if the privacy and security officers are housed in the same office or represented by the same person? Yet, the privacy and security personnel must maintain a functioning, working relationship and must not work independently in separate, segmented silos.

Security Cameras and Video Technologies
No other surveillance technology suggests “big brother” with as much immediacy as do security cameras. Yet in response to a growing demand for greater physical security on campuses, security camera usage is expanding significantly. At the University of Illinois–Urbana campus, the number of security cameras has grown from zero to nearly 1,000 in a period of 18 months. Similarly the University of Kansas campus has hundreds of cameras, inside and outside, to enhance the security of students and staff. To address privacy concerns, the University of Illinois–Urbana security camera policy was written with a number of common prohibitions on camera use and location. Three of these are paraphrased as follows:

- All locations with security cameras will have signs displayed that provide reasonable notification of the presence of security cameras.
- Security cameras may not be used in private areas, which include residence hall rooms, bathrooms, shower areas,
Privacy, Security, and Compliance: Strange Bedfellows or a Marriage Made in Heaven?

locker and changing rooms, areas where a reasonable person might change clothes, and private offices. Additionally rooms for medical, physical, or mental therapy or treatment are private. Where security cameras are permitted in private areas, they will to the maximum extent possible be used narrowly to protect money, real or personal property, documents, supplies, equipment, or pharmaceuticals from theft, destruction, or tampering.

Security camera recordings may not be used in the course of personnel investigations such as those related to (but not limited to) workplace attendance or work quality.

These typical controls are found in many such policies and are similar to those found at the University of Kansas. First, individuals want to know when they are being monitored, thus the notification provision. Covert activity not only makes people uncomfortable; it may also create a feeling that they are being treated like children or criminals. Second, people have a culturally innate sense of a “personal” or private space that should not normally be breached. Still, is the “right to be left alone” the prevailing concern? Privacy is not specifically provided in the U.S. Constitution or in any of the subsequent 27 amendments. Justices Samuel Warren and Louis Brandeis discussed the definition and common law that created the right to privacy in their 1890 Harvard Law Review article: this and the subsequent case law provide the legal basis for our concept of privacy today.

Finally, although many employees understand that the workplace and the equipment are provided by their employer, the work environment is nevertheless, for many
EDUCAUSE thanks our 2013 Corporate Partners for their continued support!

**PLATINUM PARTNERS**

CDW Government
Dell
Desire2Learn Incorporated
Ellucian
Gartner
Jenzabar
Pearson
Sonic Foundry
VeriSign

**GOLD PARTNERS**

Blackboard
Campus Management Corporation
Cengage Learning
Cisco Systems
Epson
HP
McGraw-Hill Education
Microsoft Corporation
Moodlerooms
Steelcase

**SILVER PARTNERS**

Aruba Networks
Echo360
Extron Electronics
Google
Higher One
Hobsons
IBM Corporation
Laserfiche
lynda.com
Oracle Corporation
Perceptive Software
VMware
Workday

**BRONZE PARTNERS**

AirWatch
AT&T
Big Bang
Cloudpath Networks
Computer Comfrorts
ConnectEDU
CourseSmart
Dean Evans and Associates
EMC Corporation
Enterasys Networks
Four Winds Interactive
Giftus Education Group
GovConnection
Hyland Software
Instructure
Jadu
Kivuto Solutions
Lenovo
Longsight
LoudCloud Systems
NEC
NetApp
Panasonic
TouchNet Information Systems
Turning Technologies
Vidyo

These are just some of the benefits our Corporate Partners help make a reality all year long.

To learn more, visit.educause.edu/Corporate-Partners.
employees, a kind of extension of personal space. Monitoring that space is seen as evidence of mistrust.

There is an intimacy associated with physical observation; as social creatures, we vary our behavior (and its expression through language) according to social context. Cameras create a kind of ambiguous social context and, thus, discomfort; but cameras may also provide people with a false sense of security that they are being protected by monitoring—which may or may not be occurring on a 24/7 basis. Several questions then arise: What security and privacy structure allows an institution to benefit from the very real physical safety that security cameras may provide, without creating an uncomfortable or even Orwellian environment? Further, what should the institution do with the information recorded, as far as storage, sharing, secondary use, and disposition? Finally, do these records then become subject to view by public colleges and universities with open-records requirements?

Privacy and Organizational Structure
All higher education institutions face similar or even identical challenges, yet how colleges and universities are organized strongly reflects a type of institutional character. A strategy that works at Illinois or Kansas may fail spectacularly at another campus, due to differences in expertise, personalities, or resources. Nevertheless, an examination of the following issues may lead to locally relevant solutions:

1. Does it make sense for endless varieties of compliance challenges to be housed together? Can the institution truly and meaningfully bring together research integrity (e.g., conflict of interest, contract compliance, FISMA, scholarly conduct), human subjects (e.g., IRB, HIPAA), animal safety (e.g., IACUC), life safety (e.g., environmental health, radiation, occupational health), employee accessibility, diversity, risk management, internal audit, and so forth?

2. What about the silo effect of these numerous campus groups if they remain separated physically and in reporting...
Attend an EDUCAUSE regional conference in 2013 to discuss shared challenges and discover innovative IT solutions implemented by your higher education peers.

For a full list of upcoming events, visit educause.edu/Events.
lines? Secure data handling and data privacy regulations are frequently housed in differing parts of an organization, and in practice, authority flows from these differing parts and they may report up through differing structures. Most security officers (housed in information technology), as well as privacy officers (housed in numerous locations from audit to compliance to stand-alone offices), are familiar with the challenge of trying to address data security and privacy with researchers who are used to working under the domain of a vice chancellor for research.

3. Can the institution afford to not fund separate and distinct privacy, security, and compliance functions? Given the growing tangle of privacy legislation, the nuances associated with breaches may require clearing off privacy from security. One need look no further than HIPAA (Health Insurance Portability and Accountability Act) or PCI DSS (Payment Card Industry Data Security Standards) to find where “good security” is inadequate to prevent significant fines for non-compliance.  

4. Wherever and however these varied and various duties are housed, do they have access to the top of the structure—be that the president, chancellor, or board of regents/trustees? With all of these approaches, access to the top and to the change resources that can improve or mitigate circumstances must be a consideration. Will the positioning of these groups—either separately in departments that report up differing chains or combined but still not reporting directly to the top—restrict their effectiveness? What role does an institution want its external or public relations staff to have in responding to breaches, and can that staff over-ride the privacy or security voice in decision-making?

Nurturing healthy privacy, security, and compliance functions is a balancing act. Integration of the three areas can result in conflicting missions, whereas decoupling them can make it difficult to ensure a cohesive institutional strategy. Each higher education institution must find its own balance, calibrated according to its organizational structure.

In the end, privacy is key—wherever it finds a home in an institution. It is a unique need that must be considered as a distinct component of the institutional mission. Privacy, in its purest form, is an expression of respect for our communities: individuals are informed of what data is being collected about them and what is being done with that data, and they are assured that they have some control over what happens with their information. By complying with regulations and securing data, we can show our respect for students, staff, and the broader higher education community.

Integration of the privacy, security, and compliance functions can result in conflicting missions, whereas decoupling them can make it difficult to ensure a cohesive institutional strategy.

Notes
1. This article represents the considerations of the authors in their experience and practice and does not represent the position of the institutions for which they work. This is not legal advice; please consult university counsel for guidance in this process.
2. The original position of privacy officer at the University of Kansas was a direct report to the senior vice provost from 2005 to 2012. In 2012, an institutional compliance office was created, and privacy was placed within that office structure.
8. See Amazon Simple Storage Service (Amazon S3); http://aws.amazon.com/s3/iprotecting.
15. See the HIPAA Privacy Rule, Penalties: HIPAA Administrative Simplification 45 CFR 160, Part D. For PCI compliance violations, the payment brands may fine an acquiring bank (and send it downstream to merchants) $5,000 to $10,000 per month; http://www.pcicomplianceguide.org/pciqa.jsp.

© 2013 Michael Corn and Jane Rosenthal. The text of this article is licensed under the Creative Commons Attribution 3.0 Unported License (http://creativecommons.org/licenses/by/3.0/).
Experience the Institute.

2013 EDUCAUSE Institute Programs:

**New IT Managers Program**  
March 18–20 | Chicago, IL

**Management Program**  
July 15–19 | Evanston, IL

**Learning Technology Leadership Program**  
June 24–28 | Evanston, IL

**Leadership Program**  
July 22–26 | Evanston, IL

These dynamic and immersive programs help you gain practical knowledge to apply as a current or future IT leader. They provide an opportunity to enhance your skills and create a tight-knit group of peers for brainstorming, support, and sharing resources.

Find out which program is right for you »  
educause.edu/Careers/Educause-institute
The EDUCAUSE Awards Program, under the guidance of the EDUCAUSE Recognition Committee, brings peer endorsement and distinction to professional accomplishments in higher education information technology. The Rising Star Award, introduced in 2011, recognizes an IT professional who, still early in his or her career, demonstrates exceptional leadership and accomplishment in the area of information technology in higher education. The Leadership Award is the association’s highest recognition for individual achievement. This award acknowledges and celebrates exemplary leadership that has a significant and positive impact on advancing the theory and practice of information technology in higher education. All three awards are sponsored by Moran Technology Consulting, Silver Partner.
Melissa Woo is recognized as a strong leader, one who is expected to achieve continued success in the profession. At the University of Wisconsin–Milwaukee (UWM), Woo led the promotion of a central, core research cyberinfrastructure service without identified funding or widespread research faculty support. She chartered and staffed a faculty/staff committee, led by a respected faculty researcher, to identify related campus issues. The result was a series of far-reaching recommendations made to the executive leadership to improve the campus research cyberinfrastructure. She has presented numerous times on the high-performance computing support model, which could be fully adoptable by other universities.

One of the infrastructure initiatives started by Woo was the UWM identity and access management (IAM) program. Since its inception in 2010, the program has aggressively completed a number of significant milestones: the campus Active Directory was transformed from a service with no identified support to one with a stable support structure; a SAML (Security Assertion Markup Language) service was deployed to support federation and enterprise single sign-on; and UWM became a member of the InCommon and eduroam federations. As a result, UWM is actively engaged in activities supporting the establishment of InCommon Silver compliance implementation best practices for use by other higher education institutions.

Woo is a strong supporter of staff professional development, particularly in the area of mentoring. As chair of the EDUCAUSE Professional Development Advisory Committee, she instituted a major revision of the EDUCAUSE Mentoring Information Kit to focus on new mentoring styles appropriate to 21st-century professionals and an agreement between mentors and mentees before they enter into a relationship. Additionally, she collaborated with another UWM colleague to develop two mentoring pilots for the EDUCAUSE regional conferences: “minute mentoring,” which provides advice on specific topics in a “speed dating” format; and a program launched...
Thank you to our Doctorate Level sponsor for their support of our annual meeting.
at the 2012 EDUCAUSE Midwest Regional Conference) to match mentors and mentees during conferences.

Woo is a collaborative change agent and natural leader, one able to accomplish what is needed for campus information technology.

EDUCAUSE Review: You are an active proponent of mentoring in the IT higher education profession. Why do you feel so strongly about this topic?

WOO: As I’ve been helped greatly by the assistance of numerous mentors, both formal and informal, throughout my career, in some ways I feel very much like a “poster child” for the benefits of mentoring. Mentors have served many roles in my life. They have served as role models, consultants, advocates, and guides without whom I wouldn’t be where I am. Mentors continue to aid me in my career progression, for which I’m continually grateful.

Anyone can benefit from having the right mentors. After all, there are commonalities throughout higher education information technology. Why tackle a challenge without knowledgeable help, and why reinvent the wheel? A mentor can be a great sounding board and can share past experiences in order to assist in current decision-making. Another mentor might be able to open up advancement opportunities that one might not have access to otherwise.

A strong reason for promoting mentoring in our profession is the need to develop future higher education IT leaders to fill the leadership pipeline. Without the support of mentors, some candidates may leave the profession, while other promising candidates may not be identified. Another reason I actively promote mentoring is that I believe paying it forward to others is the best way I can honor the mentors who have helped me.

EDUCAUSE Review: What are the best mentoring approaches for preparing the next generation of IT leaders?

WOO: There are many different mentoring approaches for preparing the next generation of IT leaders. There are two aspects of mentoring to consider: mentoring styles and mentoring functions.

Mentoring styles that might be most appropriate for preparing the next generation of IT leaders for the next level of leadership include the traditional, network, circle, and invisible styles. Traditional mentoring is what most of us think of when we consider the topic of mentoring. This style of mentoring is delivered on a one-on-one basis, tends to be hierarchical in the sense that a more experienced individual acts as the mentor, involves an expert who passes along knowledge, and is generally considered to require a long-term commitment. Network mentoring involves a group of people who share knowledge with each other, can be hierarchical, and generally has a variable time commitment. Circle mentoring is similar to network mentoring in that it involves a group of people who share knowledge, but it consists of peers who make a medium/long-term time commitment to the circle. Finally, invisible mentoring occurs when one observes a mentor at a distance; it is not interactive. Learning occurs through extensive research into an invisible mentor’s life, from what has been written about him/her to the invisible mentor’s articles, presentations, and the like.

Mentoring functions most relevant to the next generation of IT leaders include sponsorship, visibility, coaching, role modeling, and counseling. Sponsorship involves nominating a mentee/protégé for positions and promotions. Visibility provides a mentee/protégé with opportunities for relationships with key figures. Coaching outlines strategies for accomplishing objectives. Role modeling provides attitudes, values, and behaviors for a mentee/protégé to emulate. Lastly, counseling explores concerns that may interfere with personal and career accomplishments.

EDUCAUSE Review: Do you have advice for IT staff just entering the profession?

WOO: I can’t emphasize enough the importance of mentors in one’s professional advancement. Consider putting together a professional development plan before seeking mentors. A professional development plan can help determine which mentoring styles and functions will be most important for goal attainment. Being aware of the appropriate mentoring styles and functions will aid in the selection of mentors. Always remember to look for those outside traditional mentor roles as well. Mentors are not only managers and leaders but also peers, colleagues at any level, and friends. All kinds of individuals, representing numerous different roles, can be valuable as mentors.

Mentors can be found through many different means: conferences, social networks, and professional organizations such as EDUCAUSE. If you think someone would make a good mentor, make sure to ask if she or he would be willing. What’s the worst that could happen? More important, what’s the best that could happen?

© 2013 Melissa Woo. The text of this section is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License (http://creativecommons.org/licenses/by-nc-sa/3.0).
## Upcoming 2013 ELI Events

<table>
<thead>
<tr>
<th>Date</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>February 15</td>
<td>Short Course: Part 1—Evaluating the Effectiveness of Mobile Learning Initiatives</td>
</tr>
<tr>
<td>February 26</td>
<td>Short Course: Part 2—Evaluating the Effectiveness of Mobile Learning Initiatives</td>
</tr>
<tr>
<td>March 6</td>
<td>Short Course: Part 3—Evaluating the Effectiveness of Mobile Learning Initiatives</td>
</tr>
<tr>
<td>March 18</td>
<td>Online Seminar</td>
</tr>
<tr>
<td>April 3-4</td>
<td>Spring Focus Session: Learning and MOOCs</td>
</tr>
<tr>
<td>May 20</td>
<td>Online Seminar</td>
</tr>
<tr>
<td>June 17</td>
<td>Short Course: Part 1—Designing and Delivering a Quality MOOC</td>
</tr>
<tr>
<td>June 24</td>
<td>Short Course: Part 2—Designing and Delivering a Quality MOOC</td>
</tr>
<tr>
<td>June 27</td>
<td>Short Course: Part 3—Designing and Delivering a Quality MOOC</td>
</tr>
<tr>
<td>August 14</td>
<td>Short Course: Part 1</td>
</tr>
<tr>
<td>August 26</td>
<td>Short Course: Part 2</td>
</tr>
<tr>
<td>September 9</td>
<td>Short Course: Part 3</td>
</tr>
<tr>
<td>September 16</td>
<td>Online Seminar</td>
</tr>
<tr>
<td>November 6-7</td>
<td>Fall Focus Session</td>
</tr>
<tr>
<td>December 9</td>
<td>Online Seminar</td>
</tr>
</tbody>
</table>

Are you already an ELI member? Be sure to tune in every month for our exclusive ELI webinars. For more details on these upcoming events, visit [www.educause.edu/ELI/Events](http://www.educause.edu/ELI/Events).
The Leadership Award

David G. Swartz
Assistant Vice President and CIO
American University

For advancing best practices in IT service management, strategic planning, project management, information security, technology operations, and enterprise infrastructure life-cycle planning

David G. Swartz is recognized for his dedication to demonstrating the value of information technology to fulfill the campus mission and for his overall service to the IT profession. Throughout his career, Swartz has not feared change as an innovative way to improve IT services to the campus community, and his academic background in economics has served him well in making difficult decisions regarding the associated resource allocations. He understands the need for analytics to measure performance, track progress, and benchmark against peer institutions.

He has transformed the central IT organization at American University into a strategic business partner, enabling the effective and efficient use of technology by the institution. Incorporating fresh ideas and knowledge from past experiences, he successfully introduced industry-standard best practices in IT service management, strategic planning, project management, information security, technology operations, and enterprise infrastructure life-cycle planning. He was also among the first CIOs to understand the need for the role of the chief information security officer to build a strong security program at the institution—specifically, American University. Before joining American University, he eliminated legacy stovepipe operations and centralized information technology across George Washington University to leverage resources and target redundancies. His judicious use of outsourcing arrangements saved the university more than $1 million a year and improved service levels.

Swartz's many contributions to the profession include serving as faculty at the EDUCAUSE Institute Leadership Program, as council member at the Hawkins Leadership Roundtable, and as the Higher Education Information Security Council (HEISC) Executive Committee Chair. He has demonstrated his wide knowledge of IT issues by speaking at numerous EDUCAUSE conferences, authoring many publications, and presenting at a variety of venues. He is the recipient of honors and awards from IT authorities such as Computerworld, CIO
**SWArTZ:** Self-awareness is about being comfortable with who you are. The happier you are with yourself, the more likely you’ll be to treat others with kindness. To lead people, you must understand them, and by understanding ourselves, we are better able to understand others. Self-aware leaders have brought significant parts of their unconscious minds into consciousness, so they are less controlled by unconscious bias and filters. Self-aware leaders have developed emotional intelligence and thereby can build the relationships that allow them to lead. Once we can express more self-awareness, we have removed much of our negative self-talk and are more positive. As we express more self-awareness, we have more present-moment awareness and worry less about the future and are less obsessed about events in the past. We are better at listening and engaging fully. One of the benefits of improved self-awareness is a clear mind. With a clear mind, we are better able to focus and be one-pointed and less distracted. A self-aware leader is grounded and unshakable. This ability is measurable using galvanic skin response and blood pressure. The stress was unbelievable. I needed to find a way to better handle stress and maintain some balance if I was going to survive as a CIO. The results of this discovery process led me to the realization of the importance of self-awareness. Without the benefits of the growth of self-awareness, I would not have been successful as a CIO.

**EDUCAUSE Review:** Why is self-awareness important to leadership?

**SWArTZ:** I have found that self-awareness can be enhanced by focusing on balancing the physical, emotional, and mental dimensions of life. We all know about the importance of proper diet, rest, and exercise. Even focusing on just these areas in the physical dimension will create significant benefits. Further, we can balance the emotional dimension by flowing kindness and sharing an appreciation of others. Even simply giving a smile can uplift everyone. Next, regarding the mental dimension, I have found that positive thinking helps to address negative self-talk. All successful golfers know to stay focused on where they want the ball to go rather than on the hazards; otherwise, their ball will end up in the water or sand-trap almost every time. I have also found that meditation is the ultimate balancing technique that addresses all three of these dimensions, resulting in significant growth in self-awareness. Some of the most successful business and political leaders, entertainers, sports professionals, and inventors have discovered the benefits of meditation: Steve Jobs, Larry Ellison, Al Gore, Candy Crowley, Jerry Brown, Oprah Winfrey, William Ford Jr., Tiger Woods, Gary Player, Jerry Seinfeld, Richard Gere, Thomas Edison, and even Albert Einstein. Additional steps can be taken to consult with expert counselors who can help people see blind spots more clearly. Also, 360 reviews can provide much useful information that may be hidden from view.

**EDUCAUSE Review:** Do you have advice for how IT leaders can demonstrate the value of information technology to fulfilling the campus mission?

**SWArTZ:** Most IT leaders do not document the value of information technology to the college or university. Even after the completion of a
transformational project, we often move on to the next project rather than demonstrating the value of the recent initiative. This documentation can take the form of a traditional economic ROI, such as improved efficiency or effectiveness or qualitative improvement to services. It is good to have the process or functional owners give testimony and help to document the benefits. The higher education institution has multiple objectives in the areas of teaching, research, and service, and the benefits of information technology need to be assessed for each of these areas. This can be captured in a periodic annual report or customer forum. The word gets out to others, and it helps to build the foundation for further investment and trust in information technology. It is important that information technology demonstrate its value not just as a reliable utility, but also as a campus organization that can foster strategic improvements to the processes and competitiveness of the institution. One of the challenges is also to be sure to focus on the most important projects, not just the squeaking wheels. A mature portfolio process on the front end—one that filters out poor investments and helps to focus resources on the most critical needs—is essential to success and is more likely to result in initiatives that can demonstrate great value to the institution.

© 2013 David G. Swartz. The text of this section is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Unported License (http://creativecommons.org/licenses/by-nc-nd/3.0/).

For advancing the interlocking systems of technical, financial, professional, social, and political processes that brought about fundamental and disruptive change

Earnings L. Blythe has been one of the foremost leaders in higher education information technology, influencing change and new directions in the application of networking technology in higher education. A unifying theme for Blythe's accomplishments is his leadership across the interlocking systems of technical, financial, professional, social, and political processes that have brought about a fundamental and disruptive change in how we use communications in higher education and beyond. Blythe has played a central role in the proliferation of modern broadband networking by coordinating and educating the stakeholders on his campus, in his profession, in state and local governments, and in industry about the fundamental, qualitative advantages of a new style of networking.

At the same time that Blythe was closely involved in the critical movement toward community-owned, facilities-based networks of regional and national scale, he also made strong contributions through white papers, conferences, and visits to the Hill and the Federal Communications Commission—contributions that had demonstrable impact on national policies and programs such as the FCC's National Broadband Plan, the U.S. Broadband Technology Opportunities Program, and the proper consideration of scope and methods with regard to copyright issues and lawful surveillance on campus networks.

Blythe has repeatedly demonstrated a rare combination of brilliant creativity and pragmatic leadership to drive a long series of groundbreaking initiatives at Virginia Tech: network infrastructure and services; the Faculty Development Initiative Program; the Vir-
BLYTHE: Ultimately, an effective IT leader in higher education today must be able to see and evaluate opportunities and then match the right talent with the relevant competencies, to the chosen opportunities.

At the most basic level, three competencies essential to success in the IT profession are the ability to analyze, the ability to be precise in the use of language, and the ability to organize and synthesize. For example, an early lesson in computer languages was that computational machines do exactly what you tell them to do. Most of the worst debacles in computational systems can be traced back to an imprecise—sloppy—use of language. Assuming the presence of those basic competencies, when I am looking for a potential leader in information technology, especially at the senior management level, the first questions I ask are: What have you done? What do you know? Are you hungry to discover and to learn?

But I have also become convinced that to achieve extraordinary things, leaders need three other characteristics, ones that are tough to ascertain: vision, commitment to the ideal of higher education, and courage. For example, driving the early Internet in the form of NSFnet, we had visionaries in our community, people like Kenneth King, Stuart Lynn, Mike Roberts, Stephen Wolff, Glenn Ricart, Doug van Houwelling, and many others who recognized the opportunity and who realized the potentially extraordinary but unquantifiable benefits of the invention and of new concepts developed by university and federally sponsored researchers. These people took great risks to enable the nationwide demonstration of this new mode of communication. They did not do so for fame or fortune; they did this for our community—to enhance research, discovery, and learning.

EDUCAUSE Review: For having reached across systems and networks during your career. How can leaders encourage similar collaboration among IT staff, as well as throughout and across institutions?

BLYTHE: If there is one constant to the history of man, it is the continuous economization of information: increasing specialization and divisions of labor that have accelerated in our networked, globally connected, 21st-century world. This has brought us changes in how the global community interacts and learns—set in motion by accelerating technological innovations—and will either create great opportunity or result in significant irrelevance for traditional institutions of higher education. So the message I share with my colleagues is that with this constantly increasing specialization, we must collaborate or become irrelevant.

For great examples of leadership, we are graced by extraordinary IT professionals and researchers across the spectrum of higher education. Over my career I have realized that there is probably no emerging technology,
process, concept, or opportunity that isn’t being examined and tested somewhere in our community. More important, when that occasional great idea—that potentially disruptive technology—shows promise, there will always be a few early movers in our community who are willing to collaborate and to coalesce around large-scale proof-of-concept initiatives and, if warranted, aggressive exploitation of that breakthrough. The Internet as we know it today, large-scale and highly parallel high-performance computing, and the open-source movement have benefited from, and may even owe their existence to, this characteristic of our community.

It is especially humbling to have known and worked with accomplished leaders in information technology, at Virginia Tech and across the United States. To a very real extent, everything that my colleagues and I have accomplished at Virginia Tech over the last thirty-five years has been built on collaborations leveraging the great ideas and accomplishments of these IT leaders.

**EDUCAUSE Review: As you move into retirement and look back on your career, do you have advice for your colleagues who continue to face the challenges of the higher education IT profession?**

**BLYTHE:** Certainly, the lessons from the darkest days of my life—following the mass murders at Virginia Tech on April 16, 2007—are the starkest. The first was that a significant disconnect exists between IT practitioners and public safety principals at the campus and local community levels. I will say more about the implications and obligations related to safety and security in a future article in *EDUCAUSE Review.*

We are all part of the education community, supporting the highest of all human endeavors: learning and teaching. I am convinced that information technology is the DNA of the global education fabric and that leading-edge competencies in information technology for those involved in higher education are critical and strategic to its future.

But we are also privileged to work and lead in a national university community with broad, shared values and with traditions of inclusiveness and fairness and justice. This is who we serve, and this is what makes our jobs as IT professionals so special.
### 2013 EDUCAUSE Events

EDUCAUSE events—all designed for you to learn from and network with thought leaders and peers—range from hour-long webinars to multi-day, hybrid conferences and annual meetings.

<table>
<thead>
<tr>
<th>FEBRUARY</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>EDUCAUSE Learning Initiative Annual Meeting</td>
<td>Feb. 4–6</td>
<td>Denver, CO, and Online</td>
</tr>
<tr>
<td>West/Southwest Regional Conference</td>
<td>Feb. 12–14</td>
<td>Austin, TX, and Online</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MARCH</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>NERCOMP Annual Conference</td>
<td>Mar. 11–13</td>
<td>Providence, RI, and Online</td>
</tr>
<tr>
<td>EDUCAUSE Institute New IT Managers Program</td>
<td>Mar. 17–20</td>
<td>Chicago, IL</td>
</tr>
<tr>
<td>Midwest Regional Conference</td>
<td>Mar. 18–20</td>
<td>Chicago, IL</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>APRIL</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>EDUCAUSE Learning Initiative</td>
<td>Apr. 3–4</td>
<td>Online only</td>
</tr>
<tr>
<td>Online Spring Focus Session</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Professionals Conference</td>
<td>Apr. 15–17</td>
<td>St. Louis, MO, and Online</td>
</tr>
<tr>
<td>Advanced Core Technologies Meeting</td>
<td>Apr. 16–17</td>
<td>St. Louis, MO</td>
</tr>
<tr>
<td>Enterprise IT Leadership Conference</td>
<td>Apr. 16–18</td>
<td>St. Louis, MO</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MAY</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Southeast Regional Conference</td>
<td>May 29–31</td>
<td>Atlanta, GA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>JUNE</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Leading Change Institute, Successor to Frye</td>
<td>June 2–7</td>
<td>Washington, DC</td>
</tr>
<tr>
<td>EDUCAUSE Institute Learning Technology Leadership Program</td>
<td>June 24–28</td>
<td>Evanston, IL</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>JULY</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Breakthrough Models Academy</td>
<td>July 14–19</td>
<td>Boston, MA</td>
</tr>
<tr>
<td>EDUCAUSE Institute Management Program</td>
<td>July 15–19</td>
<td>Evanston, IL</td>
</tr>
<tr>
<td>EDUCAUSE Institute Leadership Program</td>
<td>July 22–26</td>
<td>Evanston, IL</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OCTOBER</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>EDUCAUSE Annual Conference</td>
<td>Oct. 15–18</td>
<td>Anaheim, CA, and Online</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NOVEMBER</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>EDUCAUSE Learning Initiative</td>
<td>Nov. 6–7</td>
<td>Online only</td>
</tr>
<tr>
<td>Online Fall Focus Session</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

For a comprehensive list of upcoming events, please visit [educause.edu/Events](http://educause.edu/Events).
Changing the Conversation

We live in an information culture. We are accustomed to having information instantly available and accessible, along with feedback and recommendations. We want to know what people think and like (or dislike). We want to know how we compare with “others like me.” Just as analytics powers Amazon.com, Netflix, TheRestaurantFinder.com, and Yelp, it can support tools for student empowerment.

Empowerment hinges on having access to information, which can help students make better choices to navigate college more successfully. As we have explored student empowerment in higher education, several guidelines have emerged from what we are learning.

“Use data to change the conversation.” Students, faculty, staff, and the public—we all make assumptions easily. Having data at hand can change the conversation by informing questions and providing concrete answers. In a highly complicated environment, assumptions and anecdote aren’t enough. Higher education has a responsibility to provide guidance to help students make good decisions based on data. But using data well requires the development of “data literacy.” We must help students understand the data and what it means to them.

For example, too many course choices can be confusing for students, and making poor course selections could delay graduation. Degree Compass, a course-recommendation system developed at Austin Peay State University, uses predictive analytics to help students find the courses that best fit their degree program, overlaid with a model predicting the students’ success in the course. The system guides students and advisors in deciding on a pathway to graduation. Recommended course lists, the role each course plays in a degree program, and class availability information are readily available to students.

“Move from the past to the predictive.” Much of our data use has revolved around reporting on what happened—in the past. Data use is moving to the
and predictive algorithms, system alerts trigger individualized interventions that can help students, advisors, and/or faculty tap resources to avert failure.

“Empower choice, don’t restrict it.”

For almost any decision, there are more options than we may realize—sometimes so many that decision-making can become paralyzed. As noted above, choice—without good information and guidance—can be the enemy of student success. Analytic systems allow us to personalize recommendations that help students make better-informed choices. With good information, students might ask: “What should I do differently?” And they might use data to find alternative paths to their goal.

Knowing whether they are “on track” makes a difference to students. The eAdvisor system at Arizona State University and STAR at the University of Hawaii assist students in selecting appropriate courses and tracking progress toward their major. eAdvisor was designed to take the guesswork out of how to earn a degree so that students would stay on track to graduate. For example, it helps students choose a major based on their interests and career goals, and it then highlights appropriate course sequences. Because much of the degree requirements tracking is handled online, in-person advising services can be expanded, allowing more time to explore degree and career choices and address individual needs.

“Use data for gateways, not just gatekeeping.”

We have been conditioned to think of data as summative—as an end point. A report, a grade, or a test either opens a door or closes it. Thanks to analytics, data can point learners to personalized learning pathways tailored to their needs, aspirations, abilities, and timelines. Although data has historically flowed in only one direction, serving to validate compliance or trigger funding, data is actually most useful to inform thinking, questioning, planning, and next steps.

Rapid feedback enables accelerated learning for students. Carnegie Mellon University’s Open Learning Initiative uses feedback loops based on analytics. Students receive feedback in corrections, suggestions, and cues tailored to their performance. Student learning is accelerated, along with equal or better retention and performance compared with traditional instruction. Instructors receive feedback about students’ knowledge, how students are using course materials, and students’ use patterns. Instructors have better information on which to base course refinements and inform theories of learning.

Few transactions are as complicated as college. By informing questions and providing concrete answers, analytics can empower students to make good choices. Analytics can thus change the conversation, both for students and for institutions.

© 2012 Diana G. Oblinger. 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/).

Diana G. Oblinger (doblinger@educause.edu) is President and CEO of EDUCAUSE.
**Kaseya**

**Education IT Bundle**

Automated IT systems management solution built for schools

- Scripts, Monitor Sets & Reports
- Discovery, Audit & Inventory
- Remote Control & Management
- Patch & Software Deployment
- Endpoint and Network Monitoring
- Kaseya Advanced Basics Training
- Imaging, Deployment & Migration
- Power Management & Desktop Policy
- ITIL Compliant Service Desk
- Post-Implementation Checkup

[www.kaseya.com/educause](http://www.kaseya.com/educause)

---

**Multiple Devices.**

**Multiple Sources.**

**One Solution.**

_[Logo: Moofwd.com]_  

---

**Rethink the rules.**

**Game Changers: Education and Information Technologies**

Download the free e-book » [educause.edu/GC](http://educause.edu/GC)

---

**Empower**

Student Information System

Fully integrated solution from recruitment to advancement.

Download a free SIS Buying Guide  
[www.sisbuyingguide.com](http://www.sisbuyingguide.com)

(888) 826-6773 • [www.empowersis.com](http://www.empowersis.com)
# Advertiser Index

<table>
<thead>
<tr>
<th>Company</th>
<th>Contact</th>
<th>Website</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apogee</td>
<td></td>
<td><a href="http://www.apogee.us">www.apogee.us</a></td>
<td>21</td>
</tr>
<tr>
<td>Campus Management</td>
<td>1-866-397-2537</td>
<td><a href="http://www.campusmanagement.com/vue">www.campusmanagement.com/vue</a></td>
<td>3</td>
</tr>
<tr>
<td>CDW-G</td>
<td>1-800-767-4239</td>
<td><a href="http://www.CDWG.com/datacenter">www.CDWG.com/datacenter</a></td>
<td>5</td>
</tr>
<tr>
<td>Dean Evans &amp; Associates</td>
<td>1-800-440-3994</td>
<td><a href="http://www.dea.com/educ">www.dea.com/educ</a></td>
<td>30</td>
</tr>
<tr>
<td>EMPOWER/ComSpec International</td>
<td>1-888-826-6773</td>
<td><a href="http://www.empowersis.com">www.empowersis.com</a></td>
<td>50</td>
</tr>
<tr>
<td>Epson</td>
<td></td>
<td><a href="http://www.epson.com/highered">www.epson.com/highered</a></td>
<td>7</td>
</tr>
<tr>
<td>Ginkgotree</td>
<td></td>
<td><a href="http://www.ginkgotree.com">www.ginkgotree.com</a></td>
<td>50</td>
</tr>
<tr>
<td>Hobsons</td>
<td>1-800-927-8439</td>
<td><a href="http://www.hobsons.com">www.hobsons.com</a></td>
<td>28</td>
</tr>
<tr>
<td>Jenzabar</td>
<td>1-877-536-0222</td>
<td><a href="http://www.jenzabar.com/tco">www.jenzabar.com/tco</a></td>
<td>inside back cover</td>
</tr>
<tr>
<td>Kaseya</td>
<td></td>
<td><a href="http://www.kaseya.com/educe">www.kaseya.com/educe</a></td>
<td>50</td>
</tr>
<tr>
<td>Laserfiche</td>
<td>1-800-985-8533</td>
<td><a href="http://www.laserfiche.com/educe">www.laserfiche.com/educe</a></td>
<td>23</td>
</tr>
<tr>
<td>Moofwd</td>
<td>1-855-2-MOOFWD</td>
<td><a href="http://www.moofwd.com">www.moofwd.com</a></td>
<td>50</td>
</tr>
<tr>
<td>Pearson Learning Solutions</td>
<td></td>
<td><a href="http://www.pearsonlearningsolutions.com">www.pearsonlearningsolutions.com</a></td>
<td>back cover</td>
</tr>
<tr>
<td>Perceptive Software</td>
<td></td>
<td><a href="http://www.perceptivesoftware.com/highered">www.perceptivesoftware.com/highered</a></td>
<td>6</td>
</tr>
<tr>
<td>Sonic Foundry</td>
<td>1-877-783-7987</td>
<td><a href="http://www.sonicfoundry.com">www.sonicfoundry.com</a></td>
<td>19</td>
</tr>
<tr>
<td>Steelease</td>
<td></td>
<td><a href="http://www.steelease.com/verb">www.steelease.com/verb</a></td>
<td>inside front cover</td>
</tr>
<tr>
<td>TCPN — The Cooperative Purchasing Network</td>
<td></td>
<td><a href="http://www.TCPN.org">www.TCPN.org</a></td>
<td>17</td>
</tr>
<tr>
<td>WolfVision</td>
<td></td>
<td><a href="http://www.wolfvision.com">www.wolfvision.com</a></td>
<td>50</td>
</tr>
<tr>
<td>Workday</td>
<td>1-925-951-9000</td>
<td><a href="http://www.workday.com">www.workday.com</a></td>
<td>11</td>
</tr>
</tbody>
</table>

EDUCAUSE is a nonprofit association whose mission is to advance higher education through the use of information technology.

## EDUCAUSE Board of Directors

**Debra H. Allison, Chair**  
Vice President for Information Technology and CIO  
Miami University

**Brian Voss, Vice Chair**  
Vice President and CIO  
University of Maryland

**Susan Metros, Secretary**  
Associate Vice Provost, Associate CIO, Professor  
University of Southern California

**Bruce Maas, Treasurer**  
CIO and Vice Provost for Information Technology  
University of Wisconsin–Madison

**Kara Freeman**  
Vice President of Administration and CIO  
American Council on Education

**Joy Hatch**  
Vice Chancellor, Information Technology Services  
Virginia Community College System

**David Lassner**  
Vice President for Information Technology and CIO  
University of Hawaii

**Richard Northam**  
Chief Executive Officer  
The Council of Australian University Directors of Information Technology (CAUDIT)

**Pattie Orr**  
Vice President for Information Technology and Dean of Libraries  
Baylor University

**Justin Sipher**  
Vice President of Libraries and Information Technology  
St. Lawrence University

**Vernon C. Smith**  
Chief Academic Officer and Provost  
MyCollege Foundation

**Randall J. Stiles**  
Special Advisor to the President  
Colorado College

**Ex Officio Member**  
**Diana G. Oblinger**  
President and CEO  
EDUCAUSE
Is Linking Thinking? 
Addressing and Assessing Scholarship in a Digital Era

Our analog world is being replaced with a digital one that at times replicates the features and functions of its predecessor and at other times completely turns the past on its head. Pixar made award-winning movies without calling into question the notion of what it means to be a Hollywood film. Netflix eviscerated the video-rental store. It is within this uneven and bewildering moment that those of us in higher education need to consider our approach to this new thing called digital scholarship.

The words we choose to frame this question are fraught. Digital scholarship? Digital humanities? Whose agenda are we supporting when we choose one turn of phrase instead of another? What happens to the “regular” humanities curriculum if it is replaced by a digital humanities curriculum? Will the story of digital humanities prove to be the story of Pixar or Netflix?

Here are some tricky questions that tenure committees may need to answer in the coming semesters:

- Can a blog count as scholarship?
- Is open peer review as valid as double-blind peer review?
- Does scholarship that can be read only onscreen count as scholarship?
- Do the terms of evaluation for “born digital” require a whole new vocabulary, or can new forms of scholarship be evaluated effectively within existing frameworks?

Evaluative frameworks are still in development within organizations such as the Modern Language Association and the American Historical Association and have not yet been fully tested in tenure cases on most campuses. These new frameworks will shape an institution’s faculty, its curriculum, and ultimately the campus library and technology needs. In the end, avoiding these questions will be difficult as a campus develops its digital scholarship strategy. Some of these questions may seem like threats. Others will take the form of opportunity.

Threats. Just a decade ago, humanities scholarship was relatively inexpensive to support. Give the English and History Departments an Internet connection, a word processor, and a subscription to JSTOR and the MLA bibliography, and they were all set. In contrast, today’s digital humanities scholars can be as expensive to support as the hard scientists. Now it’s not just the chemist or the computer scientist but also the English professor who is clamoring for more storage, more compute cycles, more help with compiling programs, and sustainable data-management schemes. These start-ups have not yet been factored into most operating budgets. Combine that with the general skepticism about the long-term prospects for humanities of any sort, and the prospects for this new form of scholarship seem bleak at best.

Opportunities. The U.S. Department of Labor projects that 65 percent of the U.S. children in kindergarten today will be employed in jobs that currently do not exist. As a nation and as an increasingly interconnected global society, we face massive challenges: climate change, globalization, the collapse of the social contract between employer and employee. How do we make sense of these transformations? How do we develop sensible, humane, and sustainable answers to these daunting changes that have life-altering implications for us and our children? For students, there may be short-term advantages to acquiring very specific and employable skills during a college career. However, in the long-term, students are likely better served by acquiring the general capabilities needed to navigate a rapidly changing future that demands a complex set of skills extending beyond the “merely” technical. Is there an answer to be found in a form of education and scholarship that powerfully combines a technical capability with foundational questions about identity, society, and culture? Some argue that digital scholarship can show why the humanities and the liberal arts matter more than they ever have. Others argue that the humanities and the liberal arts can be taught effectively without all of this expensive technology.

In the debate around digital scholarship, we have the perfect storm. On the one hand, we have the conservatism in the culture of most higher education institutions. On the other, we have board-level anxieties arising from the upstart challenges posed by the world of MOOCs, badges, and other emerging forms of external competition. As Clayton Christensen has taught us, disruptive innovations from outside can blind us from seeing new forms of competition for what they really are. Much as the American steel industry failed to understand the threat posed by the rebar produced by the Japanese mini-mill platform, so too higher education may be unable to see the siege from these new interlopers. But let’s make sure this crisis doesn’t push us to place the emphasis on the wrong questions. As we consider the
impact that the innovations that will follow MOOCs will have on our institutions, we need to think long and hard about how we, within our institutions and our various professional guilds, will adapt to the threats to our livelihoods and our institutions posed by these disaggregating technologies that disrupt every single means of production. The plight of digital scholarship may seem small in the grand scheme of the future of higher education. Yet this story could serve as the canary in the coalmine—as a harbinger of things to come, another market opportunity we may unwittingly cede to disruptive innovation from outside our walls.

The world of digital scholarship is a world of both promise and peril. Most schools have not yet significantly invested in this area. Are such investments merely life-support for a dying patient, or are they strategic in an existential fight for the soul of the university? The choices, the conversations, and the debates all connect in an integral way to the future of scholarship, scholarly communication, and classroom instruction.

Just as Pixar brought to the movie screen an experience previously unattainable using the traditional techniques of animation, so too there are promises associated with the transformation of scholarship enabled by the expressive and computational power of technology. We can ask new questions of large bodies of texts; we can visualize ancient ruins; we can perform pattern recognition across large bodies of visual materials to reveal underlying themes; we can embed rich media—audio, video, animation—within the very texts of our arguments, all while making scholarship more public and accessible than ever before. These new modes of argumentation and representation may allow us to re-enliven the discussion around humanities, may allow for new forms of collaboration across disciplines and among institutions that in turn could serve as a catalyst for important new working relationships necessary for the continued relevance of our institutions in the 21st century. While there is some urgency to deciding on how one chooses to approach the bewildering and accelerating change that is coming from outside, there are also difficult choices to make: is it the humanities and liberal arts or the digital humanities and the digital liberal arts that will prepare our students for a world of globalization, climate change, and all of the attendant challenges?

Notes
4. For an excellent analysis of the challenges of evaluating born digital scholarship, and of the threats and opportunities that new forms of peer review pose for our systems of evaluation, see Kathleen Fitzpatrick’s blog “Planned Obsolescence”: http://www.plannedobsolescence.net/about/.
5. See the work of Anvil Academic (http://www.anvilacademic.org), a digital-only press that is grappling with this vexing question of how to provide authority and legibility to these new forms.
7. See, for example, the Modern Language Association’s *Guidelines for Evaluating Work in Digital Humanities and Digital Media*, January 2012, http://www.mla.org/guidelines_evaluation_digital.
8. For a provocative proposal that would address the current crisis in the humanities, see Toby Miller, Blow Up the Humanities (Philadelphia: Temple University Press, 2012).

Michael Roy (mdroy@middlebury.edu) is the L. Douglas and Laura J. Meredith Dean of Library and Information Services and Chief Information Officer at Middlebury College.

© 2013 Michael Roy. The text of this article is licensed under the Creative Commons Attribution-NonCommercial 3.0 Unported License (http://creativecommons.org/licenses/by-nc/3.0/).
ds106: Not a Course, Not Like Any MOOC

Looking for something different from the current hysteria of Massive Open Online Courses (MOOCs)? A digital storytelling course started by Jim Groom at the University of Mary Washington (UMW), ds106 was set loose as an open course in January 2011 (http://ds106.us/). Yet the UMW catalog does not include such a course. Its actual course designation is CPSC 106 (Computer Science)—a small but telling example of how ds106 plays with and questions the norm.

Most classes in digital storytelling revolve around the personal video narrative form as popularized by the Center for Digital Storytelling (http://www.storycenter.org/). But ds106 storytelling explores the web as a culture, as a media source, and as a place to publish in the open. Not claiming to authoritatively define digital storytelling, ds106 is a constant process of questioning digital storytelling. Is an animated GIF a story? What does it mean to put “fast food” in the hands of Internet pioneers? Why would we mess with the MacGuffin? Is everything a remix? Though this is perhaps simply semantic wordplay, ds106 is not just “on” the web—it is “of” the web.

Characteristic of ds106 is its distributed structure, mimicking the Internet itself, and its open-source non-LMS platform. Students are charged with registering their own domain, managing their own personal cyberinfrastructure, and publishing to their own website. Via the WordPress plugin FeedWordPress, all content from students is automatically aggregated to the main ds106 site—but all links go back directly to the students’ sites.

What do students get out of this? Colin Schulz, a former UMW student, explains:

Going into DS106, I had extensive knowledge of computer programming but did not understand how to implement my programming skills with web design. By managing and creating our own blogs on the WordPress platform in ds106, I successfully learned about the WordPress platform and web design.

The summer following successfully completing the course, I interned for a company. One of my tasks was to simply put language into a newly created website that was not launched but was successfully built by a professional web developer.

Within the first week of doing minor fixes to the new website, I was asked to restart the process from scratch and fully design and develop them a new website by myself. The skills I obtained from participating in ds106 allowed me to finish the website in a month, and since then it’s been fully launched.

The idea to open up ds106 followed the lead of the first course to be called (by Bryan Alexander and Dave Cormier) a “MOOC”: the 2008 “Connectivism and Connective Knowledge” (CCK08) course taught by George Siemens and Stephen Downes. Open participants in ds106 can choose to use any blog platform, which is then subscribed to by the ds106 site. Other institutions teaching related courses connected their students into the flow of ds106: Temple University in Japan, York College (CUNY), SUNY Cortland, Kansas State University, Kennesaw State University. At any one time, the ds106 site includes overlapping work of students at UMW, students at these other institutions, and people who are just following along. Thus ds106 is more community than course.

In its present incarnation at UMW, ds106 stands apart from the current crop of MOOCs in several ways:

- There are no video lectures. Assignments are published weekly, including a mix of readings, videos, and creative work.
- There is no concept of dropping out. The structure of ds106 allows open participants to tune in only to parts they care about. One such participant, Emily Strong (http://erstrongds106.wordpress.com/), shares: “I’ve heard before that practicing creativity regularly makes you more creative, and from participating in DS106 I have to say that this is absolutely true. Between daily creates and projects from the assignment bank, I am constantly creating things, and I find myself taking more creative approaches to everything else in my life, from approaching problems at work to noticing the interesting angles and textures of a room.”
- The experience for open participants need not be the same as that for enrolled students. Most MOOCs aim to create the same experience for all participants; in ds106, open participants create their own pathways.
- Massive is about impact more than numbers. Open participants add value to the experience for enrolled students. They offer ideas and constructive feedback and are often active members of UMW students’ group projects. Regarding numbers, the ds106 website currently subscribes to 620 blogs and has aggregated 23,000 external posts since January 2011. More than 800 people have published at least one item to ds106, with some of them having published hundreds.
- ds106 offers no certificates or badges. People join out of their own interest or just to be part of a community. Open par-
The web syndication structure of the course is not limited to ds106. The same platform was deployed in a Fall 2012 open online course in Entrepreneurship in Education (http://www.edstartup.net/) and in Project Community, a course offered by the Hague University of Applied Sciences (http://projectcommunity.info/). Similar functionality is provided by gRSShopper (http://grsshopper.downes.ca), developed by Stephen Downes for a number of the Connectivist-style MOOCs.

One last characteristic of ds106 is that it is not supported by millions of dollars of investment money. Though the course started at the University of Mary Washington, ds106 truly belongs to its community. Hosted externally, the ds106 website is supported by its participants via a 2012 Kickstarter campaign (http://www.kickstarter.com/projects/jimgroom/ds106-the-open-online-community-of-digital-storyte).

No one claims ownership of ds106. Its success can be traced to innovation supported by the University of Mary Washington and carried out by the UMW Division of Teaching and Learning Technologies (DTLT) and to the vision of former UMW leaders Gardner Campbell and Chip German and DTLT team members: Jim Groom, who crafted much of the spirit and drive of ds106; Martha Burtis, who built many of the key web pieces (and has taught the class); and Tim Owens, who shaped the design and functionality of the sites. But the contributions extend further. UMW student Aaron Clemmer built a twitterbot that updates the current content on ds106 radio, itself a contribution of open participant Grant Potter (University of Northern British Columbia). From Scotland, John Johnston has created storytelling tools (e.g., http://johnjohnston.info/blog/?e=2264) that emerged from experiments in ds106 assignments. We lack enough space to list everyone who has contributed to ds106!

How can you be a part of ds106? We’ve seen K–12 teachers tap into specific tasks from the Assignment Collection. Others make use of the Daily Create or just the radio station. The value of comments on participants’ blogs can never be overlooked. And we will set up syndication for anyone who is teaching a “ds106-ish” class in 2013 (http://ds106.us/teaching-ds106/) and who wants to integrate the class into the ds106 site and community.

Much more than a course, ds106 is an experiment in the shape and potential of open education.

Alan Levine (cogdogblog@gmail.com), an independent consultant (CogDog.it), currently teaches the open digital storytelling course ds106. Levine is an innovator in educational technology, previously working as an instructional technology specialist at the University of Mary Washington, following leadership positions at the New Media Consortium and the Maricopa Community Colleges.

© 2013 Alan Levine. The text of this article is licensed under the Creative Commons Attribution-ShareAlike 3.0 Unported License (http://creativecommons.org/licenses/by-sa/3.0/).
Amassing Student Data and Dissipating Privacy Rights

From test-performance scores to student financial data to statewide longitudinal data systems, there has been a dramatic increase in the collection of students’ sensitive information over the last decade. Both the U.S. Congress and the presidential administrations have touted the amassing of student data as beneficial and necessary to a successful education system. However, the increase in the collection of student data has led to a marked decrease in student data protection. Changes to student privacy regulations and government programs such as the Education Data Initiative underscore the need for meaningful oversight for the protection of student data.

The Education Department and Privacy Safeguards

In 2008 and 2011, the U.S. Education Department amended the regulations for the Family Educational Rights and Privacy Act (FERPA). These amendments increased private company and third-party access to student data. The 2008 changes expanded the definition of “school officials” to include “contractors, consultants, volunteers, and other parties to whom an educational agency or institution has outsourced institutional services or functions it would otherwise use employees to perform.” This amendment gives companies like Google and Parchment access to education records and other private student information.

Google Apps for Education offers “free Web-based email, calendar, and documents” to “millions of students and educators worldwide.” Arizona State University, the University of Michigan, Brown University, and other higher education institutions use Google Apps for Education to provide many of the services that colleges and universities had typically provided directly to students and faculty—resources for research, e-mail, and document production. Because higher education can spend hundreds of thousands of dollars to provide e-mail servers to students and faculty, the allure of “free” e-mail service is obvious. Less obvious, however, is that students are paying the cost to use Google’s “free” servers by providing access to their sensitive data and communications.

Google states: “To the extent that Customer Data includes FERPA Records, Google will be considered a ‘School Official’ … and will comply with FERPA.” Presumably, “FERPA Records” mean “education records,” including test scores, transcripts, and disciplinary infractions. Other Google representations raise real concerns about how the student information, now in control of private companies, will be used. For instance, Google will disclose student information from its Apps for Education if it has a “good-faith belief” that such disclosure is “reasonably necessary” to comply with law enforcement requests and to protect “the rights, property or safety of Google, [Google] users or the public as required or permitted by law.” This means that Google, and not the educational institution, will be making decisions about when to disclose sensitive student (and faculty) information to law enforcement agencies.

Parchment is another popular third-party entity to which colleges and universities routinely outsource students’ most prized commodity: transcripts. Parchment is a web-based service that permits colleges to “receive, request, and analyze electronic transcripts.” Despite Parchment’s claim that its services are “fully secure and FERPA compliant,” the company’s terms of use reveal that to the extent permissible by law, Parchment disclaims any representation or warranty that its site is secure and disclaims any liability for lost data. In an era of rampant security breaches, a company’s failure to carry the responsibility for safeguarding students’ transcripts is hardly reassuring.

Surprisingly, in 2011, the Education Department again loosened the safeguards for student records by modifying the key terms “education programs” and “authorized representatives” to permit greater disclosure of student data. Under FERPA, “authorized representatives” of the U.S. comptroller general, the secretary of education, and state educational authorities may access student records to audit or evaluate federally supported “education programs.” The new regulations broadly define “education programs” to encompass programs not only focused on “improving academic outcomes” but also related to “bullying prevention, cyber-security education, and substance abuse and violence prevention” regardless of whether the program is administered by an educational agency or institution. And previously, “authorized representatives” were exclusively entities over which educational authorities had “direct control, such as an employee or a contractor of the authority.” Now, autho-
rized representatives can be any individual or entity that educational authorities select as an authorized representative. 12

By amplifying “education programs” and “authorized representatives,” the Education Department has taken very narrow circumstances that permit the disclosure of education records and has expanded those circumstances to the point that the disclosure of student data is no longer the exception but is increasingly becoming the rule.

Wider Disclosure, Fewer Safeguards
In January 2012 the Education Department, working with the Office of Science and Technology Policy (OSTP), announced the Education Data Initiative, a public-private partnership that collects and disseminates student data. 13 The Education Data Initiative involves several public-sector entities that gather student data and then disclose it to the private sector. For instance, under the Education Data Initiative, federal student aid websites feature “a ‘MyData’ download button to allow students to download their own data [and] . . . share . . . with third parties that develop helpful consumer tools.” 14

Although the Education Department and OSTP are pushing for an increase in aggregating data, these agencies do not explicitly describe how the Education Data Initiative will protect students’ privacy or safeguard against security breaches. The absence of a breach policy is ironic in light of security breaches that affected an Education Department website in October 2011. The Education Department’s Federal Student Loan Servicing website (http://www.mycedaccount.com) exposed “the personal financial details of as many as 5,000 college students” to borrowers who had logged into the website. Although the department shut down the website while it resolved the problem and “notified and offered credit monitoring services” to those affected, 15 this is an unfortunate example of the Education Department’s failure to establish appropriate technical safeguards that ensure confidentiality of personal records as required by the Privacy Act, which, like FERPA, is another landmark federal privacy law. 16

The Education Data Initiative reflects a growing trend with student data: government agencies are taking personal information that students are required to provide, skirting federal regulations, and turning student data over to the private sector with few, if any, safeguards for privacy and security.

Conclusion
In February 2012, the Electronic Privacy Information Center (EPIC) filed suit against the Education Department regarding the changes to the federal student privacy regulations under FERPA. At EPIC, we believe the agency exceeded its authority when it revised the federal privacy law to make student data more available. And we disagree with the agency’s decision to loosen the key definitions that help safeguard student records. Our case, EPIC v. Department of Education, is pending in federal district court in Washington, D.C.

When FERPA was enacted almost forty years ago, Congress made it clear that students’ personal information should not be made widely available. Congress was particularly concerned that if student records fell into the hands of private parties, these records could hurt students later in life when, for example, students were seeking jobs. Although the pressures have increased over the years to access student data, Congress and the Education Department should work to strengthen student privacy rights and provide oversight on student data disclosure.

Notes

Marc Rotenberg (rotenberg@epic.org) is Executive Director of the Electronic Privacy Information Center (EPIC) in Washington, D.C. He teaches Information Privacy Law at Georgetown University Law Center. Khaliah Barnes (barnes@epic.org) is Administrative Law Counsel at EPIC.

© 2013 Marc Rotenberg and Khaliah Barnes. 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/).
MOOCs: Get in the Game

In July 2012, John V. Lombardi (someone I have admired for nearly three decades and came to know personally during our shared time in Louisiana) wrote that investing in Massive Open Online Courses (MOOCs) as the “next big thing” in higher education is largely about institutions trying to “seek visibility and preeminence to validate their claims of significance and advertise their association with the latest educational trends and enthusiasms.” Lombardi was spot-on in assessing that these “free” courses are by no means free and that many questions remain to be answered. However, I would argue that there is value in institutions staking their proverbial toe in the MOOC waters, as my own institution—and scores of others—have done via Coursera and other MOOC efforts.

In the EDUCAUSE 2012 session “MOOCs: The Coming Revolution,” which I presented with Coursera’s co-founder Daphne Koller, I opened my portion by emphasizing that the current IT-driven disruption is not actually about information technology but is, rather, about pedagogy. I’ll take this opportunity to state my view again: the focus of this disruption should be on teaching and learning. However, I believe that there is value in having the IT organization take an active role in helping the institution to embrace this change, even going so far as to move onto “point” for change. I believe the move by my institution, the University of Maryland (UMD), into Coursera perfectly illustrates why institutions—and IT leaders and organizations—should get involved with some form of MOOC initiative at this time. I see two primary reasons, along with a third, more fundamental reason beyond those two.

First, there are opportunities available. The current “name-brand” MOOC entries are still interested in developing content-providing partners: Coursera has expanded twice, growing from its original four partners to thirty-three as of December 2012; edX has grown from the Harvard-MIT founders to include the University of California–Berkeley, the University of Texas System, Georgetown University, and Wellesley College.

Second, this is what leading institutions do. As UMD President Wallace Loh said, we stick our necks out (in the metaphor of our mascot, the terrapin). Presidents and provosts at all levels of institutions are, if not under pressure, certainly being encouraged by their boards, legislatures, donors, and others in the community to take action. They are also being pushed by their own faculty, who are eager to give MOOCs a try.

Third, and more fundamentally important, actively participating may be a better way to learn than simply watching from afar. I believe we’re at a point of change, where information technology not only is useful for automating the status quo in teaching and learning but can be truly transformative in the evolution of pedagogy (perhaps rapidly) to a “flipped classroom” model. By actively engaging in these start-up efforts, we bring the lessons directly to our campuses and, more important, to our faculty and our academic staff who must assume leadership for how our colleges and universities embrace online and blended education.

Institutions that take a responsible approach and make a reasonable investment of time and resources to get a few courses into a MOOC environment can benefit by seeing things up-close and personal. The debate about all aspects of MOOCs is only getting started; it will become even more robust as more data on experiences emerges and as more people join the discussion. Being “in the game,” rather than simply watching from the sidelines, provides a better set of insights to inform that robust debate. We will be able to use our own experiences to judge what our unique institutions do rather than basing our decisions on the experiences and views of others who are not us.

Although UMD is still in the early days with MOOCs, I can share our experience to date:

- **Contracting with the provider.** Working out our contract with Coursera was not overly challenging. I’ll credit that to the flexibility of Coursera and its understanding of the concerns of higher education institutions. The agreement is not secret, with many of them available for perusal online, including UMD’s.

- **Choosing the course offerings.** Recruiting faculty and selecting courses was a task of winnowing to a reasonable number from a large set of quality offerings (rather than hunting for volunteers). Today, we have a steady flow of faculty who are interested in being “in the next wave,” and our first Coursera offerings won’t debut until early spring of 2013. In fact, at this time, our biggest challenge involves how to deftly and sensitively say “No, not just now, maybe later” to an increasingly eager and ambitious number of faculty.

- **Preparing the courses.** Here, we are still gaining knowledge. The first to-do with Coursera involved creating the “course landing pages” (like “trailers” for a coming-attraction movie). This was revealing on many levels, including the need to establish better video support services (we used our University Relations studio and talent) and also support for our faculty on “being ready for their close-up.” What we’re only now starting to understand is how much goes in to actually preparing the course “modules”: Coursera’s structure encourages faculty-led “imparting” sessions of 12 to 15 minutes, augmented with associated assignments, discussions, and assessment.

By actively engaging and embracing MOOCs, institutions can help define what MOOCs mean to higher education and what they might become. In the long run, I believe this will be good for students and the institutions who lead the way.
exercises to create learning modules delivered via its online platform in a synchronous approach.

The challenges we’ve exposed in our process have illuminated a broader set of questions:

- **What is this new approach to pedagogy?** There is a definite need for a better understanding on the part of faculty of what the new paradigm of pedagogy means to them. Many faculty may come to the discussions thinking of the current model of IT enablement in blended and online learning, which is largely one of using information technology (learning management systems and their many attendant parts) to automate the process of course delivery, with little impact in the classroom or in the curriculum. Coursera’s approach is challenging this model and is opening up what may be a renaissance in faculty members’ approach to teaching (and students’ approach to learning) in a 21st-century IT environment. What we have here is a new way to apply an old IT term—Business Process Reengineering—to the fundamental business of our universities.

- **MOOCs are “it,” right?** The focus on this “next big thing” has often been viewed as a search for what might be called the Highlander Model—that is, there can be only one, and MOOCs are the one. Of course, MOOCs are just a single tool in the online education toolbox. We need to stop thinking in terms of a MOOC revolution and instead think in terms of teaching and learning revolution, of which MOOCs are just one (currently very disruptive) element.

- **Do we need another administrator?** A critical challenge is the shortness of time to act. Events are transpiring quickly, and the revolution in online education may not patiently wait for the evolution of our institutions in terms of how our faculty and scholarly support structures respond. Several leading institutions have decided that there is value in a senior-level position (e.g., vice provost, special assistant to the president), not necessarily to take ownership of all facets of online education but to coordinate the process by which an institution can quickly evolve its collaborative activities.

- **What is the role of information technology?** Many observers, including me, argue that MOOCs are not really about information technology and are not something that should be led by the IT organization. That said, as the debate rages in the academic divisions and the cabinets of our institutions, the IT organization is well positioned to take a “recon” role—that is, to establish a beachhead, or a pilot, or a furtive first experiment or discussion. I’m sure I’m not the only CIO to be called by the president or provost when the MOOC events began to unfold. This makes sense: those of us in information technology are well positioned to contribute in turbulent times. Our challenge will be how to do so and then how to relinquish the point position when the academic divisions are ready to assume their rightful place leading this charge into our future.

In his blog post, Lombardi advises colleges and universities to watch and wait until the leading institutions have experimented and developed a viable strategy that can deliver value (from MOOCs) to their communities. He further cautions that governing boards should exercise caution in demanding trendy responses from their institutions and that it is often best to observe, study, and evaluate and to perform a cost-benefit analysis before jumping onto the next big thing. This is sound advice for many, to be sure.

But I would argue that we can better do these things—including learning about these new environments, platforms, and processes so as to apply their value in the broader blended and online initiatives we undertake, well beyond MOOCs—by taking an active role rather than simply watching and waiting. We should be in this game, and actively so. Our higher education institutions are about creating, sharing, and preserving knowledge. By taking an active role in the MOOC revolution, we are fulfilling the first, to the benefit of the second.

### Notes


2. See, for example, Doug Guthrie, “Jump Off the Coursera Bandwagon,” *Chronicle of Higher Education* (Commentary), December 17, 2012.


Brian D. Voss is Vice President and Chief Information Officer at the University of Maryland.

© 2013 Brian D. Voss. The text of this article is licensed under the Creative Commons Attribution-NoDerivs 3.0 Unported License [http://creativecommons.org/licenses/by-nd/3.0/].
Feature

Cloud Security: Cloud Now or Cloud How?
Highlights of the sometimes sprawling yet always interesting Shel Waggener–Fred Cate debate, including a bit of color and passion. »

Case Study

Dream On: An Acting Class Explores the Digital Landscape
An acting class added digital technology to investigate how it might enhance character interpretation and explore whether it could play an integral part in the performance without becoming the performance. »

Good Ideas

Concentrating Class: Learning in the Age of Digital Distractions
Exploring technology’s impact on their learning and their lives ended with many students further enamored of technology rather than concerned by its disruptions. »

Peer-Reviewed

Building the E-University: Transforming Athabasca University
Reinventing itself as an online university required sweeping changes in culture, effective leadership, and faculty/staff flexibility. Today, real change is visible. Here’s how they did it. »

Editors’ Picks for 2012

Changing the Game in Higher Ed IT
Education changes lives and societies, but can we sustain the current model? In this video, find out how new models and new technologies allow us to rethink many of the premises of education. »
Need to **squeeze** more value out of your IT budget?

Technology leaders are increasingly asked to provide more services while maintaining costs. Jenzabar, a leading provider of software, strategies, and services for higher education, can help you to get the most from your technology spending. Contact us today to:

+ Assess Total Cost of Ownership and what it means for your campus
+ Support student success without over-spending
+ Identify opportunities for cost-effective support

Visit [jenzabar.com/tco](http://jenzabar.com/tco) for insights you can use.
Pearson is leading the movement to bring digital learning technologies, content, and services to higher education.

BREAK THROUGH
To a new world of learning

By powering online learning experiences, we’re helping to accelerate college and career readiness and ultimately drive student success. Pearson’s learning environments supply everything from customized, concept-to-completion learning management systems to digital content repositories – all provide effective platforms to develop, optimize and expand your institution’s current blended and online offerings.

To learn more about Pearson’s online learning solutions, visit pearsononlinelearning.com

© 2013 Pearson. All Rights Reserved.

@PearsonLS