Strange Bedfellows or a Marriage Made in Heaven?

By Michael Corn and Jane Rosenthal

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.
Strange Bedfellows or a Marriage Made in Heaven?
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. 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). Security has existed much longer as a business component, since it involves not just the technical component but also the physical and administrative areas. Most major higher education institutions have a dedicated security staff. Generally tracking the growth of the Internet over the last thirty years, security has matured as a professional field of practice and study, with degrees, conferences, certifications, and an expanding commercial market of products and services. Meanwhile, the compliance function in the educational sphere had evolved over the prior decades as the requirements of law and ethical behavior came together within such far-ranging areas as human and animal subject research, environmental health and safety, and other areas that have laws and regulations that must be met by organizations.

So why does privacy matter to an organization? In 2006, Lauren Steinfeld, chief privacy officer at the University of Pennsylvania, and Kathleen Archuleta, former chief privacy officer for the University of Colorado System, listed the following roles of the chief privacy officer in any organization:

- Champions the issue of privacy within the organization
- Leads or monitors major compliance initiatives around global, federal, and local privacy laws
- Assists in assessing privacy-related risks throughout the organization and promotes strategies to mitigate these risks through the development and implementation of infrastructure, standards for the collection, use, and sharing of personal information, vendor requirements, training, and other appropriate mechanisms
- Participates as a key team member in responding to and managing incidents resulting in the loss or potential

---

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.

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."

**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. 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.

**Privacy, Security, and Compliance in Conflict**
As those of us who work in security and compliance know, there is a strong delineation between the two areas. We may be completely satisfied that a third party—for example, Amazon—runs a very tight ship regarding security within its storage environment. Yet without contractual assurances, a higher education institution cannot agree to the storing of regulated data (e.g., FERPA or HIPAA data) within that environment. This leads to various cases that lie at the boundaries between privacy, security, and compliance. We will discuss three: IP address tracking and web browsing; mobile device management/application technologies; and security cameras and video technologies.

**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-
ing the information at risk, versus the user’s inherent privacy rights to avoid these intrusions on a personally owned device.

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,
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.13 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.14 Finally, although many employees understand that the workplace and the equipment are provided by their employer, the work environment is nevertheless, for many
Privacy, Security, and Compliance: Strange Bedfellows or a Marriage Made in Heaven?

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
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.

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 cleaving 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.¹⁵

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.

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 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/protecting.


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 $100,000 per month: http://www.pcicomplianceguide.org/pci/faqs.php.

© 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/).