COSMOS
Navigate the Compliance Universe

CEP Magazine - February 2022
The privacy 'evolution to revolution' in higher education

By Decanda M. Faulk, Esq., RN, CIPP/US


Decanda M. Faulk

Decanda M. Faulk (df@faulk-associates.com) is General Counsel of US Post-Acute Service Solutions in Union, New Jersey, and Founder of Faulk & Associates in Newark, New Jersey, USA.

Protecting the personal information of students and employees is an ongoing concern for higher education institutions (HEIs), such as colleges and universities, that rely on modern information systems to store essential business and resource data. The security of these information systems must be adeptly handled by applying both technical and behavioral controls. However, the security culture in HEIs remains challenging because of the reportedly lax attitude of employees (particularly faculty, staff, leadership, and governing bodies) toward the HEIs' resources and their obligations to maintain their privacy and security. In addition, the ease and comfort with which students use technology, specifically social media platforms, increase the vulnerabilities of campus information systems and exposure to malware.

Thus, balancing traditional legal and regulatory compliance with contemporary threats to privacy (e.g., data protection, data governance) and cybersecurity are top priorities for HEIs. Yet navigating the legal and regulatory landscape when managing privacy and cybersecurity threats is becoming more challenging. The legal and compliance departments of many HEIs in the United States may not be as familiar with the complexities of data privacy laws and regulations or how to comply with these laws as other sectors. Today, the growth and expansiveness of data privacy laws and risks of ransomware attacks, which pose a threat of significant reputational harm and subject HEIs to penalties for noncompliance, make robust cybersecurity and privacy programs an important compliance endeavor for HEIs.

While security has been around much longer than privacy in HEIs and, therefore, is better established in most HEIs than privacy, this situation is changing. With the numerous pieces of privacy legislation that went into effect in 2020 and 2021, as concern over data breaches, use of data-tracking people's behavior, and biometric surveillance technologies became part of the national discourse, the privacy posture of HEIs is shifting. As privacy concerns grow, HEIs are taking a more deliberate approach to scaling up their privacy and cybersecurity efforts.

The privacy revolution in higher education

Although HEIs are falling behind other sectors in terms of privacy, some appointed privacy officers and security officers after the enactment of the Health Insurance Portability and Accountability Act (HIPAA) of 1996. For example, the University of Pennsylvania was the first HEI to appoint a chief privacy officer (CPO) in 2001.[1] Eighteen years later, the university reportedly had seven full-time privacy staff members.

Over the past decade, as questions and concerns over privacy have become front and center in the public eye, HEIs have been forced to shift positions on privacy beyond the Family Educational Rights and Privacy Act

(FERPA). Today, more HEIs are creating designated CPO roles, and CPOs are now taking on ever-evolving responsibilities, such as working closely with chief information security officers (CISOs) and legal, compliance, and procurement departments. These are encouraging signs, and such actions demonstrate the marriage between privacy and security with respect to collecting, storing, and protecting the voluminous data HEIs are responsible for handling and maintaining.

Notwithstanding some HEIs not having the resources to hire both dedicated CPOs and CISOs, HEIs' recognition of the importance of privacy and privacy oversight beyond FERPA compliance (typically directed to other departments in HEIs, e.g., the registrar's office, the security office) is prompting them to add privacy issues to the agendas of existing committees, such as those for compliance, audits, policy, risk, governance, data stewardship, security, IT, transparency and accountability, physical security, and surveillance. Some HEIs have even added committees dedicated to addressing privacy not only for students but also for faculty and staff. Although subject to applicable laws and regulations, an HEI can generally take any approach it deems appropriate to develop its privacy program. Although some programs are more mature than others, the privacy initiatives of several HEIs began with policy statements and documents that demonstrate an understanding of the relationship between privacy and security and, specifically, how privacy and security domains and objectives are separate.

In 2018, several universities put in place early stage working groups to direct campus efforts on the European Union's General Data Protection Regulation. At that time, their goal was to identify affected systems and processes. In 2019, it was predicted that most HEIs would have privacy officers in the next five to seven years. Reportedly, the number of CPOs is rising and has increased slowly over the years. However, it is still more common for HEIs to have a CISO than a CPO.

Of the many examples that make the case for strong cybersecurity and privacy hygiene, the Accellion case best illustrates why adopting a strong privacy and cybersecurity posture is prudent and essential for HEIs. Vulnerabilities in the IT security company's file transfer software were exposed when it was exploited by cybercriminals in December 2020.[2] Several HEIs were victims of the data breach connected to the vulnerabilities in the file transfer software sold by Accellion.[3] According to reports on the technology news website Gizmodo, files were discovered on the dark web containing sensitive information from several universities: Stanford University; the University of Maryland, Baltimore; the University of Miami; the University of California, Merced; the University of Colorado; and Yeshiva University.[4]

Data files of the affected HEIs were shared on a website called Clop, whose users are known to share snippets of stolen information and demand a ransom in return for not publishing the rest of the stolen data. "Clop has posted data relating to multiple [HEIs], most, if not all, of which have already confirmed their breaches were Accellion-related."[5] Clop published the data from the Accellion breach on a staggered basis and continued to expose new victims, which suggested more HEIs may have been affected.