DATA PROTECTION BASICS: A PRIMER FOR COLLEGE AND UNIVERSITY COUNSEL

JOHN L. NICHOLSON AND MEIGHAN E. O'REARDON*

INTRODUCTION

American colleges and universities are subject to significant regulation with respect to how they collect, store, and use personal information they compile. United States federal laws provide a fragmented, "sectoral" approach to data-privacy protection, offering separate laws protecting students' rights through the Family Educational Rights and Privacy Act ("FERPA"),[1] patients' rights through the Health Insurance Portability and Accountability Act ("HIPAA"),[2] as well as personal financial information

* John L. Nicholson is Counsel and Meighan E. O'Reardon is an Associate with Pillsbury Winthrop Shaw Pittman LLP's Global Sourcing Practice and Privacy Group. Both are based in the firm's Washington, DC, office and can be contacted at john.nicholson@pillsburylaw.com and meighan.oreardon@pillsburylaw.com, respectively. The authors would like to thank Ann Chang for her assistance with this article.

1. Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g (2006) [hereinafter FERPA].

2. Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1996) [hereinafter HIPAA] (codified as scattered sections

through the Gramm-Leach-Bliley Act ("GLBA").[3] In addition to these federal laws, institutions may be required to comply with various state laws related to the protection of personal information, including requirements that range from regulating the collection and use of information to data-breach-notification provisions to restricting the use of students' personal information for credit card marketing.[4] As if those requirements were not enough, various campus business operations may be required to comply with the Payment Card Industry Data Security Standards ("PCI DSS").[5]

For educational institutions with foreign students and international campuses, international regulations, such as the European Union's directive regarding the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (the "EU Directive")[6] and Canada's Personal Information Protection and Electronic Documents Act,[7] impose restrictions on the transborder transfer of personal data. Colleges and universities should also be aware of the efforts underway in the Pacific Rim countries to adopt the Asia-Pacific Economic Cooperation's ("APEC") Privacy Framework.[8] New and evolving data-privacy protections in South America and the Middle East are also important to understand as educational institutions expand their campuses to these regions.[9]

This article offers college and university legal counsel an overview of the current status of the various privacy laws, regulations, and standards that could apply to their institutions, as well as some insight into current developments related to these laws.[10] The article opens by providing an

---

of U.S.C. titles 29 and 42 (2006)).

3. Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–09 (2006) [hereinafter GLBA].

4. *See* discussion *infra* Part I.E.

5. Security Standards Council, Payment Card Industry Data Security Standard (PCI DSS) Requirements and Security Assessment Procedures, v. 1.2.1, Req. 3 (Oct. 2008), http://www.pcisecuritystandards.org/security_standards/pci_dss_download.html (last visited Oct. 14, 2009).

6. Council Directive 95/46, The Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L281) 31 (EU) [hereinafter EU Directive].

7. Personal Information Protection and Electronic Documents Act, 2000 S.C., ch. 5 (Can.) [hereinafter PIPEDA].

8. *See* APEC Privacy Framework, http://www.apec.org/apec/news___media/fact_sheets/200908fs_privacyframework.html (last visited Oct. 14, 2009).

9. *See, e.g.*, Law No. 25.326, Oct. 4, 2000, [No. 29.517] B.O. 1 (Argentina's law for the protection of personal data); Lei No. 9.507, de 12 de noviembro de 1997, D.O. 220: 26025, nov. 1997 (Brazil's habeas data law); Law No. 17.838, Oct. 2004 (Uruguay's law for the protection of personal data); DIFC Data Protection Law of 2007, Law. No. 1, Jan. 2007.

10. The purpose of this article is not to provide an in-depth coverage or analysis of any of these laws or regulations. Readers experienced at dealing with these areas will recognize that there are nuances and exceptions too detailed to be covered in a survey article, and each of these areas have been the subject of numerous detailed articles (and

overview of applicable U.S. privacy authorities and continues by exploring the practical applications of these legal authorities to many of the traditional activities of colleges and universities. The article then goes on to explore some of the international privacy considerations facing institutions with foreign students and campuses. Finally, the conclusion outlines steps that college and university counsel can take to comply with the myriad of federal, state, and international laws and standards that apply to educational institutions.

I. OVERVIEW OF U.S. DOMESTIC PRIVACY AUTHORITIES APPLICABLE TO COLLEGES AND UNIVERSITIES

The U.S. has no single definition of protected personal information; the definitions that exist are provided in the specific statutes and regulations to which they apply. Unlike other countries and the European Union, Congress has been reluctant to enact comprehensive legislation protecting all of an individual's private information. Instead, federal privacy laws are focused on a few industries and sectors where it has been deemed that disclosure of personal information could result in significant harm to the individual. These industries include health care, with the passing of HIPAA in 1996[11] and its recent modification by the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"), part of the American Recovery and Reinvestment Act of 2009,[12] and financial institutions, with the enactment of GLBA in 1999.[13] Additionally, and most relevant to colleges and universities, Congress enacted FERPA in 1974 to protect personal information contained within education records.[14] FERPA and its supporting regulations have been amended a number of times since being adopted, most recently in 2008.[15]

Due to the lack of comprehensive federal legislation, states have assumed a role in data protection, forcing organizations to comply with similar, but slightly varying, laws across the different jurisdictions where such organizations may be held accountable. Data-breach-notification laws provide the best example of the variation among states. Many states have started to apply their data protection laws broadly to organizations that

---

books) in their own right.

11. *See* HIPAA, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as scattered sections of U.S.C. titles 29 and 42 (2006)).

12. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009) (parts codified as scattered sections of U.S.C.).

13. GLBA, 15 U.S.C. §§ 6801–09 (2006).

14. *See* FERPA, 20 U.S.C. § 1232g (2006).

15. *See id.*; United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (PATRIOT Act), Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified as scattered sections of U.S.C. (2006)); *see, e.g.*, Family Educational Rights and Privacy, 34 C.F.R. §§ 99.3, 99.5 (2009).

have only modest interaction with the particular state and its residents.[16] California's data-breach-notification law, as discussed in Part I.E.1, was one of the first state laws to impose one state's data protection authorities on individuals and businesses outside its borders. To date, the extra-territorial reach of these state laws has not been tested, primarily due to the proliferation of other similar notification laws.

Non-governmental data protection standards are also becoming increasingly relevant to colleges and universities. One of the most significant for educational institutions is PCI DSS. Colleges and universities should be familiar with PCI DSS and some of the other data protection standards[17] as many of these industry best practices are now becoming codified in laws that apply to educational institutions.

Up to this point, the U.S. Congress, states, and other regulatory bodies have been reactive, rather than proactive, in passing data-privacy laws, but this may be changing as states become more active in protecting the personal information of their citizens.[18] For colleges and universities, the

16. See discussion Part I.E *infra*.

17. *See, e.g.*, International Organization for Standardization, *ISO/IEC 27001: 2005 Information Security Management Systems – Requirements* (Oct. 15, 2008), http://www.iso.org/iso/catalogue_detail?csnumber=42103 (last visited Oct. 14, 2009); *ISO 2007/2005 Code of Practice for Information Security Management* (Apr. 22, 2008), http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297 (last visited Oct. 14, 2009); National Institute of Standards and Technology, Computer Security Division, *Minimum Security Requirements for Federal Information and Information Systems* (Mar. 2006), *available at* http://www.csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf.

18. For example, the Video Privacy Protection Act of 1988 was passed after reporters gained access to titles of videos rented by Supreme Court nominee Robert Bork, which led some critics to joke that in the United States "video rentals are afforded more federal protection than are medical records." Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Data Privacy Standards*, 25 YALE J. INT'L L. 1, 25 (2000); *see also* Trevor Shaw, Dir. Gen., Audit & Review, Office of the Privacy Comm'r of Can., International Perspectives on Privacy & Security, Address to the Dep't of Homeland Sec. Data Privacy & Integrity Comm. (Sept. 28, 2005), http://www.privcom.gc.ca/speech/2005/sp-d_050928_ts_e.asp (last visited Oct 14, 2009). The murder of Hollywood actress Rebecca Shaffer by a stalker who got her address from the California Department of Motor Vehicles led to the enactment of the U.S. Driver's Privacy Protection Act of 1994. Francesca Bignami, *Transgovernmental Networks vs. Democracy: The Case of the European Information Privacy Network*, 26 MICH. J. INT'L L. 807, 814 (2005). Consumer concerns over misuse of their phone numbers by telemarketers led to the Do-Not-Call Implementation Act of 2003, establishing the Do-Not-Call Registry administered by the Federal Trade Commission. *See* Do-Not-Call Implementation Act of 2003, Pub. L. No. 108-10, 117 Stat. 557 (2003). Similarly, growing concerns from Internet Service Providers (ISPs) and consumers regarding e-mail spam resulted in the Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM) of 2003. *See* CAN-SPAM Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (2003) (codified at 15 U.S.C. §§ 7701–13 (2006)).

result is a variety of continually evolving legal authorities that may now apply to campus activities. The most relevant legal authorities for colleges and universities are outlined in the remainder of this section. This patchwork of federal and state privacy laws and standards intersects with the traditional activities of colleges and universities in a number of unique ways. The various campus activities implicated by many of the privacy authorities are also discussed in this Section. Naturally, an educational institution's specific activities will dictate the degree to which these and other state and federal authorities may apply, and those activities and each of these privacy authorities need to be monitored and evaluated as they change over time.

A. Family Educational Rights and Privacy Act (FERPA)

FERPA currently governs the privacy of students' education records in the United States. Originally enacted in 1974, Congress has amended FERPA nearly a dozen times.[19] FERPA regulates the access to, amendment of, and disclosure by schools of education records.[20] All schools receiving funds from any U.S. Department of Education program must comply with FERPA, and parents or eligible students either over the age of eighteen or attending post-secondary schools are protected by FERPA.[21] It is important to note, however, that FERPA is an education-record-privacy law, not a student-privacy law. For the purposes of FERPA, "education records" means any information that is recorded in any way (but does not include personal knowledge) that (1) directly relates to a student (i.e., it contains personally identifiable information about the student) and (2) is maintained by an educational agency or institution or by a party acting for the agency or institution.[22] FERPA covers education records for any individual who is or has been in attendance at the educational institution, regardless of whether such attendance has been in person or via correspondence or the internet.[23]

FERPA provides that post-secondary level educational institutions may not disclose or provide unauthorized access to personally identifiable student information from the education records maintained by that

19. *See* 20 U.S.C. § 1232g (2006).

20. *See id.*; 34 C.F.R. § 99.3 (2009).

21. Under FERPA, parents have the right to control disclosure of and access to, and seek amendment of, education records until the student turns eighteen or attends a post-secondary institution. Once an eligible student possesses FERPA rights, there are only very limited circumstances under which a parent may, at the institution's discretion, access the eligible student's records (*e.g.* if the parents claim the eligible student as a dependent under the federal tax regime). *See* Family Educational Rights and Privacy, 34 C.F.R. §§ 99.10–99.12 (2009).

22. 20 U.S.C. § 1232g(a) (2006).

23. *Id.*

institution without either the signed, written consent of the student[24] or as otherwise specifically authorized by FERPA.[25] To provide consent, the student must be informed of the records that may be disclosed, the purpose for which they may be disclosed, and the person or classes to whom they may be disclosed.[26] In general, an education record may be disclosed only on the condition that the information will not be redisclosed without the student's consent, and the recipients may only use the disclosed information for the specified purpose.[27] The disclosures authorized directly by FERPA include disclosure to other school officials with a "legitimate educational interest," to other schools to which a student is transferring or has transferred, and to authorities performing audits or enforcing relevant state or federal laws.[28] There is also an exception to the disclosure requirement rooted in the United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (PATRIOT Act) that allows the U.S. Attorney General, through an *ex parte* court order, to collect and use education records to investigate and prosecute acts of terrorism.[29]

In addition to the above exceptions, schools may also disclose information from education records pursuant to a subpoena or court order. A school may also disclose, among other things, any information that constitutes "directory information."[30] According to the current rules under FERPA, directory information can include, at the institution's discretion, an eligible student's name, address, telephone number, date and place of birth, honors and awards, dates of attendance, and certain similar items of information.[31]

As part of complying with FERPA, an educational institution must make a record of each request for education records, and each disclosure of such education records, and maintain it with the relevant education record. In addition, educational institutions must allow students to inspect and review their own education records within forty-five days of the student's request. The institution is not required to provide the student with copies of the

24. *See* 34 C.F.R. § 99.30.

25. *See id.* §§ 99.5, 99.31.

26. *See id.* § 99.30.

27. *See id.* § 99.33.

28. 20 U.S.C. § 1232g.

29. *See id.* Exemptions to FERPA with potential implications for foreign students on U.S. campuses include the PATRIOT Act, Pub. L. No. 107-56, title IV, subtitle B, § 416, 115 Stat. 272 (2001) and section 641(a) of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, 8 U.S.C. § 1372(a) (2006). In addition to other FERPA exemptions implemented by the PATRIOT Act, the U.S. Attorney General is permitted to access student records and information collected through the Student Exchange and Visitor Information System ("SEVIS") by educational institutions on foreign students, including name, address, and visa classification.

30. 20 U.S.C. § 1232g.

31. *Id.*

records unless circumstances effectively prevent the student from exercising his or her right to inspect and review without receiving the copies. This right does not include financial aid records of the student's parents or confidential letters of recommendation to which the student has waived the right of access. If the student's records include personally identifiable information about any other student, the information must be redacted or the other student must consent. FERPA also enables a student to request amendment of any records containing information that is inaccurate, misleading, or in violation of the student's privacy rights. The student cannot force the institution to make the amendment; if the request is denied, however, the student must have an opportunity for a hearing and the ability to include a statement about the desired amendment with the disputed record.[32]

FERPA also requires educational institutions to provide an annual privacy notice that must include a statement of students' rights to inspect and review their own education records and seek amendment of inaccurate or misleading records, along with the procedures for doing so; to consent to most disclosures; and to file a complaint with the U.S. Department of Education related to their education records.[33]

In 2008, the Department of Education amended and adopted several FERPA regulations.[34] The changes sought to incorporate prior legislative amendments and two Supreme Court FERPA decisions, as well as to address disclosure concerns raised by the tragic shootings that occurred at Virginia Tech in 2007.[35] The changes, which focused primarily on clarifying privacy rules governing the release of confidential student information in health and safety emergencies, took effect on January 8, 2009.[36]

In particular, the changes clarify the existing right of parents to access information about eligible students; the scope of the term "school official" defining to whom a disclosure may be made without prior written consent; and permissible redisclosures of student information by third parties.[37] In

32. *See* Family Educational Rights and Privacy, 34 C.F.R. §§ 99.20–99.22 (2009).

33. For an example of a "model notice," see United States Department of Education, *Model Notification of Rights Under FERPA for Postsecondary Institutions*, http://www.ed.gov/policy/gen/guid/fpco/ferpa/ps-officials.html (last visited Oct. 14, 2009).

34. *See* Family Educational Rights and Privacy, 73 Fed. Reg. 74,806–855 (Dec. 9, 2008) (codified at 34 C.F.R. §§ 99.1–99.67 (2009)).

35. Bureau of National Affairs, *Privacy Law Watch*, "Education Department Issues Amendments to FERPA Privacy Requirements in Final Rule" (Dec. 10, 2008).

36. *See id.*; Alyson Klein, *Ed. Dept. Releases New Rules on Privacy*, EDUC. WK. (Bethesda, MD), Jan. 7, 2009, at 4; s*ee also* Elizabeth Bernstein, *Education Department Reworks Privacy Regulations*, WALL ST. J., Dec. 9, 2008, *available at* http://online.wsj.com/article/SB122878222728889843.html?mod=googlenews_wsj.

37. *See* FERPA, 20 U.S.C. § 1232g(b) (2006).

addition, the new regulations expand the scope of information traditionally covered under the law to include "biometric information," which includes such things as fingerprints, retina and iris patterns, DNA sequences, and so forth.[38]

The revised regulations also provide greater flexibility for institutions to disclose private student information to various parties in certain health- and safety-emergency situations. While institutions were previously permitted to disclose confidential student information without consent if necessary to protect the health and safety of the student or other individuals, the regulations previously stated that this exception must be "strictly construed."[39] This limiting language has been removed and the new regulations permit institutions to make such disclosures "if there is an articulable and significant threat to the health or safety of a student or other individuals."[40] However, under these new regulations, institutions that rely upon the health and safety exception to justify the disclosure of student information must now also record the threat that formed the basis for the disclosure as well as the identity of the parties to whom the disclosure was made.[41]

Another significant change to the regulations was the revision of the definition of what information qualifies as "personally identifiable information." Prior regulations defined personally identifiable information to include any information "that would make the student's identity easily traceable."[42] The new definition removes this language and provides a more objective standard for determining when information is properly "de-identified." Under the new definition, personally identifiable information is "other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty," which could include indirect information, such as an address or place of birth, that can be used to identify an individual.[43] The revised regulations also prohibit the use of Social Security numbers and, in some cases, student identification numbers in student directories.[44] The regulations further clarify that when responding to "targeted" requests for information, an educational institution may not release information from a student's education records if the institution has reason to believe that the person requesting the information knows the identity of the student to whom the

38. *See id.* § 1232g.
39. *Id.*
40. *Id.*
41. *Id.*
42. *Id.*
43. *Id.*
44. *See* 34 C.F.R. § 99.37 (2009).

record relates.[45] These changes were made to provide greater clarity in responding to requests related to identifiable students or requests made in the wake of highly publicized incidents within the school environment.[46]

Additional significant changes encompassed by the amendments include: including outside contractors, volunteers, and other third parties conducting business on behalf of a school in the definition of "school officials" with whom data may be shared (so as to permit schools to disclose information pursuant to an outsourcing relationship); requiring schools without physical or technological access restrictions to adopt policies for controlling access; and allowing schools to share protected information with other schools whenever the sharing is related to the student's enrollment or transfer.[47]

Finally, the new regulations expand the scope of the FERPA enforcement procedures. In particular, the regulations broaden the scope of materials that the Family Policy Compliance Office (FPCO), the Federal body authorized by the Secretary of Education to conduct FERPA investigations, can require an educational institution to provide during the course of an investigation. [48]

B. Gramm-Leach Bliley Act (GLBA)

GLBA is recognized as a financial industry privacy authority; however, U.S. colleges and universities are also potentially subject to GLBA. To the extent that an educational institution engages in lending funds (whether to students or faculty), collecting loan payments, or facilitating the process of applying for financial aid, the institution may be considered a "financial institution" subject to GLBA regulation.[49]

There are two categories of compliance requirements under GLBA: (1) the Privacy Rules, and (2) the Safeguarding Rules.[50] The Privacy Rules govern the use and disclosure of personal nonpublic information ("NPI") while the Safeguarding Rules set forth requirements with respect to the manner in which financial institutions are expected to protect NPI in their custody or control.[51] Any institution of higher learning that complies with FERPA and the regulations promulgated pursuant to FERPA is considered to be in compliance with the Privacy Rules. However, there is no similar accommodation for institutions of higher learning in connection with the

45. *See id.* § 99.3.
46. *See* 73 Fed. Reg. 74,806 (Dec. 9, 2008).
47. Family Educational Rights and Privacy, 34 C.F.R. §§ 99.1–99.67 (2009); s*ee also* Bernstein*, supra* note 36.
48. *See* 34 C.F.R. §§ 99.1–99.67 (2009).
49. *See* 15 U.S.C. § 6809(3) (2006).
50. 15 U.S.C. §§ 6801(a)–(b).
51. *See id.*

Safeguarding Rules. The Safeguarding Rules require financial institutions to develop, implement, and maintain a comprehensive security program consisting of administrative, technical, and physical safeguards to protect against the unauthorized use or disclosure of NPI.[52] However, the GLBA Safeguarding Rules provide financial institutions some flexibility when developing and administering security programs. Notably, the Safeguarding Rules include a reasonableness standard, which means that the security measures required will be dependent on the institution in question and the NPI collected.[53] Colleges and universities that may be subject to GLBA should evaluate their information security policies in light of this reasonableness standard and be able to justify decisions and trade-offs made.

C. Health Insurance Portability and Accounting Act (HIPAA)

HIPAA is a complex framework of privacy laws and regulations that govern the safeguarding and privacy of individuals' health information.[54] U.S. colleges and universities should be aware of HIPAA due to its application to college and university health centers, medical schools, and hospitals. HIPAA is the federal statute that provides for privacy and standardized transmission of health records and information.[55] This statute specifically applies to health plans, health care clearinghouses, and regulation-specified providers (called "Covered Entities") that transmit health records.[56] HIPAA protects "individually identifiable health information," which includes demographic information collected from an individual that is either created by a health care provider or relates to treatment of an individual.[57] The lead agency for HIPAA management and enforcement is the Department of Health and Human Services ("HHS").[58]

Like GLBA, HIPAA includes both a Privacy Rule and a Security Rule.[59] The Privacy Rule requires Covered Entities to have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information ("PHI") whereas the Security Rule outlines the framework for organizations to exercise the privacy requirement and

52. *Id.* § 6801(b).

53. 16 C.F.R. § 314.3 (2009) (stating that safeguards "shall be reasonably designed" to insure the security and confidentiality of customer information).

54. *See* HIPAA, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as scattered sections of U.S.C. titles 29 and 42 (2006)).

55. *Id.* § 261.

56. *Id.* § 1172.

57. *Id.* § 1177.

58. *See* Dep't of Health and Human Servs., HIPAA Privacy Rule Enforcement, http://www.hhs.gov/ocr/privacy/hipaa/enforcement (last visited Oct. 14, 2009).

59. *See generally* HIPAA.

secure PHI.[60] Notably, the Security Rule applies to both paper and electronic PHI and is aimed at protecting against any reasonably anticipated threats to the security of PHI (including uses and disclosures of PHI that are not permitted or required).[61] Colleges and universities should be most concerned with the HIPAA Security Rule since HHS, through the Centers for Medicare and Medicaid Services ("CMS"), has recently begun to step up enforcement. In 2008, Providence Health Services became the first entity to be fined for non-compliance with the HIPAA Security Rule.[62] The health provider was fined $100,000 for failing to provide adequate safeguards for PHI on backup media and laptops.[63]

Until recently, there has been a great deal of confusion over the boundaries of HIPAA and FERPA related to student health records. In response to the Virginia Tech incident, the Department of Health and Human Services and the Department of Education issued guidance (the "Joint Guidance") in November 2008 to clarify the intersection between these two privacy laws.[64] The Joint Guidance explains that colleges and universities providing healthcare to students are accurately categorized as health care providers under HIPAA. If, however, the only health records the school maintains fall within the definition of education records or "treatment records"[65] under FERPA, a HIPAA exemption applies and FERPA governs.[66] Notably, if the educational institution's health clinic provides healthcare services to non-students (e.g., staff, faculty, the public, etc.) the information maintained for those patients is governed by HIPAA.[67] Additionally, the Joint Guidance highlights that university hospitals are

60. *Id.* § 1173.

61. *Id.*

62. *See* Thompson, *Providence to Pay First HIPAA Fine of $100,000*, EMPLOYEE BENEFITS NEWSBRIEFS, Jul. 18, 2008, http://www.thompson.com/public/newsbrief.jsp?cat=BENEFITS&id=1853 (last visited Oct 16, 2009).

63. *Id.*

64. United States Dep'ts of Educ. and Health and Human Servs., Joint Guidance on the Application of the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to Student Health Records (Nov. 2008), *available at* http://www.ed.gov/policy/gen/guid/fpco/doc/ferpa-hippa-guidance.pdf [hereinafter Joint Guidance].

65. "Treatment Records" are excluded from the definition of education records and are defined as records on a student who is eighteen years of age or older or who is attending an institution of post-secondary education, which are made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his professional or paraprofessional capacity, or assisting in that capacity, and which are made, maintained, or used only in connection with the provision of treatment to the student, and are not available to anyone other than persons providing such treatment, except that such records can be personally reviewed by a physician or other appropriate professional of the student's choice. 20 U.S.C. § 1232g(a)(4)(B)(iv) (2006); 34 C.F.R. § 99.3 (2009).

66. Joint Guidance, *supra* note 64.

67. *See id.*

distinct from university health clinics and HIPAA typically governs all patients treated at such hospitals regardless of their status as students.[68] This distinction is due to the fact that university hospitals provide healthcare services without regard to the patient's status as a student and are not providing care on behalf of the educational institution.[69]

As mentioned above, HIPAA was recently modified as part of the American Recovery and Reinvestment Act of 2009.[70] In addition to a number of provisions addressing the development, implementation, and use of electronic health records ("EHRs"), the HITECH Act substantially modified the HIPAA Privacy Rule and Security Rule to provide additional privacy and security rights and requirements. In general, the effective date of these new provisions is February 17, 2010 (i.e., twelve months from the date of enactment of the HITECH Act).[71]

Prior to the passage of the HITECH Act, Covered Entities were required to enter into specialized confidentiality agreements with third parties that perform business functions on behalf of Covered Entities (e.g., outsourced service providers, subcontractors and consultants, collectively "Business Associates").[72] Business Associates were not specifically required to comply with HIPAA, but, rather, were only subject to a claim of contractual breach if they failed to comply with the terms of their contract with the Covered Entity (the "Business Associate Agreement").[73] Under the HITECH Act, Business Associates are directly subject to HIPAA's privacy and security requirements, including being required to implement administrative, physical, and technical safeguards, as well as HIPAA's criminal and civil fines and penalties.[74] Also, the HITECH Act extends the reach of the HIPAA requirements by providing that organizations that provide data transmission of PHI to Covered Entities or their Business Associates, such as health information exchange organizations, regional health information organizations, or vendors that contract with a Covered Entity to offer a personal health record ("PHR") to patients as part of its EHR, are considered Business Associates and must have a Business Associate Agreement with such Covered Entities.[75] However, these PHR vendors and related entities are subject to regulations promulgated by the

68. *See id.*

69. *See id.*

70. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009) (some sections codified as scattered sections of U.S.C.).

71. *See id.*

72. *See* DECHERT, LLP, HEALTHCARE REFORM UPDATE, *available at* http://www.dechert.com/library/hru_02-26-09.pdf.

73. *See id.*; *see also* American Chiropractic Association, Business Association Agreement, http://www.acatoday.org/pdf/businessassociate.pdf (last visited Oct. 14, 2009).

74. *See* §§ 13401, 13404, 123 Stat. at 260, 264.

75. *See id.* § 13408.

U.S. Federal Trade Commission ("FTC") rather than those promulgated by HHS.[76]

The HITECH Act provides numerous restrictions and obligations with regard to PHI. Among other things, an individual may also request that his or her PHI not be disclosed to his or her health plan if the individual pays for medical care in full.[77] Covered Entities must, to the extent practicable, disclose only the "minimum necessary" information to accomplish the intended purpose for such disclosure.[78] In addition, an individual may request an accounting of the disclosures of his or her electronic PHI, as contained in the EHR, over the preceding three years.[79] Therefore, educational institutions that are Covered Entities using EHRs may want to begin accounting for disclosures as early as January 1, 2011, depending on when they acquire and begin to use an EHR. Under the HITECH Act, the sale of PHI by a Covered Entity or a Business Associate is prohibited without patient authorization except in certain specified circumstances.[80]

The HITECH Act also provides new data-breach-notification obligations that require Covered Entities and Business Associates to report most security breaches directly to affected individuals.[81] In general, notices provided under these provisions must be sent within sixty days, [82] which may be a short period of time to investigate and mitigate a data breach. Covered Entities and Business Associates are also required on an annual basis to notify the Secretary of HHS of all data breaches, and must provide notice of any breach of more than 500 records immediately.[83] These notice provisions apply to "unsecured" PHI[84] which the Secretary of HHS has defined as information that has not been rendered "unusable, unreadable, or indecipherable to unauthorized individuals," either through encryption or destruction.[85] As required by the HITECH Act, on April 27, 2009, the

76. *See* FTC Health Breach Notification Rule, 74 Fed. Reg. 42962, 42962–82 (April 25, 2009) (to be codified at 16 C.F.R. pt 318), http://www.ftc.gov/os/fedreg/2009/august/090825healthbreachrule.pdf.

77. *Id.* § 13405(a).

78. *Id.* § 13405(b). The HITECH Act specifies that the government will provide new guidance with regard to what constitutes the "minimum necessary" for disclosures under the Privacy Rule within eighteen months after the enactment of the HITECH Act (i.e. by August 17, 2010).

79. *Id.* § 13405(c).

80. *Id.* § 13405(d).

81. *Id.* § 13402.

82. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 13402(d)(1), 123 Stat. 115, 261 (2009) (§ 13402 codified at 42 U.S.C. § 17932).

83. *Id.* § 13402(e).

84. *Id.* § 13402.

85. Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements Under Section 13402 of Title XIII of the American Recovery and Reinvestment Act of 2009, 74 Fed. Reg.

Secretary provided guidance regarding acceptable technologies for securing PHI, and will update that definition on an annual basis.[86]

As a result of these changes, educational institutions that are Covered Entities should take steps to review their current privacy and security practices to confirm that they are in compliance with the law, update their privacy and security policies, develop a data-breach-notification policy that complies with the HITECH Act (and state law counterparts), and update any Business Associate Agreements to reflect the new obligations under the HITECH Act. Because of the recent nature of the HITECH Act and the number of requirements that have yet to be defined or clarified, educational institutions should pay close attention to developments in this area.

D. Red Flag Rules

Colleges and universities are likely to be subject to one or more of the three new rules on Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transactions Act of 2003 (the "Red Flag Rules").[87] These rules implement sections 114 and 315 of the Fair and Accurate Credit Transactions ("FACT") Act, which specifically call for "establishment of procedures for the identification of possible instances of identity theft" and "reconciling addresses."[88]

The Red Flag Rules are not limited to financial organizations traditionally regulated by the federal government. In fact, because the FTC is one of the six agencies that issued the Red Flag Rules, a broad cross-section of organizations must comply.[89]

The Red Flag Rules contain three requirements:

1. Debit and credit card issuers must develop policies and procedures to assess the validity of a request for a change of address that is followed closely by a request for an

19006, 19006–10) (to be codified at 45 C.F.R. pt. 160, 164), http://edocket.access.gpo.gov/2009/pdf/E9-9512.pdf.

86. *Id. See also* 42. U.S.C. § 13402(h).

87. Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003 (FACT Act), 72 Fed. Reg. 63,718, 63,719–721 (Nov. 9, 2007) (codified as scattered sections of 12 C.F.R. and 16 C.F.R. pt. 681). The rules have been promulgated by the Department of Treasury Office of the Comptroller of the Currency, the Federal Reserve System, the Federal Deposit Insurance Corporation, the Department of Treasury Office of Thrift Supervision, the National Credit Union Administration, and the Federal Trade Commission.

88. Fair and Credit Transactions Act of 2003 (FACT Act), Pub. L. No. 108-159, §§ 114, 315, 117 Stat. 1952, 1960, 1996 (2003) (codified as elements of 15 U.S.C. §§ 1681c, 1681m (2006)).

89. *See* 72 Fed. Reg. at 63,727–728.

additional or replacement card.[90]

Most colleges and universities now have some type of payment card system in place that allows students, faculty, and staff to pay for goods and/or services at multiple locations on campus, and in some cases even at off-campus venues. While this shift to a cash-free environment has eased certain aspects of student life, the result is an activity that may implicate the Red Flag Rules, since institutions engaging in such activities may fall within the definition of "creditor."[91] If the program in question is more like a credit card, for which the user is billed by the educational institution "after delivery," or if use of the card debits money from a personal account established by the student with the educational institution, then the educational institution is likely to be considered a creditor.[92] If the program in question is more like a stored-value card (where the usable amount is stored on the card itself, not in a separate account that is debited as a result of the transaction), the educational institution is probably not a creditor.[93] This provision could implicate student IDs that also can be used as part of a national debit card network, such as Visa or MasterCard.[94] Educational institutions that offer such a payment card program will need to develop policies and procedures for handling student (or other user) changes of address and requests for new cards.

2. Users of consumer reports must develop reasonable policies and procedures to apply when they receive notice of an address discrepancy from a consumer reporting

---

90. *Id.* at 63,733.

91. *See* FTC Enforcement Policy: Identity Theft Red Flags Rule, 16 C.F.R. § 681.2 (2008) (FACTA defines "creditor" the same way as the Equal Credit Opportunity Act (ECOA): any entity that "regularly extends, renews, or continues credit; any [entity] that regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who is involved in the decision to extend, renew, or continue credit." 15 U.S.C. § 1691(a) (2006). The ECOA definition of "credit" includes a right granted to defer payment for any purchase. Thus, any entity who delivers a service or product for which the consumer pays after delivery is a "creditor." *See id.*).

92. *See* 72 Fed. Reg. at 63,718.

93. *See id.* at 63,734 (where the definition of "debit card" specifically does not include stored-value cards).

94. The Red Flag Rules also applies to "financial institutions." 15 U.S.C. § 6827(4)(A) defines a "financial institution" as "any institution engaged in the business of providing financial services to customers who maintain a credit, deposit, trust, or other financial account or relationship with the institution." Transaction accounts include checking accounts, negotiable order of withdrawal accounts, savings deposits subject to automatic transfers, and share draft accounts. *See* 12 U.S.C. § 461(b)(1)(C) (2006). Colleges and universities that offer students the option of having their student ID also operate as a Visa or MasterCard debit card should coordinate with the bank through which such services are offered to ensure that the bank has an adequate Identity Theft Prevention Program in place.

agency.[95]

This provision will apply to educational institutions when they use consumer credit reports to conduct credit or background checks on prospective employees or applicants for credit.

3. Financial institutions and "creditors" holding "covered accounts" must develop and implement a written identity theft prevention program for both new and existing accounts.[96]

Organizations subject to the Red Flag Rules are categorized as either financial institutions or creditors.[97] The term "creditors" includes any person or organization that regularly extends, renews, or continues credit; who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit.[98] Since the definition is so broad, colleges and universities that have payment card programs described above or that extend credit in their bookstores or through meal plans or other campus lending programs could be held to comply with the Red Flag Rules. In fact, the FTC stated "[w]here non-profit and government entities defer payment for goods or services, they, too, are to be considered creditors."[99]

Activities that could cause educational institutions to be considered "creditors" under the Red Flag Rules may include:

- Participating in the Federal Perkins Loan program;
- Participating as a school lender in the Federal Family Education Loan Program;
- Offering institutional loans to students, faculty, or staff; or
- Offering a plan for payment of tuition throughout the semester rather than requiring full payment at the beginning of the semester.

Under the Red Flag Rules, if an institution is a creditor, the institution must determine if any of its extensions of credit are "covered accounts."[100] Under the Red Flag Rules, a "covered account" is a consumer account that involves multiple payments or transactions, such as a loan that is billed or

95. 16 C.F.R. § 681.2 (2009).
96. *Id.*
97. *See* 72 Fed. Reg. at 63,719.
98. 15 U.S.C. § 1691a(e) (2006).
99. FTC Business Alert, *New "Red Flag" Requirements for Financial Institutions and Creditors Will Help Fight Identity Theft*, June 2008, http://www.ftc.gov/bcp/edu/pubs/business/alerts/alt050.shtm (last visited Oct. 14, 2009).
100. 72 Fed. Reg. at 63,754.

payable monthly.[101] The Red Flag Rules and the FTC's guidance on it indicate that covered accounts include certain types of arrangements in which an individual establishes a "continuing relationship" with the enterprise, including billing for previous services rendered.[102] Any type of account or payment plan that involves multiple transactions or multiple payments in arrears (as opposed, for example, to payment of a semester's tuition in full in advance), however, likely is a "covered account."[103]

The Red Flag Rules mandate that financial institutions and creditors develop and implement a written "Identity Theft Prevention Program" (a "Program") to identify relevant "red flags" (patterns, practices, and specific activities that signal possible identity theft) and incorporate them into the program; detect the red flags that the Program incorporates; respond appropriately to detected red flags to prevent and mitigate identity theft; and ensure that the Program is updated periodically to reflect changes in risks. [104] The board of directors (or appropriate board committee) of the financial institution or creditor must approve the initial written Program.[105] Board approval may be necessary only for the first written Program if the board delegates to appropriate senior management further responsibility.[106] The new identity theft and address discrepancy rules took effect on January 1, 2008, and, originally, entities under FTC jurisdiction had until November 1, 2008, to review their current practices, develop their Programs, and implement the necessary changes before full compliance was expected.[107] However, due to repeated requests from organizations for more time, and, most recently, a request from Congress, the FTC has delayed the compliance date at total of four times and it is currently June 1, 2010.[108]

The path to developing a Program will vary and will depend in large part on each institution's existing fraud and compliance programs and experience with identity theft. The Red Flag Rules permit flexibility in the scope of the Program, depending on the creditors' activities and level of identity theft risk associated with the relevant covered accounts. In

101. *Id.* at 63,721.

102. *Id.*

103. *Id.* at 63,719.

104. *Id.* at 63,720.

105. *Id*. at 63,718.

106. Press Release, Federal Trade Commission, FTC Will Grant Three-Month Delay of Enforcement of "Red Flags" Rules Requiring Creditors and Financial Institutions to Adopt Identity Theft Prevention Programs (April 30, 2009), http://www.ftc.gov/opa/2009/04/redflagsrule.shtm (last visited Oct. 16, 2009).

107. 72 Fed. Reg. at 63,718. *See* Press Release, Federal Trade Commission, FTC Announces Expanded Business Education Campaign on the 'Red Flags' Rule, (July 29, 2009), www.ftc.gov/opa/2009/07/redflag.shtm (last visited Nov. 11, 2009).

108. FTC Moves 'Red Flag' Deadline to June Following Request from House Lawmakers,Privacy Watch (BNA) No. 209 (Nov. 2, 2009).

developing a Program, educational institutions should assess whether they have "covered accounts," as described above. Such analysis and an initial risk assessment will enable the educational institution to identify types of accounts the Program must address and identify the risks the institution faces, based in large part on the institution's previous experiences with identity theft. An appropriate identity theft prevention program may not need to be detailed or complex, but should be written, duly approved, and implemented.

Appendix J to the Red Flag Rules, the "Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation,"[109] provides an outline for developing a Program. The document provides 26 sample "red flags" that could be incorporated into an educational institution's Program. Examples include:

- Address discrepancy;
- Name discrepancy on identification and insurance information;
- Presentation of suspicious documents;
- Personal information inconsistent with information already on file;
- Unusual use or suspicious activity related to a covered account;
- Notice from customers, law enforcement, or others of unusual activity related to that covered account.[110]

In addition to addressing relevant red flags, an educational institution subject to the Red Flag Rules must "train staff, as necessary" to implement the Program effectively.[111] According to the preamble to the Red Flag Rules, institutions need train only "relevant staff" and only insofar as necessary to supplement other training programs.[112] The Red Flag Rules also require covered institutions to exercise "appropriate and effective oversight" of service provider arrangements.[113] According to the preamble to the Red Flag Rules, this provision is intended to remind covered institutions that they remain responsible for compliance with the rule even if they outsource operations to a third party.[114] Educational institutions that outsource operations that would be impacted by the Red Flag Rules should review existing contracts to determine whether the service provider is obligated to have policies and procedures that would be sufficient to comply with the Red Flag Rules, and future service contracts should include specific requirements to comply with the Red Flag Rules.[115]

---

109. *Id.* at 63,754.
110. *Id.*
111. *Id.* at 63,731.
112. *Id.* at 63,718.
113. 16 C.F.R. § 681.1 (2009).
114. 72 Fed. Reg. at 63,723.
115. A general obligation to comply with laws may not be sufficient, since, frequently, such provisions are drafted in a manner that requires the service provider to comply with all laws and regulations applicable to the service provider's business and

E. Key State Laws

States have also assumed a prominent role in regulating data privacy and security, thus necessitating educational institutions' compliance with another layer of laws. A significant element of many of these state data-privacy laws is that many states have started to impose their data protection laws on "foreign" entities. This means that a physical presence in the state is often not required for an institution to be subject to the law. The two most popular standards for being covered under a particular state's data-privacy laws include "doing business" in that particular state and holding a resident's personal information.[116] The "doing business" standard is the more traditional standard applied by states when determining whether the state's laws apply to out-of-state entities.[117] As mentioned in the introductory section, the extended reach of laws applying simply due to the data held by an entity has yet to be challenged. If, however, an educational institution's marketing and recruiting practices were to rise to the level of "doing business" in a state with such an extended reach statute, the question might never need to be reached by a court. Assuming that the laws are valid and enforceable, for colleges and universities, this means being subject to state laws and regulations based on the geographic makeup of their applicant pool and student body, and not merely the physical location of the institution. Some of the more significant state laws applicable to educational institutions are outlined in this section, but colleges and universities should institute a compliance program that actively monitors developments in state and local data-privacy laws.

1. California

California was one of the first states in the country to regulate privacy, and today it has the most comprehensive framework of state-level privacy laws in the country.[118] California privacy laws are also some of the most stringent in the country, requiring safeguards for a wide variety of personal

---

operations. Unless a service provider is also held to be a creditor or financial institution, such a general compliance obligation would not require the service provider to comply with the Red Flag Rules.

116. *See* Christopher Wolf and Timothy P. Tobin, *Privacy, Data Security and Outsourcing*, *in* 93 PRACTICING L. INST.: PATENTS, COPYRIGHTS, TRADEMARKS, AND LITERARY PROP. COURSE HANDBOOK SERIES 57, 63–64 (2007); Jennifer Chandler, *Negligence Liability for Breaches of Data Security*, 23 BANKING & FIN. L. REV. 223, 226 (2008).

117. *See generally* Mary Twitchell, *Why We Keep Doing Business with Doing-Business Jurisdiction*, 2001 U. CHI. LEGAL F. 171 (2001).

118. *See generally* CAL. CONST. art. 1, § 1 ("All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.").

information.[119] As such, most of the privacy laws in existence in other states encompass some aspect of the California privacy framework. Understanding California's privacy laws offers insight into the breadth of state privacy laws in existence throughout the country.

California privacy laws cover a broad set of subject areas, including: arrest records, cable television subscriber information, check printing, computer crimes, credit card numbers, credit reporting, debt collection processing, motor vehicle records, e-commerce, employment records, false impersonation, financial records, invasion of privacy, investigative consumer reports, insurance information, medical records, police records, school records, sex offender registration, stalking, tax records, telephone records and solicitation, video store lists, voter registration records, and wiretapping.[120] A notable component of California's privacy laws is that some of the laws reach beyond California state borders. Many of the state's privacy laws apply to any entity that stores a California resident's information or transacts business with a Californian, regardless of where that entity is located.[121] While the enforceability of this extended reach has yet to be tested, for colleges and universities, this means that, unless the institution wants to risk being the test case for the enforceability of the provision, as long as one student on campus is from California, the institution may be subject to California privacy laws with regard to that person's information. The unfortunate consequence of laws drafted in this way is that the most stringent law becomes the *de facto* standard, since the alternative is for institutions to implement multiple policies and procedures depending on the home residence of their prospective and actual students, parents, donors, faculty, and alumni.

2. Minnesota

In 2007 Minnesota was the first state to codify elements of the PCI DSS.[122] In response to the TJX Companies, Inc., credit card data breach, which compromised over 45 million cardholders' information, Minnesota enacted the Plastic Card Security Act.[123] This law imposes strict liability

119. The California Office of Privacy Protection is a valuable resource for counsel who wish to acquire a broader understanding of the various types of state privacy laws in existence. Cal. Office of Privacy Prot., http://www.oispp.ca.gov/consumer_privacy/default.asp (last visited Oct. 14, 2009).

120. Cal. Office of Privacy Prot., *Privacy Laws,* http://www.oispp.ca.gov/consumer_privacy/laws/#two (last visited Oct. 14, 2009).

121. *See, e.g.*, California's Online Privacy Protection Act of 2003, CAL. BUS. & PROF. CODE §§ 22575–79 (West 2008) (requiring website operators who collect personally identifiable information on California residents to post a privacy policy on their websites describing their data practices, regardless of the operator's location).

122. *See* discussion *infra* Part I.F.

123. H.F. 1758, 2007–08 Leg., 85th Sess. (Minn. 2007); s*ee also* Joseph Pereira, *Breaking The Code: How Credit-Card Data Went Out Wireless Door – In Biggest*

on any entity that retains credit or debit card security data.[124] Any organization conducting business in Minnesota after August 1, 2007, may not keep "card security code data, the PIN verification code number, or the full contents of any track of magnetic stripe data" after a transaction is authorized.[125] In the event of a security breach, the Plastic Card Security Act imposes strict liability, meaning entities will be liable regardless of whether the security breach was the result of negligence or some other factor such as poor security.[126] The law also holds organizations responsible for violation of the data retention requirements by their service providers.[127]

Where security data has been retained in violation of the law and a data breach occurs, organizations will be liable to any financial institution for the costs incurred to remediate and recover from the breach.[128] Entities will also be liable for damages that financial institutions pay to injured cardholders as a result of the security breach.[129] The costs imposed by this new Minnesota law are in addition to any other remedies that are already available to financial institutions.[130]

Even organizations not physically located in Minnesota potentially face liability under this law, since the statute applies to anyone *conducting business* in Minnesota.[131] Since many transactions with and on college and university campuses, including application fees paid online and bookstore, cafeteria, and tuition payments, are conducted using credit cards, the Minnesota Plastic Card Security Act likely applies to many educational

---

Known Theft, Retailer's Weak Security Lost Millions of Numbers, WALL ST. J., May 4, 2007, at A1.

124. MINN. STAT. ANN. § 325E.64(2) (West Supp. 2008).

125. *Id.*

126. *Id.*

127. *Id.*

128. *Id.*

129. MINN. STAT. ANN. § 325E.64(3) (West Supp. 2008).

130. *Id.*

131. Determining whether a particular merchant is conducting business in Minnesota for purposes of this statute is a fact-specific inquiry. Rather than list activities that *are* considered conducting business in Minnesota, the Minnesota Foreign Corporation Act identifies a number of activities that *are not* considered to be conducting business in the state. *See* MINN. STAT. ANN. § 303.03 (West Supp. 2008). In particular, the statute notes that a foreign corporation will *not* be transacting business in the state if it is "conducting an isolated transaction completed within a period of 30 days and not in the course of a number of repeated transactions of like nature." *See id*. § 303.03(h). Furthermore, Minnesota's long-arm statute asserts personal jurisdiction over foreign corporations causing injury within the state, subject to a pair of exceptions probably included for due-process reasons. *See id*. § 543.19. Merchants conducting business with Minnesotans will need to determine whether their conduct constitutes conducting business within Minnesota and whether any data breach would constitute an injury there. Given the current public sensitivity to the consequences of data breaches and the potential cost of violations of the Plastic Card Security Act, merchants may wish to err on the side of caution and comply with the Minnesota requirements.

institutions' activities. In particular, if any students on a campus are from Minnesota, the Plastic Card Security Act could apply. The Act may likewise apply if there are repeat transactions conducted within Minnesota's borders that rise to the level of "conducting business" in Minnesota. Colleges and universities that accept credit cards should already be working with their banks to comply with PCI DSS, regardless of whether they are covered by the Minnesota law. Institutions covered by the Minnesota law may limit their exposure under the law by taking the following steps: (1) educational institutions in, or that do regular business with residents of, Minnesota should confirm that they are not storing security card data in violation of the Minnesota law, including auditing their existing data retention policies and practices and updating them where appropriate; (2) existing contracts with service providers should be reviewed and updated to reflect the new data retention provisions. As appropriate, educational institutions should work with their third party providers to ensure compliance with the Minnesota law. Additionally, service provider contracts should include provisions to indemnify the merchant in cases where the service provider has breached the Plastic Security Card Act; and (3) any educational institution handling credit card data should regularly monitor PCI DSS updates and modify its security practices accordingly.

3. Massachusetts

Originally set to be phased in during 2009 and 2010, and now delayed to a single compliance date of March 1, 2010,[132] Massachusetts has released regulations, entitled "Standards for the Protection of Personal Information of Residents of the Commonwealth" ("the MA Regulations"), that establish data security standards for any entity that "own[s], license[s], store[s], or maintain[s] personal information about a resident of the Commonwealth of Massachusetts."[133] The purpose of the MA Regulations is to establish "minimum standards to safeguard personal information in both paper and electronic records."[134] Similar to many other state data protection laws, the MA Regulations apply broadly to businesses located outside of Massachusetts' borders. Even if an organization does not have a significant presence in the state, the MA Regulations may still apply if the

132. Press Release, Massachusetts Office of Consumer Affairs & Business Regulation, Patrick Administration's Final Data Security Regulations Filed and Take Effect March 1, 2010; State Received Notice of More than 1 Million Instances of Exposure in Two Years (Nov. 4, 2009), http://www.mass.gov/?pageID=ocapressrelease&L=1&L0=Home&sid=Eoca&b=pressrelease&f=20091104_idtheft&csid=Eoca (last visited Nov. 22, 2009).

133. 201 MASS CODE REGS. 17.01(1) (2009).

134. *Id.*

organization holds personal information about a Massachusetts resident.[135] As with other similar statutes, the enforceability of this extended reach has yet to be tested.

The MA Regulations govern both paper and electronic records and require entities to develop and implement a comprehensive, written information security program for personal information ("Program").[136] Each such Program must follow industry standards and include certain administrative, technical, and physical safeguards, as well as specific encryption requirements for electronic records containing personal information.[137] Under the MA Regulations, personal information includes a Massachusetts resident's first and last name, or first initial and last name in combination with any one or more of the following data elements: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any pin number or password.[138] The MA Regulations allow for tailoring each entity's Program based on the size and type of business, resources available to the business, amount of personal data stored, and need for security and confidentiality of the information.[139] Despite the flexibility granted under the MA Regulations, each Program must address certain activities defined in the MA Regulations.[140]

As mentioned above, the MA Regulations also include specific encryption requirements for any electronic transmission or storage of

---

135. *See id.*

136. The Regulations were adopted pursuant to chapter 93H, section 2 of the Massachusetts General Laws, which grants the Department of Consumer Affairs and Business Regulation the authority to adopt regulations that "safeguard the personal information of residents of the Commonwealth . . . ." This same law also grants the Supervisor of Records the authority to create similar rules and regulations applicable to Massachusetts Executive Offices. *See* MASS. GEN. LAWS. ch. 93H, § 2(b) (2008).

137. 201 MASS. CODE REGS. 17.03 (2008).

138. *Id.* 17.02.

139. *Id.* 17.03.

140. *Id.* These required activities include: designating employee(s) to maintain the Program; identifying and assessing the risks associated with electronic or paper records containing personal information; developing security policies for employees, including measures related to transport of personal information outside of the business' premises; imposing disciplinary measures for violations of the Program; preventing terminated employees from accessing records containing personal information; taking reasonable steps to verify that third-party service providers with access to personal information can provide adequate protections; limiting the amount of personal information collected; identifying records, media, and devices that contain personal information; applying reasonable restrictions on physical access to records containing personal information; monitoring and upgrading the Program to ensure that it is operating to prevent unauthorized access to personal information; reviewing the Program annually; and documenting actions taken in response to a breach of security and implementing post-incident reviews of such events. *Id.*

personal information.[141] The statute defines "encryption" to require the use of a 128-bit or higher algorithmic process, unless further defined by the MA Regulations.[142] Specifically, the MA Regulations require businesses storing or transmitting personal information to address the following in their Program: (1) user authentication protocols; (2) secure access control measures; (3) encryption of records that travel across public networks or wirelessly; (4) monitoring systems for unauthorized access; (5) encryption of personal information stored on portable devices; (6) updating firewalls and system security; (7) maintaining current virus protections; and (8) training for employees on computer security and protecting personal information.[143]

Most significantly, and in response to the countless data breaches involving lost or stolen laptops, the MA Regulations require businesses to encrypt personal information stored on portable devices.[144] Compliance with this requirement means equipping laptops and other similar devices with encrypted hard drives or installing data encryption software to protect sensitive data.

Finally, the MA Regulations require businesses to take a closer look at outsourcing arrangements. In particular, businesses must verify that third-party service providers with access to personal information about Massachusetts' residents have the capacity to protect that data.[145] This includes:

> 1. [t]aking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measure to protect such personal information consistent with these regulations and any applicable federal regulations; and 2. Requiring such third-party service providers by contract to implement and maintain such appropriate security measures for personal information.[146]

Massachusetts has provided a grace period for this element of the MA Regulations: until March 1, 2012, this requirement will not be applicable for contracts with an effective date prior to March 1, 2010. All contracts with effective dates after March 1, 2010, must comply with this element of

141. *Id.* 17.04(3), (5).

142. MASS. GEN. LAWS ch. 93H, § 1 (2008).

143. 201 MASS. CODE REGS. 17.04. Massachusetts is one of the states specifying a particular level of encryption. As computers become more powerful, this level of encryption will become easier to break, potentially requiring Massachusetts to increase the required level of encryption. Legally mandated higher levels of encryption, however, could place organizations at risk of violating the federal government's restrictions on exporting strong encryption technologies.

144. *Id.* 17.04(5).

145. *Id.* 17.03(3).

146. *Id.* 17.03(3)(f).

the MA Regulations.[147] In advance of the March 1, 2012, deadline, educational institutions that may collect Massachusetts residents' personal information should revisit existing outsourcing agreements to verify that compliance by their service providers is addressed.

Like many of the other state laws analyzed in this section, the Massachusetts law applies to colleges and universities that hold the personal information of a Massachusetts resident.[148] This means if the student body is comprised of any Massachusetts residents, compliance with the MA Regulations is warranted. Furthermore, colleges and universities with hospitals will want to examine how the Massachusetts law applies to their medical records, since medical records both at rest and in transit may require encryption, depending on the personal information contained therein (e.g., SSNs, credit card information, etc.). An important consideration regarding such records will be the extent to which existing electronic filing systems at such hospitals possess the capability to encrypt these records at rest. While the MA Regulations do not specifically include medical records, the fact that California[149] and certain other states have included medical records in the definition of personally identifiable information covered by those state's data-breach-notification laws means that Massachusetts' definition could easily be extended to include such information in the future.

4. Nevada

In 2008, Nevada enacted the "Restrictions on Transfer of Personal Information through Electronic Transmission" law, which became effective on October 1, 2008. [150] This law requires businesses in the state to encrypt all electronic transfers of a customer's personal information.[151] In Nevada, personal information includes the following unencrypted data: a person's first name or first initial and last name in combination with a social security number; driver's license number or identification card number; and/or account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to the person's financial account.[152] Significantly, the Nevada law also caps damages at $1,000 per customer for companies that comply with

147. Press Release, Massachusetts Office of Consumer Affairs & Business Regulation, Patrick Administration's Final Data Security Regulations Filed and Take Effect March 1, 2010; State Received Notice of More than 1 Million Instances of Exposure in Two Years (Nov. 4, 2009), http://www.mass.gov/?pageID=ocapressrelease&L=1&L0=Home&sid=Eoca&b=pressrelease&f=20091104_idtheft&csid=Eoca

148. 201 MASS. CODE REGS. 17.01.

149. CAL. CIV. CODE § 1798.3 (West 2009).

150. NEV. REV. STAT. § 597.970 (2008).

151. *Id.* The law excludes transfers using facsimile.

152. NEV. REV. STAT§ 603A.040.

the law but none-the-less suffer a data breach whereas those companies not complying face unlimited damages.[153]

Nevada is not the only state to mandating data security measures for personal information, but the Nevada encryption law is unique in mandating the use of a particular security measure, rather than "reasonable" security procedures. For example, the California Security Safeguard Act[154] requires a company that owns or licenses unencrypted "personal information" about California residents to implement and maintain "reasonable security procedures and practices" to protect such data. Texas[155] and Rhode Island[156]have enacted similar laws requiring companies to adopt procedures relating to information security, but neither of those are as specific as the Nevada encryption law.

While the Nevada encryption law is specific in requiring encryption, it is far less specific in several other areas. First, it does not define a "customer." Because neither the "personal information" nor the "customer" covered by the Nevada encryption law is limited with respect to a Nevada resident, the law could be interpreted as applying to a covered entity's transmission of "any personal information of a customer," regardless of where the customer resides. Second, the Nevada encryption law does not define the scope of "[a] business in this state" that is subject to the law. However, in addressing whether a foreign corporation had satisfied qualification requirements under Nevada law, the Nevada Supreme Court interpreted "doing business" in Nevada by approvingly citing a two-pronged standard: (a) the nature of the company's business in the state; and (b) the quantity of business conducted by the company in the state. In that case, the Court noted that assessing whether a foreign company is "doing business" in the state is "often a laborious, fact-intensive inquiry resolved on a case-by-case basis."[157] Like the Minnesota Plastic Card Security Act, the more interaction an educational institution has with individuals in Nevada, the more likely the institution will be to be subject to the Nevada encryption law.

On May 29, 2009, Nevada became the second state to require compliance with the PCI DSS when Nevada governor Jim Gibbons approved Senate Bill No. 227 (the "Amendment"), which amended Nevada's Security of Personal Information law.[158] The Security of Personal Information law

153. Ben Worthen, "*New Data Privacy Laws Set for Firms*," WALL ST. J. (October 16, 2008).

154. CAL. CIV. CODE § 1798.81.5(b).

155. TEX. BUS. & COM. CODE § 48.102(a) (2006).

156. R.I. GEN. LAWS § 11-49.2-2(2) (2006).

157. Executive Mgmt. Ltd. v. Ticor Title Ins. Co., 38 P. 3d 872 (Nev. 2002).

158. NEV. REV. STAT. §603A. For text of the amendment, see https://www.leg.state.nv.us/75th2009/Bills/SB/SB227_EN.pdf (last visited Sept. 9, 2009).

establishes requirements with respect to the destruction of records containing personal information;[159] the maintenance of reasonable security measures;[160] and the disclosure of security breaches impacting personal information.[161]

The Amendment provides that, if a data collector doing business in Nevada accepts a payment card in connection with a sale of goods or services, the data collector must comply with the current version of the PCI DSS.[162] Furthermore the data collector's compliance must not be later than the date set forth in the PCI DSS.[163] Under the Amendment, a data collector means any governmental agency, institution of higher education, corporation, financial institution or retail operator or any other type of business entity or association that, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates or otherwise deals with nonpublic personal information.[164]

The Amendment provides a safe harbor by stating that a data collector shall not be liable for damages for a breach of security if the data collector is in compliance with the PCI DSS *and* the breach is not caused by gross negligence or intentional misconduct.[165] Previously, an affected party would have recourse under various theories of law, with varying (and often undefined) standards of care or duty. Absent gross negligence or willful misconduct, an otherwise PCI-compliant merchant that suffers a data loss could arguably escape liability in Nevada.

The Amendment also expands on the obligations under the encryption laws by providing that organizations not involved in payment card transactions, but that transmit personally identifiable information outside of their own secure systems (either via electronic transmission or through the movement of physical data storage devices), must use encryption to ensure the security of the information. Unlike many other laws in this area, the amendment provides a very precise definition of what constitutes satisfactory encryption, "the protection of data in electronic or optical form, in storage or in transit, using: (1) An encryption technology that has been adopted by an established standards setting body, including, but not limited to, the Federal Information Processing Standards issued by the National Institute of Standards and Technology, which renders such data indecipherable in the absence of associated cryptographic keys necessary to

159. *Id.* at § 603A 200.

160. *Id.* at § 603A.210.

161. *Id.* at § 603A.220.

162. For the latest PCI DSS requirements, see https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml.

163. It should be noted that the current version of the PCI DSS does not provide compliance deadlines which are instead set by the individual payment card contracts.

164. NEV. REV. STAT. § 603A.030.

165. S.B. 227, 2009 Leg., 75th Sess. (Nev. 2009).

enable decryption of such data; and (2) Appropriate management and safeguards of cryptographic keys to protect the integrity of the encryption using guidelines promulgated by an established standards setting body, including, but not limited to, the National Institute of Standards and Technology."[166]

Although the effect of the Amendment with regard to PCI DSS compliance may be somewhat academic, since all entities covered by it are already contractually obligated to comply with the PCI DSS, this new law, in combination with Minnesota's Plastic Card Security Act, may inspire other states to legislate compliance with the PCI DSS.

5. State Data-breach-notification Laws

One of the most significant areas of state-level data-privacy regulation relates to data-breach-notification. As of the date of this article, at least forty-three states, the District of Columbia, and Puerto Rico have enacted data-breach-notification laws.[167] The primary purpose of these laws is to

166. *Id.*at Section 5(b).

167. Alaska (ALASKA STAT. §§ 45.48.010–.090 (2009)); Arizona (ARIZ. REV. STAT. § 44-7501 (Supp. 2008)); Arkansas (ARK. CODE ANN. §§ 4-110-101 to -107 (Supp. 2007)); California (CAL. CIV. CODE § 1798.92 (West 2009)); Colorado (COLO. REV. STAT. ANN. § 6-1-716 (West Supp. 2008)); Connecticut (CONN. GEN. STAT. § 36a-701(b) (West Supp. 2009)); Delaware (DEL. CODE ANN. tit. 6, §§ 12B-101 to -104 (Supp. 2008)); District of Columbia (D.C. CODE ANN. §§ 28-3851 to -3853 (LexisNexis Supp. 2009)); Florida (FLA. STAT. ANN. § 817.5681 (West 2006)); Georgia (GA. CODE ANN. §§ 10-1-910 to -912 (2009)); Hawaii (HAW. REV. STAT. § 487N-2 (LexisNexis Supp. 2009)); Idaho (IDAHO CODE ANN. §§ 28-51-104 to -107 (Supp. 2009)); Illinois (815 ILL. COMP. STAT. 530/1–30 (West 2008)); Indiana (IND. CODE § 4-1-11-1 to -10 (2005)); Iowa (IOWA CODE § 715C.1–C.2 (2008)); Kansas (KAN. STAT. ANN. § 50-7a02 (Supp. 2008)); Louisiana (LA. REV. STAT. ANN. § 51:3071–:3076 (Supp. 2009)); Maine (ME. REV. STAT. ANN. tit. 10, §§ 1347–1350-B (Supp. 2008)); Maryland (MD. CODE ANN., COM. LAW § 14-3501 to -3506 (LexisNexis Supp. 2008)); Massachusetts (2007 H.B. 4144, Chapter 82); Michigan (MICH. COMP. LAWS §§ 445.61–.77 (Supp. 2009)); Minnesota (MINN. STAT. ANN. §§ 325E.61, 325E.64 (West Supp. 2008)); Missouri (MO. REV. STAT. § 407.1500 (2009 H.B. 62)); Montana (MONT. CODE ANN. § 30-14-1701 to -1736 (2007)); Nebraska (NEB. REV. STAT. §§ 87-801 to -807 (2008)); Nevada (NEV. REV. STAT. §§ 603A.010–.920 (LexisNexis Supp. 2007)); New Hampshire (N.H. REV. STAT. ANN. §§ 359-C:19 to :21 (LexisNexis 2008)); New Jersey (N.J. STAT. ANN. § 56:8-163 (West Supp. 2009)); New York (N.Y. GEN. BUS. LAW § 899-aa (McKinney Supp. 2009)); North Carolina (N.C. GEN. STAT. § 75-65 (2007)); North Dakota (N.D. CENT. CODE § 51-30-01 to -07 (2005)); Ohio (OHIO REV. CODE ANN. §§ 1347.12, 1349.19, 1349.191–.192 (LexisNexis 2006)); Oklahoma (OKLA. STAT. tit. 74, § 3113.1 (West Supp. 2009)); Oregon (2007 S.B. 583, Chapter 759); Pennsylvania (73 PA. CONS. STAT. ANN. § 2303 (West 2008)); Puerto Rico (P.R. LAWS ANN. tit. 10, §§ 4051–4053 (Supp. 2007); Rhode Island (R.I. GEN. LAWS § 11-49.2-1 to -7 (2005)); South Carolina (S.C. CODE ANN. § 1-11-490 (Supp. 2008)); Tennessee (TENN. CODE ANN. § 47-18-2107 (Supp. 2008)); Texas (TEX. BUS. & COM. CODE ANN. § 521.053 (Vernon Supp. 2008)); Utah (UTAH CODE ANN. §§ 13-44-101 to -102, -201 to -202, -310 (Supp. 2009)); Vermont (VT. STAT. ANN. tit. 9 § 2430–2435 (2007)); Virginia (VA. CODE § 18.2-186.6 (2009));

establish guidelines for when entities that store personal information must inform individuals that their information has been compromised.

California's data-breach-notification law, which was the first law of its kind when adopted, now serves as the model for most other states.[168] California's law requires an entity to disclose the unauthorized access to unencrypted personal information if the breached personal information is coupled with the resident's first name, or first initial, and last name. The personal information that triggers the California statute includes: (1) Social Security number; (2) driver's license number or California Identification Card number; (3) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (4) medical information; or (5) health insurance information.[169] Under this law, notice must be given in "the most expedient time possible and without unreasonable delay."[170] Furthermore, if immediate notice is not offered, residents have a private cause of action for damages and injunctive relief.[171]

The goal of tying the notice requirement to the lack of encryption was intended to cause companies to encrypt their data, on the theory that organizations would rather spend the time and resources necessary to encrypt than risk disclosing a data breach to the public. This premise failed for two major reasons: (1) encryption of stored data proved more difficult than the legislators imagined, and (2) increases in computing power made it easier to break higher-level encryptions, meaning that data holders could not guarantee that encrypted information subject to unauthorized access had not been decrypted, thus requiring them to notify the data subjects despite the encryption.

While California has served as the model, there is still tremendous variation among each of the existing state data-breach-notification statutes. In particular, most data-breach-notice laws have divergent standards related to the type of breach that triggers notice, the timing requirements of notice, and exemptions for notification if encrypted data is compromised or other factors are satisfied. For example, Kansas, Colorado, and Delaware "have provisions exempting companies from disclosure if, upon investigation, it is believed that the stolen data will likely not be misused."[172] Some states'

Washington (WASH. REV. CODE § 19.255.010 (West Supp. 2007)); West Virginia (W. VA. CODE ANN. §§ 46A-2A-101 to -105 (LexisNexis Supp. 2009)); Wisconsin (WIS. STAT. ANN. § 895.507 (2006)); Wyoming (WYO. STAT. ANN. § 40-12-501 to -509 (2007)).

168. CAL. CIV. CODE §§ 1798.29, 1798.82 (West 2009).

169. *Id.* § 1798.29(e).

170. *Id.* § 1798.82(a).

171. *Id.* § 1798.84(a).

172. Philip Alexander, *Data Breach Notification Laws: A State-by-State Perspective*, INTELLIGENT ENTERPRISE, Apr. 9, 2007, http://www.intelligententerprise.com/showArticle.jhtml?articleID=198800638 (last

laws specifically exempt compromised redacted data from notification requirements.[173] For example, in Maryland, notice must first be given to the state attorney general or other regulator prior to notifying the data subject.[174] And, in a handful of states, including California, New York, Utah, Vermont, and Virginia, the data-breach-notification laws are not limited to electronic data, but also apply to data printed on paper.[175] These divergent data-breach-notification standards present compliance challenges, and the data-breach-notification provisions of the HITECH Act have made the situation even more complex. While national legislation to unify these standards has been debated,[176] and such action has been recommended by the FTC on several occasions, including in its recent report on Social Security Numbers and Identity Theft,[177] as of yet, no action on the national stage has been taken.

As numerous industry reports indicate, colleges and universities are particularly susceptible to data breaches. In fact, some studies indicate that one in four data security breaches involves educational institutions.[178] As such, for most colleges or universities, the question is not whether a data breach will happen, but when and how severe it will be. Colleges and universities must acquire expertise in complying with state data-breach-notification laws. In particular, having a data-breach response plan is a critical component of effectively responding to a breach and maintaining compliance with the various state laws implicated in the event of a breach.

At present, there is no seamless mechanism for data-breach-notification compliance. Since most data-breach-notification laws apply when a state resident's personal information has been compromised, colleges and universities will often face a situation where they must comply with multiple states' statutes. The geographic diversity of the institution's student body will dictate the applicable state laws. As such, many colleges and universities will opt to build a response plan that abides by the most stringent state law in effect at the time. However, notice requirements to the individuals whose personal information has been breached and to the

visited Oct. 14, 2009).

173. For example, Ohio's breach notification law is not triggered if data elements are redacted to four digits or otherwise made to be unreadable. OHIO REV. CODE § 1349.19 (LexisNexis 2009).

174. MD. CODE ANN., COM. LAW § 14-3504(h) (LexisNexis Supp. 2008).

175. *See* CAL. CIV. CODE § 1798.92 (2009); N.Y. GEN. BUS. LAW § 899-aa (Supp. 2008); UTAH CODE ANN. §§ 13-44-101 to -102, -201 to -202, -310 (Supp. 2009); VT. STAT. ANN. tit. 9 §§ 2430–2435 (2006); VA. CODE § 18.2-186.6 (2009).

176. *See* Data Accountability and Trust Act, H.R. 958, 110th Cong. (2007); Personal Data Privacy and Security Act of 2007, S. 495, 110th Cong. (2007).

177. *See* FED. TRADE COMM'N, SECURITY IN NUMBERS: SSNS AND ID THEFT (Dec. 2008), *available at* www.ftc.gov/os/2008/12/P075414ssnreport.pdf [hereinafter SECURITY IN NUMBERS].

178. Schools Account for 25% of Data Breaches, 8 THE PRIVACY ADVISOR, INT'L ASSOC. OF PRIVACY PROFESSIONALS, August 2008.

appropriate state regulatory authority will vary. Colleges and universities should clearly understand what personal information they are storing, how to best protect that information, and the requirements of the state that each of its students declares as his or her residence.

6. Social Security Number Protection

The use of Social Security numbers ("SSN") by colleges and universities raises a number of privacy considerations. Many educational institutions use SSNs as the primary means of tracking students, alumni, and donors. The recent amendments to FERPA prohibit publication of SSNs in student directories.[179] Many colleges and universities, however, still use SSNs for administrative purposes and store this information electronically.[180] For example, many colleges and universities used the SSN as a student identification number for a long time, and, for that reason, continue to track alumni using the SSN despite having changed to an assigned numbering system for new students.

The use of SSNs by organizations as a unique identifier or for administrative purposes has long raised identity-theft concerns. In May 2006, the President's Identity Theft Task Force was established and their work subsequently recommended (1) studying how the private sector uses consumer SSNs, (2) developing a deeper understanding of the relationship between SSNs and identity theft, and (3) exploring approaches to preserve beneficial use of SSNs while limiting availability and value to identity thieves.[181] The FTC issued its report in December 2008 and made several recommendations to strengthen the methods by which businesses authenticate customers, while reducing unnecessary display and transmission of SSNs.[182]

In addition to the attention that SSN use is receiving at the federal level, many states have enacted legislative protections for SSNs. All but eight[183] states, as well as the District of Columbia, currently have statutes that provide some form of SSN protection. These laws vary from comprehensive to very specific statutes that protect SSNs from disclosure.

---

179. 34 C.F.R. §§ 99.1–99.67 (2009).

180. *See, e.g.*, Northwestern Univ., Secured Handling of Social Security Numbers: Approved Uses of SSNs, *available at* http://www.it.northwestern.edu/bin/docs/ApprovedUsesAppB.pdf.

181. The President's Identity Theft Task Force Report (Sept. 2008), *available at* www.idtheft.gov/reports/IDTReport2008.pdf.

182. *See* SECURITY IN NUMBERS, *supra* note 177.

183. Alaska, Iowa, Kentucky, Massachusetts, New Hampshire, Ohio, West Virginia, and Wyoming. Fed. Trade Comm'n, *State Laws: Social Security Numbers*, http://www.ftc.gov/bcp/edu/microsites/idtheft/law-enforcement/state-laws-social-security.html (last visited Oct. 15, 2009); ANDREW B. SERWIN, 2 INFORMATION SECURITY AND PRIVACY: A PRACTICAL GUIDE TO FEDERAL, STATE AND INTERNATIONAL LAW, 84–172 (Thompson Reuters/West 2008).

Most notably, many states have enacted laws that restrict the use and display of an individual's SSN, printing of SSNs on identification cards, and the mailing of SSNs.[184] Colleges and universities should be cognizant of these laws, especially if using SSNs as unique identifiers for students, alumni, or donors.

7. Marketing

Two states (Maine and Illinois) have recently enacted statutory provisions which impact the method and extent to which student information can be shared with companies for marketing purposes.

Illinois: A recent Illinois law has expanded the state's restrictions on sharing student personal information with credit card companies. The Credit Card Marketing Act of 2009, set to take effect on January 1, 2010, applies to all Illinois colleges and universities, and their affiliates such as student groups and alumni organizations.[185] The law prohibits institutions of higher education from providing debit or credit card issuers the personal information of students under the age of twenty-one. Previously, the Illinois restrictions were limited to public schools and did not apply to educational affiliates that typically act as intermediaries for credit card marketing efforts to students. Illinois colleges and universities should focus on educating all organizations on campus about the law's implications and prohibited information sharing with credit card companies. The law carries a potential penalty of up to $1,000 per incident.[186]

Maine: This summer, Maine enacted legislation that would effectively prohibit direct marketing of products and services to Maine residents under the age of 18.[187] As drafted, Maine's "Act to Prevent Predatory Marketing Practices Against Minors" could significantly impact the way that educational institutions gather information about and market to potential students, and how they can collect essential information about students who have selected to attend their institutions.

The new law, scheduled to go into effect on September 12, 2009, prohibits the collection of "personal information" or "health-related information" from a minor[188] without first obtaining "verifiable consent" from the minor's parent or legal guardian. Under the law, "Personal Information" is defined to mean (1) the minor's first name or first initial

184. *See* Consumers Union, Social Security Number Protection Legislation for States, http://www.consumersunion.org/pub/2007/11/004801print.html (last visited Oct. 15, 2009).

185. Credit Card Marketing Act of 2009, 110 ILL. COMP. STAT. 26/25 (West 2009).

186. *Id*. at 26/30.

187. ME. REV. STAT. ANN. tit. 10, §§ 9551–54 (2009).

188. *Id.* at § 9552 (1). Although the term "minor" is not defined in the law, presumably it is intended to mean anyone under 18.

and last name, (2) the minor's home or other physical address, (3) the minor's Social Security number, (4) the minor's driver's license or state identification card number, and (5) any information concerning the minor that is collected in combination with one of the identifiers described above.[189] "Health-Related Information" is defined as any information about an individual or a member of the individual's family relating to health, nutrition, drug or medication use, physical or bodily condition, mental health, medical history, medical insurance coverage or claims or other similar data.[190] The law defines "Verifiable Consent" as any reasonable effort, taking into consideration available technology, including a request for authorization for future collection, use and disclosure described in the notice, to ensure that a parent of a minor receives notice of the collection, use and disclosure practices and authorizes the collection, use and disclosure, as applicable, of Personal Information and the subsequent use of the information before that information is collected from that minor.

The law prohibits the sale (including offering for sale) or transfer to another person of a minor's Health-Related Information or Personal Information if the information was collected in violation of the statute, individually identifies the minor, or will be used for the purpose of marketing a product or service to that minor.[191] As drafted, the law appears to be somewhat internally inconsistent, so it may be ripe for amendment. The law prohibits the use of a minor's Personal Information or any Health-Related Information for the purpose of marketing any product or service to that minor, even if the information was collected with parental consent and the marketing activities also received advance parental consent.[192] Similarly, the restriction on the sale or transfer of any information that "individually identifies the minor" seems to cast an overly broad net over the Personal Information of all minors, even if their parents have consented to the collection and transfer. Such a provision could prevent college testing organizations from passing information about potential applicants to colleges and universities even if such transfer of information were requested by the minor. The law also gives private litigants the right to sue for damages and injunctive relief and to recover attorneys' fees in the event of a successful lawsuit.[193]

As of early September, the law's future is unclear. A group of parties that includes the Maine Independent Colleges Association has filed suit to obtain an injunction blocking the legislation from going into effect.[194] On

189. *Id.* at § 9551 (4).
190. *Id.* at § 9551 (1).
191. *Id.* at § 9552.
192. *Id.* at §§ 9552–3.
193. *Id.* at § 9554 (3).
194. Marisa Taylor, *Maine Backs Away From Marketing-Privacy Law*, WALL ST. J. BLOGS, Sept. 2, 2009, http://blogs.wsj.com/digits/2009/09/02/maine-backs-away-from-

September 9, 2009, the U.S. District Court of Maine agreed with the plaintiffs that the law is likely unconstitutional, but dismissed the suit on the grounds that Maine's Attorney General has stated that she will not prosecute companies that do not comply with the law.[195] The Maine Senate will review the bill before the next legislative session in January 2010.[196] Unfortunately, private parties can still file costly class action lawsuits and the law provides significant financial incentives for them to do so, although the court stated that such private causes of action could suffer from the same Constitutional infirmities.[197] In anticipation of the law being amended, educational institutions should evaluate where and whether it is feasible to implement age and residency screening measures where consumer data is collected and, if necessary, how to prevent Maine residents who are minors to participate in activities that require the collection of personal information, such as signing up for online newsletters.

F. Payment Card Industry Data Security Standard (PCI DSS)

The PCI DSS is not a law but applies to any institution that processes credit card payments (e.g., at the campus bookstore, restaurants, or dining halls, or for tuition or donations).[198] In December 2004, Visa and MasterCard announced an agreement to align their data security programs for merchants and third-party processors, which led to the creation of a standard known as the Payment Card Industry Data Security Standard ("PCI DSS").[199] The PCI DSS was designed to guard against attacks that involve theft and subsequent misuse of cardholder information, and

---

marketing-privacy-law.

195. Me. Indep. Colls. Ass'n v. Baldacci, No. 09-cv-00396 (D. Me., Sept. 9, 2009) (stipulated order of dismissal), stating:

> The Court finds that the Plaintiffs have met their burden of establishing a likelihood of success on the merits of their claims that Chapter 230 is overbroad and violates the First Amendment. The Attorney General has acknowledged her concerns over the substantial overbreadth of the statute and the implications of Chapter 230 on the exercise of First Amendment rights and accordingly has committed not to enforce it. She has also represented that the Legislature will be reconsidering the statute when it reconvenes. As a result, third parties are on notice that a private cause of action under Chapter 230 could suffer from the same constitutional infirmities. In light of these considerations, the parties have agreed to a dismissal of this action without prejudice and the Court hereby SO ORDERS.

196. Taylor, *supra* note 194.

197. Sheri Qualters, *Maine Agrees Not to Enforce Predatory Marketing Law*, NAT'L L. J., Sept. 11, 2009, http://www.law.com/jsp/article.jsp?id=1202433718455, (last visited Nov. 22, 2009).

198. *See* Payment Card Industry Data Security Standard, *supra* note 5.

199. *Id.*

consists of twelve requirements (though each requirement includes a few sub-requirements).[200]

Depending upon how many payment transactions a college or a university processes each year, the payment card associations may require the school to validate its compliance with PCI DSS through an on-site assessment performed by an independent assessor.[201] For example, Level 1 compliance is reserved for more than 6 million Visa or MasterCard transactions per year or more than 2.5 million American Express transactions a year. Level 2 covers 150,000 to 6 million transactions for MasterCard; 1 million to 6 million transactions for Visa; and 50,000 to 2.5 million American Express transactions. Level 3 covers 20,000 to 1 million Visa e-commerce transaction; 20,000 to 150,000 e-commerce MasterCard transactions; and less than 50,000 American Express transactions. Levels 1 and 2 require an annual on-site PCI DSS data security assessment performed by a qualified auditor and signed by an officer of the complying school, and a quarterly network scan performed by a qualified independent vendor.[202] Level 3 requires an annual PCI DSS self-assessment questionnaire by the school and a quarterly network scan performed by a qualified vendor.[203]

Most colleges and universities accept credit card payments in one or multiple outlets on campus. Depending on the credit card company requirements and card processor mandates, colleges and universities may be required to comply with PCI DSS. The degree to which the PCI DSS applies to an educational institution's activities is dictated by the number of transactions processed. As such, the requirements for larger colleges and universities, where there is likely to be a high volume of transactions, will be more stringent than at smaller colleges and universities that process fewer transactions.

II. INTERNATIONAL DATA PROTECTION CONSIDERATIONS

Colleges and universities no longer exist on isolated campuses, but, rather, often have an international dimension to their student bodies and

200. The twelve PCI DSS requirements include: (1) installing and maintaining a firewall configuration to protect cardholder data; (2) not using vendor-supplied defaults for system passwords and other security parameters; (3) protecting stored cardholder data; (4) encrypting transmission of cardholder data across open, public networks; (5) using and regularly updating anti-virus software; (6) developing and maintaining secure systems and applications; (7) restricting access to cardholder data by business need-to-know; (8) assigning a unique ID to each person with computer access; (9) restricting physical access to cardholder data; (10) tracking and monitoring all access to network resources and cardholder data; (11) regularly testing security systems and processes; and (12) maintaining a policy that addresses information security. *Id.*

201. *Id.*

202. *Id.*

203. *Id.*

operations. Student exchange programs have been popular for many years but, more recently, many colleges and universities have been opening independent campuses overseas.[204] Both the recruiting of foreign students, faculty, and staff and the management of overseas campuses implicate international privacy laws from jurisdictions that have data-privacy laws very different from the domestic approach to data protection.

Nations around the world have enacted various laws designed to protect data privacy. At this time, it is difficult to pinpoint how many countries have such data-privacy laws. Most developed and developing countries, however, offer some form of data-privacy protection.[205] The groundwork for the international data-privacy regime was laid in the 1970s, with the development and adoption of the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data promulgated by the Organization for Economic Cooperation and Development ("OECD").[206] The OECD Guidelines include provisions regarding notice, consent, transfers, access, integrity, and safety of personal information.[207]

This Section outlines some of the international data-privacy authorities applicable in different regions of the world and the implications each presents for colleges and universities that have campuses in those regions.

A. European Union and Canada

In 1995, the European Union ("EU") Parliament passed the EU Directive, which set a minimum standard for EU member states' comprehensive legislation on data-privacy protection.[208] Broadly speaking, the EU Directive allows private entities to collect only a limited amount of protected personal data and only for a specific permitted purpose.[209] Further, any private entity collecting protected personal data is required to provide notice to data subjects regarding the purpose for which the information is being gathered, and also may be required to obtain consent from the data subjects in order to use or disclose the information to a third party.[210] Finally, the EU Directive closely regulates transborder transfers of protected data, and allows for imposition of serious sanctions against

---

204. *See* Public Broadcasting Service, NOW: U.S. Colleges with Foreign Campuses, http://www.pbs.org/now/shows/420/foreign-campuses.html (last visited Oct. 16, 2009).

205. *See* Information Shield, Inc., International Privacy Laws, http://www.informationshield.com/intprivacylaws.html (last visited Oct. 15, 2009).

206. Org. for Econ. Co-Operation and Dev., *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html (last visited Oct. 15, 2009).

207. *Id.*

208. *See* EU Directive, *supra* note 6.

209. *Id.*

210. *Id.*

violators.[211]

The EU and the U.S. approach the protection of personal information from very different perspectives.[212] Much of this cultural difference stems from the extreme abuse of personal information that occurred under Nazi leadership during World War II.[213] The EU begins with the premise that information belongs to the data subject and the data subject should have the right to control how that data is used and to whom it is disclosed.[214] The U.S., on the other hand, starts from a tradition of freedom of speech and, thus, free use of information,[215] and generally treats the possessor of information as the owner of that information and, until recently, when a data subject provided personal information to a business entity, it was treated more like a sales transaction.[216] The "privacy contract" between the U.S. data subject and the business is monitored by the FTC, but as long as that contract is honored, the business could do whatever it wished with the personal information. In the U.S., only information that was deemed to have potentially harmful effects if disclosed in an unregulated manner (i.e., financial information (GLBA, FACT Act, etc.), health information (HIPAA), and children's information (FERPA and the Children's Online Privacy and Protection Act) has been subject to regulation.[217] Understanding the difference between the European approach and the American approach is essential for U.S. entities dealing with many foreign countries' data protection regimes.

The EU places severe restrictions on the export of personal information from the EU by private actors.[218] Protected data may be transferred outside

---

211. *Id.*

212. *See* Int'l Trade Admin., *Safe Harbor Overview,* EXPORT.GOV, http://www.export.gov/safeharbor/eg_main_018236.asp (last visited Nov. 22, 2009).

213. PRACTISING LAW INSTITUTE, INTERNATIONAL CORPORATE PRACTICE § 24.2.2 (1st ed. 2009).

214. *Id.* (stating that the object of the Directive is to "protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data").

215. INTERNATIONAL CORPORATE PRACTICE, *supra* note 213, § 24.2.2.

216. *See, e.g.* Dwyer v. American Express Co., (App. Ct. of Ill.) 652 N.E.2d 1351 (1995). American Express cardholders sued American Express for renting their names to merchants under theories of both invasion of privacy and appropriation The court held that when a cardholder uses a credit card,, the cardholder is giving information to the credit card company that reveals the cardholder's spending habits and shopping preferences, which led the court to conclude that there was no invasion of privacy. On the appropriate claim, the court reasoned that one individual's information had little value, and the value of the personal information is only created through the aggregation by American Express. .

217. *See* Int'l Trade Admin., *Safe Harbor Overview,* EXPORT.GOV, http://www.export.gov/safeharbor/eg_main_018236.asp (last visited Nov. 22, 2009).

218. Public actors are allowed much more leeway in using or disclosing personal information to a third party for diplomatic or national security reasons. *See* EU Directive, *supra* note 6.

of the EU only to a country with "adequate" data-privacy protections, meaning protections substantially similar to or greater than those offered by the EU Directive.[219] The EU Directive does permit transfers of personal data to countries that have not received an adequacy ruling through (1) model contracts, or (2) in the case of the U.S., the U.S. Department of Commerce's Safe Harbor Program.[220] Model contracts are contractual agreements between the data exporter in the EU and the foreign entity that will be receiving the personal information (known as the data importer)[221] that provide for security and protection of the transferred personal information in accordance with the requirements of the EU Directive. The Safe Harbor Program is unique to the U.S. and is a means by which U.S. businesses that are regulated by the FTC can be certified as possessing policies and procedures that conform to the requirements of the EU Directive, and, therefore, import protected data from the EU without further administrative requirements.[222] Additionally, transfers of personal information to an entity in a country that does not guarantee an adequate level of privacy protection and that has not completed a model contract or assented to Safe Harbor are permitted if: (1) the data subject unambiguously consents to the transfer; (2) transfer is necessary for the performance of a contract between the data subject and the organization; (3) transfer is necessary for the entry into, performance, or both, of a contract between the organization and a third party for the data subject's benefit; (4) transfer is justified on "important public interest grounds" or for purposes of a lawsuit; (5) transfer is necessary to protect the vital interests of the data subject; or (6) information is from a database to which the public has routine access because of national laws on access to documents.[223] EU member states may create other exceptions to the transborder transfer restrictions, but they must notify the European Commission and other member states of any such exemptions.[224]

Canada occupies the middle of the spectrum of data-privacy protection,

---

219. *Id.* Those jurisdictions that have received an adequacy ruling from the EU include: Argentina, Comm'n Decision 1731 of 30 June 2003, 2003 O.J. (L168) 19; Canada, Council Decision of 18 July 2005, 2006 O.J. (L82) 14; Guernsey, Comm'n Decision of 21 November 2003, 2003 O.J. (L308) 27; Isle of Man, Comm'n Decision of 28 April 2004, 2004 O.J. (L151) 48; Jersey, Comm'n Decision of 8 May 2008,2008 O.J. (L138) 21; and Switzerland, Comm'n Decision of 26 July 2000, 2000 O.J. (L215) 1. [hereinafter collectively Commission Decisions].

220. *See* EU Directive, *supra* note 6.

221. *Id.*

222. *See* Int'l Trade Admin., *Safe Harbor Overview,* EXPORT.GOV, http://www.export.gov/safeharbor/eg_main_018236.asp (last visited Oct. 15, 2009).

223. *See* Bignami, *supra* note 18, at 826; *see also* EU Directive*, supra* note 6, art. 7.

224. One example of an exception is allowing a transborder transfer if a contract between a member and a receiving party outside the EU—specifically, not a "safe" country for personal information—renders that party liable in tort for any loss or theft of the personal information. *See* Bignami, *supra* note 18, at 826.

somewhere between the *laissez-faire* approach of the United States and the strictly regulated EU model.[225] However, Canada began moving closer to the EU approach with the passage of the Personal Information Protection and Electronic Documents Act ("PIPEDA").[226] With PIPEDA's passage in 2000 and its full implementation in 2004, the EU recognized Canada as providing "adequate" data-privacy protection, which connotes protection at least equal to that afforded by the EU Directive.[227] PIPEDA brought significant changes to how businesses use Canadians' personal information.

PIPEDA also regulates transborder transfers of protected data.[228] PIPEDA applies to information gathered prior to its enactment, and applies to non-Canadian businesses gathering information about Canadians.[229] PIPEDA follows an organization-to-organization approach and does not prohibit organizations from transferring personal information to another jurisdiction for processing; PIPEDA, however, holds organizations accountable for the protection of personal information transferred in any such arrangement.[230] American colleges and universities gathering information on prospective students, employees, or other individuals, such as alumni and parents, may be affected by PIPEDA while collecting the information in Canada, or acquiring it from a Canadian partner, because PIPEDA's secondary data transfer requirement forces Canadian businesses to include PIPEDA's privacy requirements in all contracts contemplating transfer of Canadians' personal information abroad.[231]

Both the EU Directive and PIPEDA adopt an extraordinarily broad definition of "personal information."[232] The EU Directive covers all information "relating to an identified or identifiable natural person."[233] Specifically, the European Union's definition of "personal data" means "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."[234] PIPEDA applies to entities using or disclosing such information during the course of a "commercial activity," which includes selling or leasing donor, membership or other

225. *See* PIPEDA, 2000 S.C., ch. 5.
226. *See id.*
227. *See* Commission Decisions, *supra* note 184.
228. *See* PIPEDA.
229. *See id.* § 4.
230. OFFICE OF THE PRIVACY COMM'R OF CAN., CROSS-BORDER PERSONAL DATA TRANSFERS, *available at* http://www.privcom.gc.ca/information/guide/2009/gl_dab_090127_e.pdf (last visited Oct. 15, 2009).
231. *Id.*
232. See EU Directive, *supra* note 6, art. 2(a); PIPEDA, 2000 S.C. ch. 5, § 2(1).
233. *See* EU Directive, *supra* note 6.
234. *Id.*

fundraising lists (the latter being crucial to any development efforts for educational institutions or hospitals).[235] Protected personal data under both the EU Directive and PIPEDA includes (but is not limited to): first name or initials, last name, e-mail address, phone numbers, credit reports, and, most relevant to colleges and universities, education records.[236] Notably, in the EU, IP addresses are also considered to be protected personal information.[237]

The EU Directive and PIPEDA are significant to any college or university that operates a campus in either location or that attempts to transfer student information back to its U.S. campus. Under the data-privacy laws of both regions, education records are clearly personally identifiable information requiring stringent protection. For educational institutions in the U.S., transfer of such information outside of the EU is limited to situations where student consent is provided or a contractual arrangement has been instituted to assure security protections equivalent to the EU's requirements.[238] Satisfying the data transfer requirements of the EU is burdensome for even large corporations, and, as such, presents challenges for any U.S. based college or university operating in the EU or Canada. The EU's privacy regime is particularly daunting, considering that the EU has twenty-seven members, each with its own set of privacy laws.

B. Asia: Asia-Pacific Economic Cooperation (APEC) Privacy Framework

Colleges and universities operating in and around Asia should become familiar with the data-privacy framework currently being developed by the Asia-Pacific Economic Cooperation ("APEC"). APEC is an intergovernmental group comprised of "Member Economies" along the Pacific Rim that work to enhance economic growth for the region and to strengthen the Asia-Pacific community.[239] In 2002, the APEC Privacy Subgroup was formed to develop a privacy framework for the region. The APEC Privacy Framework (the "Framework"), which is still under development, is a permissive set of privacy principles that, once fully developed, will become the accepted standards for any business that

---

235. PIPEDA, § 4. Canadian law gives an equally broad scope to the definition of "commercial activity," defining it as "any particular transaction, act, or conduct that is of a commercial character, including selling, bartering or leasing of donor, membership, or other fundraising lists." *Id.*

236. *See, e.g.*, Rebecca Herold, *Privacy, Compliance and International Data Flows: White Paper*, NETIQ, June 2006, at 4.

237. Data Protection Working Party, *Opinion 1/2008 on Data Protection Issues Related to Search Engines* (April 4, 2008) *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp148_en.pdf (last visited Oct. 15, 2009).

238. *See* EU Directive, *supra* note 6.

239. *See generally* Asia-Pacific Econ. Cooperation, About APEC, http://www.apec.org/apec/about_apec.html (last visited Oct. 15, 2009).

chooses to operate in any of the APEC Member Economies.[240]

Recognizing that there must be a balance between free flow of information and privacy protections for personal information, the Framework provides guidance to APEC Member Economies that have not yet addressed privacy issues from a regulatory or policy standpoint.[241] The Framework aids global organizations that collect personal data in APEC Member Economies to develop consistency within their organizations with regards to the use of that information.[242] The Framework balances information privacy with business needs and commercial interests, while recognizing cultural and other diversities that exist between nations.[243] While the Framework is intended to promote a consistent approach to information privacy protection throughout APEC, the privacy principles specified in the Framework are aspirational rather than binding. Thus, there is no person or entity that actively enforces the Framework.

Despite still being under development, colleges and universities with operations in APEC Member Economies should monitor progress on the APEC Privacy Framework and make adjustments to their data protection compliance programs as the Framework evolves.

C. Other Regions

Approaches to data protection in other regions of the world range from totalitarian to non-existent, and from the United States' *laissez-faire* sectoral approach to the comprehensive European framework. The data protection laws in other regions of the world with which colleges and universities may wish to become familiar include some of the South American countries, notably Argentina, and the Middle East. In South America, particularly Argentina, the notion of "Habeas Data" governs the protection of personal information.[244] Habeas Data is a constitutional right found in several Latin-American countries. The concept varies from country to country, but, in general, is designed to protect, by means of an individual complaint presented to a constitutional court, the image, privacy, honor, information self-determination, and freedom of information of a person.[245] Additionally, as U.S. campuses expand into the Middle East, educational institutions should monitor developments in that part of the world. Most recently the United Arab Emirates created the Federal Data Privacy Commission: a comprehensive data-privacy law for the country is

240. *See* APEC Privacy Framework, *supra* note 8.
241. *Id.*
242. *Id.*
243. *Id.*
244. Privacy International, *Argentine Republic,* http://www.privacyinternational.org/survey/phr2003/countries/argentina.htm (last visited Oct. 15, 2009).
245. *See id*.

expected.[246] Institutions wishing to recruit or operate in these countries may be required to negotiate a data export agreement with the relevant governmental agency. In these cases, engaging local counsel is strongly recommended.

III. CONCLUSION

U.S. colleges and universities are subject to significant regulation with respect to how they collect, store, and use personal information. Educational institutions collect and use information from prospective applicants (both students, many of whom are under the age of eighteen, and potential employees), parents of applicants and students, alumni and their spouses, and, of course, donors. Colleges and universities also collect personal information, including sensitive financial information, in a variety of ways: over the internet, through mail and telephone solicitation, at campus health centers and hospitals, and at campus events. Finally, educational institutions collect information across a wide range of geographies, including numerous U.S. states and foreign countries. Thus, most institutions must comply with the various data-privacy-protection regulations. In conclusion, this article suggests the following general guidelines for attempting to comply with both domestic and international data protection laws.

First, accountability serves as the cornerstone of compliance with privacy laws. Every educational institution collects, stores, and uses personal information, and each school is ultimately responsible for keeping all such personal information safe. This means that colleges and universities should adopt privacy and security policies that comply with basic principles of data-privacy protection and train the relevant staff with respect to these policies. Institutions should appoint an individual or team (e.g., a chief privacy officer or a similar senior administration official) who will be responsible for compliance and will have the ability to address complaints. In the for-profit higher education industry, it is important to note that subsidiaries and affiliates may be considered separate entities under international privacy laws, and may require additional staff and resources for compliance. Significantly, academic administrations must provide meaningful support and sponsorship to their privacy specialists.

Unfortunately, a recent study indicated that, unlike corporations, many of which have hired Chief Privacy Officers ("CPO"), colleges and universities have been slow to adapt.[247] The decentralized operations of

246. *See* Privacy International, *PHR2006 – United Arab Emirates*, http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-559480 (last visited Oct. 15, 2009).

247. Lisa Guernsey, *A Wealth of Data, and Nobody in Charge*, CHRON. OF HIGHER EDUC. (Washington, D.C.), Nov 21, 2008, *available at* http://chronicle.com/weekly/v55/i13/13a00103.htm.

most educational institutions may be one of the primary reasons that the CPO role is more difficult to define and fill at educational institutions. Since data privacy at colleges and universities spans across academic departments, administration, the affiliated hospital system, residence life, vendor relationships, and on-campus concessions, training must be an integral part of any institution's privacy compliance program. Such training should be tailored to the various organizations on campus and their distinctive requirements.

Second, colleges and universities should also consider using waiver and consent forms for their applicants, potential applicants, and students, and implementing clear privacy policies for visitors to their web sites. Educational institutions must make their privacy policies and procedures transparent. They have to make readily available to individuals specific information about their policies and practices relating to the management of personal information.

Third, colleges and universities should develop and implement procedures to assure that the personal information collected is necessary, accurate, complete, and up-to-date (including, where applicable, whether the identified purpose for collecting and using such information is accurate and up-to-date). The data subject should have the right to access the information held by the institution. In some instances, schools may be required to inform the data subject (upon request) of the existence, use, and disclosure of his personal information and provide access to that information. Data subjects must be able to challenge the accuracy and completeness of the information, and schools must amend the information accordingly. The simplest way for any institution to comply with these requirements is to include contact information for its privacy office on its web site, in its published privacy policy, or both. Also, data subjects should have the ability to file a complaint directly with the college or university regarding the school's use of personal information. The Safe Harbor program and its privacy principles articulate sound data-privacy practices that colleges and universities can emulate.[248]

Educational institutions should also implement policies to safeguard protected information (such as classification or authorization schemes for accessing information) and have the technological savvy to protect such data from loss or theft. One of the surest ways to safeguard personal information is not to keep it at all. Among other things, schools should work to minimize or eliminate the use of Social Security numbers. In fact, the PCI DSS standards demand that all credit card data (including magnetic data) be purged within hours of the relevant payment transaction. Therefore, schools should regularly dispose of protected personal

248. The Safe Harbor Privacy Principles cover (1) notice, (2) choice, (3) onward transfer, (4) security, (5) data integrity, (6) access, and (7) enforcement. *See* Int'l Trade Admin, *supra* note 212.

information, especially once the original purpose for collecting such information is fulfilled, and should provide training to faculty and administrative staff regarding the financial, operational, and reputational risks associated with unauthorized disclosure of data.

Finally, some international jurisdictions, particularly the EU countries and Canada, may require the "knowledge and consent" of the data subject for collection, use, or disclosure of personal information. Consequently, schools should be aware of what data they are collecting, using, or disclosing, and whether the data is from international locations. International data-privacy laws are extremely complex and varied, and it is important for colleges and university administrators to seek counsel from in-house or outside privacy experts on compliance issues.