COLLEGE AND UNIVERSITY DATA BREACHES: REGULATING HIGHER EDUCATION CYBERSECURITY UNDER STATE AND FEDERAL LAW

KATIE BEAUDIN*

* J.D. Candidate, Notre Dame Law School, 2015. I would like to thank Professor Patricia Bellia, Professor John Robinson, and Kathleen Rice for their input and insight throughout the writing of this note. I would also like to thank the staff of the *Journal of College and University Law* for their hard work on this note, and the entirety of Volume 41.

INTRODUCTION

As our reliance on technology increases, so do threats of cyberattacks. Recently, there has been a serious increase in breaches of data and information security. These breaches have attacked some of the largest corporations in the United States, including Target Corp., Neiman Marcus, and eBay. However, these breaches are not confined to public corporations. Colleges and universities have access to a great deal of private information, including educational and medical records, as well as employee data. Because of this wealth of private information, and, oftentimes, shoddy security measures, there have been over 700 data breaches involving educational institutions publicly recorded between 2005 and 2014.[1] The way that these institutions prepare for and respond to these breaches is indicative of how likely they are to be subjected to litigation or government action.

1. Chronology of Data Breaches – Educational Institutions, PRIVACY RIGHTS CLEARINGHOUSE, https://www.privacyrights.org/data-breach/new (last visited Apr. 14, 2015).

A recent study by BitSight Technologies rated the cyber security performances of a number of colleges and universities based on their collegiate athletic conferences.[2] The study determined that colleges and universities are not adequately addressing cybersecurity challenges, and can easily fall victim to high levels of malware infections.[3] Many colleges and universities do not have cyber plans in place and are not ranking information security as a key issue on campus.[4]

Colleges and universities are in a unique position in that they are subject to a multitude of federal and state statutes regulating data privacy, from consumer reporting laws to the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act (HIPAA). Additionally, they can face class action lawsuits and Federal Trade Commission (FTC) action in the wake of a cyber breach.[5] This Note will discuss the types of breaches commonly faced by higher education institutions and what steps these institutions can take to limit liability and properly respond to potential litigation.

Part I will address how data breaches occur, and Part II will outline what kind of data breaches commonly affect colleges and universities, including examples of colleges and universities that have recently experienced those types of breaches. Part III will address the statutes that control how colleges and universities must treat data, react to breaches and notify students. Part IV highlights recent data breaches, how those colleges and universities have dealt with them, and what type of litigation, if any, has resulted. Part V offers advice for college and university counsel on how best to insulate from liability, including timely notification and free credit monitoring services, and how to defend against class actions stemming from a breach. Finally, Part VI addresses potential future regulations that colleges and universities should anticipate having to follow.

I. WHAT IS A DATA BREACH?

The Identity Theft Research Center defines a data breach as "an incident in which an individual name plus a Social Security number, driver's license number, medical record or financial record (credit/debit cards included) is potentially put at risk because of exposure."[6] These breaches can lead to

---

2. *Powerhouses and Benchwarmers: Assessing the Cyber Security Performance of Collegiate Athletic Conferences*, BITSIGHT TECHNOLOGIES (Aug. 2014), http://media.scmagazine.com/documents/90/bitsight_insights_athletics_q3_22351.pdf.

3. *Id.* at 2.

4. *Id.* at 6.

5. *See infra* Part III for a discussion of FTC action related to data breaches, and Part IV for a discussion of class actions resulting from higher education data breaches.

6. *Data Breaches*, IDENTITY THEFT RESEARCH CENTER, http://www.idtheftcenter.org/id-theft/data-breaches.html (last visited Apr. 14, 2015). The Privacy Technical Assistance Center defines a data breach as "any instance in

identity theft, privacy violations, and fraud.[7] Stored personal information can be compromised in numerous ways, including insider theft, employee error, hacker attack or physical theft.[8]

a. Hacking

A survey of data breaches over the past several years found that hackers caused thirty–one percent of all breaches.[9] In the higher education context, thirty–six percent of breaches are attributable to hackers and malware.[10] A major hacker tactic is an advanced persistent threat, which employs undetectable access into a computer system through software vulnerabilities and the eventual theft of large amounts of data.[11]

Hackers are interested in the theft of valuable personal information such as credit card numbers or other personal information that can be used for bank fraud.[12] The hackers use a systematic process for initiating an attack on a computer network.[13] The process begins by gathering information about the organization and targeting individuals with access to sensitive data.[14] The hackers then identify the weaknesses in the network to find openings, which they use to penetrate the system by exploiting a valid user account with a weak password.[15] Once they are in the system, they find another user account that has greater access privileges to sensitive information.[16] They use this account to install malware on the computer and gain command over network infrastructure to transmit the stolen data to their hacking platform.[17] The last step involves concealing the attack by

---

which there is an unauthorized release or access of [personally identifiable information] or other information not suitable for public release." *Data Breach Response Checklist*, PRIVACY TECHNICAL ASSISTANCE CENTER 2 (Sep. 2012), *available at* http://ptac.ed.gov/sites/default/files/checklist_data_breach_response_092012.pdf.

7. DATA BREACH AND ENCRYPTION HANDBOOK 7 (Lucy Thomson ed., 2011).

8. *See Data Breaches*, *supra* note 6.

9. *Data Loss Statistics*, OPEN SECURITY FOUND., http://datalossdb.org/statistics (last visited Apr. 14, 2015).

10. *Just in Time Research: Data Breaches in Higher Education*, EDUCASE 6 (2014) [hereinafter Data Breaches in Higher Education], https://net.educause.edu/ir/library/pdf/ECP1402.pdf. There is some overlap between the various types of data breaches, meaning that sometimes a hacking incident could also be classified under insider theft. *Id.*

11. JILL D. RHODES & VINCENT I. POLLEY, THE ABA CYBERSECURITY HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS, AND BUSINESS PROFESSIONALS 13 (2013).

12. THOMSON, *supra* note 7, at 27.

13. *Id.* at 59.

14. *Id.*

15. *Id.*

16. *Id.*

17. *Id.* at 60.

clearing the history and leaving no trace back to the hackers.[18]

b. Theft

Theft of laptops or other electronic devices are another source of data breaches.[19] These devices can include laptops, desktop computers, portable electronic devices such as smart phones, or hard drives.[20] Theft of such devices compromised seven million sensitive medical records and student personal information records from 2009 to the beginning of 2010.[21]

A major problem with theft of mobile devices is the lack of encryption on these devices.[22] Many colleges and universities have a Bring Your Own Device (BYOD) culture that allows employees to use their personal smart phones or laptops for professional work.[23] Allowing personal devices can involve the transfer of a great deal of confidential information to the device, and the creation and access of sensitive data on a device the college or university does not adequately control.[24] Because of this data transfer, the theft of employees' personal devices, which are rarely encrypted, can put student information at risk.

c. Malicious Insiders

Roughly ten percent of all data breaches occur at the hands of a malicious insider.[25] A malicious insider is defined as "a current or former em-

---

18. *Id.*

19. *See, e.g.*, *Data Loss Statistics*, *supra* note 9. Eleven percent of data breaches have occurred because of a stolen laptop, four percent from a stolen computer, and one percent from a stolen drive. *Id.* In the higher education context, seventeen percent of reported breaches have involved theft. *Data Breaches in Higher Education*, *supra* note 10, at 6.

20. RHODES & POLLEY, *supra* note 11, at 16.

21. THOMSON, *supra* note 7, at 23. In California, during 2012 and 2013, physical theft and loss of devices accounted for 25% of education industry data breaches. *California Data Breach Report*, OFFICE OF THE ATTORNEY GEN. 11 fig. 7 (Oct. 2014), *available at* https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/2014data_breach_rpt.pdf.

22. THOMSON, *supra* note 7, at 18. The University of San Francisco had to alert patients when an unencrypted personal laptop computer was stolen from an employee's locked car. Elizabeth Fernandez, *UCSF Alerts Some Patients About Laptop Computer Theft*, U.C. SAN FRANCISCO (Oct. 2, 2013), http://www.ucsf.edu/news/2013/10/109381/ucsf-alerts-some-patients-about-laptop-computer-theft. The laptop contained personal information for 3,541 patients. *Id.* There were also paper documents for thirty-one patients stolen along with the laptop that contained personal information such as name, date of birth, and health information. *Id.*

23. RHODES & POLLEY, *supra* note 11, at 7.

24. *Id.*

25. *Data Loss Statistics*, *supra* note 9. However, only three percent of higher education data breaches were the result of an insider. *Data Breaches in Higher Education*, *supra* note 10, at 6.

ployee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems."[26]

Insider threats involve individuals abusing their security privileges to access sensitive records.[27] Employees choose to steal data for reasons such as financial gain, with the intent to sell the data to third parties, or for revenge on the institution.[28] Additionally, many insider threats involve employees who were recently fired, resigned, or changed positions and steal as an act of revenge, or involve employees who just joined the entity and lack a sense of loyalty to the institution.[29] About a quarter of insider-initiated data breaches involved these types of newly hired or fired employees.[30]

Malicious insiders can be students as well as employees. In August 2014, a former Brigham Young University student was arrested for remotely hacking the BYU network to change his student status.[31] He also admitted to hacking the systems through computers belonging to professors and administrators in order to change his grades and access other students' personal information.[32] This has become increasingly prevalent on campuses, as students use keystroke loggers to capture professors' passwords and then use this information to change grades.[33] These actions only highlight the ease with which other hackers could access personal information stored on college and university systems.

d. Improper Disposal

Although most personal information is now stored electronically, there can be breaches resulting from an improper disposal of paper records in-

26. *Insider Threat*, CERT, http://www.cert.org/insider-threat/ (last visited Apr. 14, 2015).

27. THOMSON, *supra* note 7, at 25.

28. RHODES & POLLEY, *supra* note 11, at 20. Other motivations for insider hacking can include fame, capability, divided loyalty, delusion, or even just a perceived challenge to hack the system. *See* Charles P. Pfleeger, *Reflections on the Insider Threat, in* INSIDER ATTACK AND CYBER SECURITY: BEYOND THE HACKER 5, 7 (Salvatore J. Stolfo et al. eds., 2008).

29. RHODES & POLLEY, *supra* note 11, at 20.

30. *Id.*

31. Candi Higley, *Police: Former BYU student hacked into school computers to change grades*, DAILY HERALD (Aug. 5, 2014), http://www.heraldextra.com/news/local/crime-and-courts/police-former-byu-student-hacked-into-school-computers-to-change/article_1d68bda3-ab1e-5ecb-a7ce-6757c8bda858.html.

32. *Id.*

33. Gerry Smith, *Why Study? College Hackers Are Changing F's To A's*, HUFF POST (Mar. 7, 2014), http://www.huffingtonpost.com/2014/03/05/student-hacking_n_4907344.html.

volving personally identifiable information.[34] These paper breaches make up nearly twenty-six percent of breaches.[35] Sometimes the breach comes from something as simple as someone throwing confidential information in the trash as opposed to taking more secure measures such as using a shredder.[36] The same issue can arise with electronic records, due to the improper disposal of hard drives or other media in too public of places.[37]

e. Accidental Exposure

Thirty percent of higher education data breaches stem from unintended disclosures.[38] There are many different kinds of accidental exposure, including human error, pure accidents, or natural disasters.[39] People make simple errors such as mistakes in judgment, failure to follow procedures, accidental deletion, and even something as easy as clicking the wrong button.[40] Moreover, incidents on a campus such as fire, damage to computers, earthquakes, or flooding can lead to unintentional exposure of data.[41]

II. DATA BREACHES IN THE HIGHER EDUCATION CONTEXT

Colleges and universities are susceptible to numerous kinds of data breaches due to the vast amount of data they compile from students, faculty, employees, and other individuals affiliated with the campus. In addition to educational records, many colleges and universities have "on-campus healthcare systems, restaurants, book stores, conference centers, research labs and more."[42] One of the reasons higher education institutions are so susceptible to cyber attacks is because of the openness of their online communities.[43] These institutions need to balance the security of their in-

34. RHODES & POLLEY, *supra* note 11, at 22.

35. THOMSON, *supra* note 7, at 23.

36. *See id.*

37. *Id.* at 25.

38. *Data Breaches in Higher Education*, *supra* note 10, at 6.

39. RHODES & POLLEY, *supra* note 11, at 23−24.

40. *See id.* at 23. In June 2014, an official at University of Virginia Law School accidentally sent an email to 160 students releasing personal information related to clerkship applications. Valerie Strauss, *U-Va. Law School Mistakenly Sends Out E-Mail with Private Student Data*, WASH. POST (June 5, 2014), http://www.washingtonpost.com/blogs/answer-sheet/wp/2014/06/05/u-va-law-school-mistakenly-sends-out-e-mail-with-private-student-data/. The email included a great deal of personal information, and was simply a mistake of sending an email to the wrong listserv. *Id.*

41. RHODES & POLLEY, *supra* note 11, at 23−24.

42. *Powerhouses and Benchwarmers*, *supra* note 2, at 5.

43. Matt Zalaznick, *Cyberattacks on the Rise in Higher Education*, UNIV. BUS. (Oct. 2013), http://www.universitybusiness.com/article/cyberattacks-rise-higher-education. The article quotes the Director of the Indiana University for Applied Cybersecurity Research as saying "We want our faculty and our students and our public and

formation systems with their focus on the free flow of information.[44] Colleges and universities "have a complex mix of private and public areas, secure and open networks, and have a vast amount of personal and intellectual property information" that makes them increasingly vulnerable to hacker attack.[45]

The following part will outline the types of data that colleges and universities typically store and what makes them so susceptible to cyber attacks.

a. Information Collected by Medical Centers

Many colleges and universities have medical centers that treat students, as well as the general public, and are a part of the institution itself.[46] These medical centers store medical records and patient information. Under section 13402(e)(4) of the Health Information Technology for Economic and Clinical Health Act (HITECH Act), institutions that experience a breach of unsecured protected health information affecting 500 or more individuals must report to the Secretary of the Department of Health and Human Services, who then must post a list of the breaches.[47] Therefore, the institutions are required to publicize any large-scale compromise of confidential or sensitive information that they have experienced.

Some of the breaches reported since 2013 include two at the University of Pennsylvania Health System.[48] On November 26, 2013, University of Pennsylvania reported a paper breach involving a third party business associate that affected 3,000 individuals.[49] Additionally, there was a paper theft affecting 661 individuals that occurred from May 1, 2014 to June 19, 2014.[50] The paper theft involved stolen receipts from a locked office that

---

our donors to connect pretty easily to us." *Id.*

44. Richard Pérez-Peña, *Universities Face a Rising Barrage of Cyberattacks*, N.Y. TIMES (July 16, 2013), http://www.nytimes.com/2013/07/17/education/barrage-of-cyberattacks-challenges-campus-culture.html?pagewanted=all&_r=0.

45. Sue Poremba, *5 Higher Education Information Security Threats You Should Know Before Your Child Leaves for College*, FORBES (Nov. 5, 2014), http://www.forbes.com/sites/sungardas/2014/11/05/5-higher-education-information-security-threats-you-should-know-before-your-child-leaves-for-college/.

46. *See, e.g.*, *Ronald Reagan UCLA Medical Center*, UCLA HEALTH, https://www.uclahealth.org/reagan/Pages/default.aspx (last visited Apr. 14, 2015).

47. *Breaches Affecting 500 or More Individuals*, HHS, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Apr. 14, 2015). An example of a university having to report a data breach occurred at Duke University Health System on July 1, 2014 when it experienced a theft of a portable electronic device that affected 10,993 individuals. *Id.* For more information on the HITECH Act, *see infra* Part III(c).

48. *Breaches Affecting 5000 or More Individuals*, *supra* note 47.

49. *Id.*

50. *Id.*

included information such as "patient name, date of birth, and the last four digits of credit card numbers."[51] The University sent notification letters and began conducting an internal investigation into the breach.[52]

The University of California – San Francisco (UCSF) experienced a burglary in 2014 of unencrypted desktop computers from a satellite office that contained personal and health information.[53] UCSF launched an investigation into what information was available on those computers and found that the computers stored personal and health information, including "individuals' names, dates of birth, mailing addresses, medical records, health insurance ID numbers, and driver's license numbers."[54] UCSF sent out notification letters, offered credit monitoring, and established a hotline to provide information about the breach.[55]

Sometimes breaches are targeted at campus student health centers, rather than large-scale medical centers. In March 2014, the University of California – Irvine experienced a breach of student information.[56] Three computers in the Student Health Center were infected with a keylogging virus that captured keystrokes as the user typed and transmitted that information to hackers.[57] The information collected included "name, unencrypted medical information" and "bank name" as well as address and other medical information.[58] The University offered free credit reporting services to affected students.[59]

b. Personal Information from Education and Admissions Records

Colleges and universities store a lot of personal information data from students. This data can include name, address, date of birth, social security numbers, and financial information. Two of the largest data breaches of personal information in recent history occurred at the University of Maryland and Indiana University, respectively.

On February 18, 2014, the University of Maryland reported a breach of

51. Stacey Burling, *Penn Medicine Rittenhouse has Data Breach*, PHILLY.COM (July 18, 2014), http://articles.philly.com/2014-07-18/news/51663609_1_data-breach-social-security-numbers-identity-theft.

52. *Id.*

53. Elizabeth Fernandez, *Computer Theft at UC San Francisco*, UNIV. OF CAL. SAN FRANCISCO (Mar. 12, 2014), https://www.ucsf.edu/news/2014/03/112556/computer-theft-uc-san-francisco.

54. *Id.*

55. *Id.*

56. Letter from J. Patrick Haines, Exec. Dir. of the Student Health Ctr., Univ. of Cal. Irvine & Marcelle C. Holmes, Assistant Vice Chancellor for Wellness, Health and Counseling Services, Univ. of Cal. Irvine, to Students (Apr. 21, 2014), *available at* http://oag.ca.gov/system/files/UCIrvine%20Notice%20Letter%20Sample_0.pdf?.

57. *Id.*

58. *Id.*

59. *Id. See also infra* Part V(e).

data systems by a computer security attack.[60] The breached database included 287,580 records of students, staff, faculty, and affiliated persons.[61] The data accessed included name, date of birth, University identification number, and social security number.[62] The University responded by offering free credit monitoring services, launching a large-scale investigation into the breach, and holding information sessions on data privacy.[63]

On February 25, 2014, Indiana University notified the Indiana Attorney General that personal data for students and recent graduates might have potentially been exposed, including names, addresses, and social security numbers for roughly 146,000 individuals.[64] The University opened up a call center to establish whether or not any of the individuals were victims of identity theft.[65] Because the data was encrypted, it was difficult for hackers to decode and ultimately, no cases of identity theft were found.[66] In July 2014, the University shut down the call center and closed the investigation, but not after spending around $130,000.[67]

Personal information can also be found in admissions records. In March 2013, hackers accessed a database of student admission records at Kirkwood Community College in Cedar Rapids, Iowa.[68] They used an international IP address to unlawfully access a website with archived application information.[69] The information accessed "may have included applicant names, birthdates, race, contact information and social security numbers."[70] The Community College responded by alerting law enforcement, hiring an outside firm to do a forensic analysis of the breach, and offering credit monitoring to affected individuals.[71]

c. Financial Information

Colleges and universities have access to student financial information including account balances, loan history, credit information, credit cards,

60. *UMD Data Breach*, UNIV. OF MD., http://www.umd.edu/datasecurity/ (last visited Apr. 14, 2015).

61. *Id.*

62. *Id.*

63. *Id.*

64. *Id.*

65. *IU says no victims reported in data breach*, INDIANAPOLIS BUS. J. (July 17, 2014), http://www.ibj.com/articles/48628-iu-says-no-victims-reported-in-data-breach.

66. *Id.*

67. *Id.*

68. *Kirkwood Website Experienced Unlawful Access*, KIRKWOOD CMTY. COLL. (Apr. 8, 2013), http://kirkwoodonlinenews.org/?p=3947.

69. *Id.*

70. *Id.*

71. *Data FAQs*, KIRKWOOD CMTY. COLL., http://www.kirkwood.edu/datafaqs (last visited Feb. 5, 2015).

debit cards, and other payment forms.[72] Many are also putting in place payment card systems that allow payments on-campus and at certain off-campus venues, which essentially operates as a credit card.[73] Additionally, these institutions often use consumer credit reports for background checks on employees and for determining if students should obtain loans.[74] This wide array of financial information is extremely valuable to hackers interested in identity theft and is therefore very vulnerable to data breaches.

III. LEGISLATION HOLDING COLLEGES AND UNIVERSITIES ACCOUNTABLE FOR DATA SECURITY

Colleges and universities come under the umbrella of a multitude of federal regulations and state statutes. This part will highlight the major regulations that higher education institutions are required to follow, and how they affect institutional decisions.

a. Health Insurance Portability and Accountability Act (HIPAA)

HIPAA focuses on health insurance portability and on the prevention of health care fraud and abuse by adoption of standards and requirements for electronic transmission of health information.[75] There are three separate part of HIPAA's information security component: the privacy regulations, the electronic transaction standards, and the security regulations.[76] These three parts regulate the security standards for protected health information[77], the privacy of patient-identifiable information[78], and the standardization of electronic transactions.[79]

Higher education institutions fall under the definition of a "covered entity" under HIPAA if they provide health care services and engage in one or more covered electronic transaction.[80] Electronic transactions include health care claims, health care payments, coordination of benefits, eligibil-

72. David Shannon & John Farley, Presentation, *Privacy and Network Security Liability in Higher Education* 6, WELLS FARGO INSURANCE SERVICES (Nov. 6, 2012), http://www.dedcmdasfaa.org/docs/conferences/Conference2012Fall/presentations/PrivacyAndNetworkSecurityLiabilityInHigherEducation.pdf.

73. *See* John L. Nicholson & Meighan E. O'Reardon, *Data Protection Basics: A Primer for College and University Counsel*, 36 J.C. & U.L. 101, 115 (2009).

74. *Id.*

75. Toby D. Sitko et al., *Life with HIPAA: A Primer for Higher Education*, CTR. FOR APPLIED RESEARCH (Apr. 1, 2003), *available at* https://net.educause.edu/ir/library/pdf/ERB0307.pdf.

76. *Id.* at 3.

77. *See infra* Part III(i).

78. *See infra* Part III(ii).

79. *Id.*

80. *Id.* at 4.

ity for a health plan, and enrollment in a health plan.[81] Many colleges and universities fall under HIPAA because they provide health services to students and often run medical centers in concert with their medical programs. However, because of the exception for FERPA educational records, if a center solely services students, it may be exempt from HIPAA.[82]

The type of information protected is "individually identifiable health information," defined as "information that is a subset of health information, including demographic information collected from an individual" that "identifies the individual" or provides "a reasonable basis to believe the information can be used to identify the individual."[83] Protected health information does not include "education records covered by [FERPA]" or "employment records held by a covered entity in its role as employer."[84]

The HITECH Act covers electronic medical records, and requires a covered entity to notify affected individuals when unsecured personal health information has been breached.[85] It extended application of both the security and privacy rules of HIPAA.[86] It also amended HIPAA to increase civil and criminal penalties, require notification of data breaches, and change disclosure rules, among others.[87]

i. Security Standards

The Security Rule requires that covered entities have security standards for properly training those who have access to health records, and accounting for the costs of security and the capabilities of systems used in maintenance of health records.[88] Colleges and universities that are considered

---

81. *Id.* at 5, Table 2.

82. Sitko, *supra* note 75, at 9.

83. 45 C.F.R. 160.103 (2014).

84. *Id.* For more information on FERPA, *see infra* Section III (b).

85. Health Information Technology for Economic and Clinical Health Act, P.L. 111-5 §§ 13402, 13407, 123 Stat. 260−71 (Feb. 17, 2009).

86. GINA STEVENS, CONG. RESEARCH SERV., FEDERAL INFORMATION SECURITY AND DATA BREACH NOTIFICATION LAWS 11 (Jan. 28, 2010).

87. *Id.* at 13. HITECH amended HIPAA with the creation of:

> [E]xtended application of certain provisions of the HIPAA Privacy and Security Rules to the business associates of HIPAA-covered entities making those business associates subject to civil and criminal liability for violations; established new limits on the use of protected health information for marketing and fundraising purposes; provided new enforcement authority for state attorneys general to bring suit in federal district court to enforce HIPAA violations; increased civil and criminal penalties for HIPAA violations; required covered entities and business associates to notify the public or HHS of data breaches (regardless of whether actual harm has occurred); changed certain use and disclosure rules for protected health information; and created additional individual rights.

Id.

88. 42 U.S.C. § 1320d-2(d)(1)(A) (2014). The statute states that the "Secretary

covered entities under HIPAA must maintain "reasonable and appropriate administrative, technical and physical safeguards."[89] These safeguards include insuring "the integrity and confidentiality of information" as well as protecting "against any reasonably anticipated" threats to security and unauthorized use of information.[90] It is the responsibility of the covered college or university to "ensure compliance with" the standards "by the officers and employees" of the entity.[91]

Covered entities are required to conduct a risk assessment of their practices that takes into account "the size of the entity, its infrastructure and security capabilities, the cost of security measures, and the potential likelihood that identified threats will exploit security vulnerabilities to compromise the confidentiality, integrity, or availability of" personal health information.[92] The assessment should provide information to the covered entity to aid them in designing personnel screening processes, identify important data, determine "whether and how to use encryption" and "determine the appropriate manner of protecting health information transmissions."[93]

ii. Privacy Safeguards

The privacy rule of HIPAA "limits the circumstances under which an individual's protected health information may be used or disclosed by covered entities."[94] Covered entities are required to ensure that protection information is not used or disclosed in violation of the Act.[95] Entities must set up a security management process that includes a risk analysis, risk management, a sanction policy, and information system activity review.[96] It is important that covered colleges and universities establish a contingen-

---

shall adopt security standards" that assess:

> (i) the technical capabilities of record systems used to maintain health information; (ii) the costs of security measures; (iii) the need for training persons who have access to health information; (iv) the value of audit trails in computerized record systems; and (v) the needs and capabilities of small health care providers and rural health care providers.

Id. at § 1320d-2(d)(1)(A)(i)−(v).

89. 42 U.S.C. § 1320d-2(d)(2) (2014). The "reasonable and appropriate" standard can be contrasted with the Gramm-Leach-Bliley Act "appropriate standard" for security program implementation. 15 U.S.C. § 6801 (2014).

90. *Id.* at § 1320d-2(d)(2)(A)−(B).

91. *Id.* at § 1320d-2(d)(2)(C).

92. ABA SECTION OF ANTITRUST LAW, DATA SECURITY HANDBOOK 27 (2008).

93. *Guidance on Risk Analysis Requirements under the HIPAA Security Rule*, HHS at 3 (July 14, 2010), *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf.

94. STEVENS, *supra* note 86, at 11.

95. 45 C.F.R. § 164.530(c) (2014).

96. 45 C.F.R. § 164.308(a)(1)(ii)(A)–(D) (2014).

cy plan, which requires "policies and procedures for responding to an emergency or other occurrence. . .that damages systems that contain electronic protected health information."[97]

iii. Notification

HIPAA does not require mandatory notification after a breach. However, it is recommended that after "discovery of a breach of unsecured protected health information", each individual is notified if his or her health information "has been, or is reasonably believed. . .to have been, accessed, acquired, used or disclosed as a result of such breach."[98]

iv. Monetary Penalties

HIPAA, following the implementation of the HITECH Act, sets out a detailed penalty scheme for the Secretary to follow when a violation of a provision has occurred. It has penalties specific to when an entity did not know and "by exercising reasonable diligence would not have known" that a provision had been violated.[99] Additionally, there are penalties for when a "violation was due to reasonable cause and not to willful neglect."[100] The greatest penalties attach when an institution acted with willful neglect.[101] The civil penalties can be as low as $100 per violation but cannot exceed $1,500,000 no matter the number of violations.[102] If it is found that the college or university knowingly and deliberately violated HIPAA, criminal penalties can be imposed.[103] If a violation was for personal gain or malicious harm, it could result in ten years' imprisonment.[104]

v. Enforcement

In May 2013, Idaho State University paid $400,000 to the Department of Health and Human Services (HHS) following alleged violations of HIPAA.[105] The penalty stemmed from a breach of unsecured electronic

97. 45 C.F.R. § 164.308(a)(7) (2014).
98. 45 C.F.R. § 164.404(a)(1) (2014).
99. 42 U.S.C. § 1320d-5(a)(1)(A) (2014).
100. *Id.* at § 1320d-5(a)(1)(B).
101. *Id.* at § 1320d-5-(a)(1)(C).
102. Manuel R. Rupe, *Beyond Privacy: FERPA Exceptions and Communication Within the University Regarding Student Conduct*, UNIV. OF COL. OFFICE OF UNIV. COUNSEL (Summer 2007), http://www.ucdenver.edu/life/services/CARE/Documents/FERPA%20Resources.pdf
103. 42 U.S.C. § 1320d-5(a)(3) (2014).
104. 42 U.S.C. § 1320d-6(b)(3) (2014).
105. News Release, *Idaho State University Settles HIPAA Security Case for $400,000*, HHS (May 21, 2013), http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/isu-agreement-press-release.html.html.

protected health information at the University's Pocatello Family Medicine Clinic.[106] A Health and Human Services Office of Civil Rights investigation indicated that the University "did not conduct an analysis of the risk to the confidentiality of [electronic protected health information] as part of its security management process" and "did not adequately implement security measures sufficient to reduce the risks and vulnerabilities."[107]

One year later, in May 2014, Columbia University agreed to settle charges that it had violated HIPAA and pay $1.5 million in HIPAA settlements.[108] In 2010, the medical center, in tandem with New York Presbyterian Hospital, reported a breach of electronic protected health information related to 6,800 individuals.[109] The Office of Civil Rights found that they did not make efforts "to assure that the server was secure and that it contained appropriate software protections."[110]

vi. Private Causes of Action

HIPAA itself does not create a private cause of action; HIPAA can, however, be used to establish a standard of care in a tort action.[111] In *Acosta v. Byrum*, the plaintiff claimed that her doctor improperly allowed his office manager, Robin Byrum, to use his medical record access code number to retrieve the plaintiff's confidential medical and healthcare records.[112] Byrum then provided this information to third parties without the plaintiff's authorization or consent.[113] The plaintiff filed an action alleging negligent infliction of emotional distress against the doctor alongside a claim of invasion of privacy against Byrum.[114] The court allowed the plaintiff to proceed with her claim because HIPAA established the standard of care that the doctor allegedly breached.[115]

A federal district court in Missouri also held that HIPAA may provide a basis for a state law private cause of action.[116] In *I.S. v. Washington University*, the plaintiff alleged that the defendant had forwarded a set of medical records relating to her HIV status, mental health issues, and insomnia

106. *Id.*

107. Resolution Agreement, Idaho State University, HHS (May 13, 2013), http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/isu-agreement.pdf.

108. *Data Breach Results in $4.8 Million HIPAA Settlements*, HHS (May 7, 2014), http://www.hhs.gov/news/press/2014pres/05/20140507b.html.

109. *Id.*

110. *Id.*

111. Acosta v. Byrum, 638 S.E. 2d 246 (N.C. Ct. App. 2006).

112. *Id.* at 249.

113. *Id.*

114. *Id.*

115. *Id.* at 251.

116. I.S. v. Wash. Univ., No. 4:11CV235SNLJ, 2011 U.S. Dist. LEXIS 66043, at *4 (D. Mo. June 14, 2011).

treatments to her employer without her consent.[117] The plaintiff brought a claim for negligence per se using HIPAA, arguing that she was referencing HIPAA solely to establish the standard of care by which to judge whether the defendant's acts were negligent.[118] The court found that a federal statute, such as HIPAA, that does not provide a private cause of action may be a legitimate element of a state law claim.[119]

These two cases, while weak as precedent, suggest that colleges and universities could face suit for negligence using HIPAA as the standard of care, as well as facing civil, criminal or monetary penalties. Under HIPAA, colleges and universities must have strong policies in place to protect patient information and react efficiently if a breach does occur.

b. Family Educational Rights and Privacy Act (FERPA)

FERPA covers educational institutions that receive funds for programs administered by the Department of Education.[120] The information covered includes education records, defined as records that "contain information directly related to a student" and are maintained by the educational institution.[121] Additionally, directory information is covered, defined as information "that would not generally be considered harmful or an invasion of privacy if disclosed."[122] Because directory information is not harmful, all that is required of a covered college or university is "public notice of the categories of information which it has designated as such information."[123]

i. Enforcement

Like HIPAA, FERPA does not establish a private cause of action. Only the Secretary of Health and Human Services can bring an action to enforce FERPA.[124] In *Gonzaga University v. Doe*, the Supreme Court held that a plaintiff could not sue for damages under 28 U.S.C. §1983 to enforce a FERPA provision.[125]

---

117. *Id.* at *3.
118. *Id.* at *3–*4.
119. *Id.* at *4.
120. 20 U.S.C. § 1232g(a)(3) (2014).
121. *Id.* at § 1232g(a)(4)(A).
122. 34 C.F.R. § 99.3 (2014). Directory information includes:

> the student's name, address, telephone listing, date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, and the most recent previous educational agency or institution attended by the student.

20 U.S.C. § 1232g(a)(5)(A) (2014).
123. 20 U.S.C. § 1232g(a)(5)(B) (2014).
124. *See* Girardier v. Webster Coll., 563 F.2d 1267, 1277−78 (8th Cir. 1977).
125. Gonzaga Univ. v. Doe, 536 U.S. 273, 290 (2002).

Unlike HIPAA, courts have found that FERPA cannot be used to establish a state law tort claim. The Sixth Circuit found that FERPA does not support a claim of negligence per se because it does not define a standard of care.[126] Moreover, a district court in North Carolina held that FERPA does not establish a fiduciary relationship so there is evidence that plaintiffs cannot use a FERPA violation to create a state tort claim for breach of fiduciary duty.[127]

While private actors cannot sue using FERPA to support a cause of action, they can file a complaint with the Family Policy Compliance Office or the Secretary of the Department of Education.[128] From there, the Secretary can withhold further payments from the college or university, compelling compliance through a cease and desist order, or terminating eligibility to receive funds under a program.[129] Since the passage of FERPA, "the Family Policy Compliance Office has never withheld funds because voluntary compliance has always been secured."[130]

ii. FERPA and Cloud Computing

Some critics have suggested that FERPA should be amended now that cloud computing is more popular with colleges and universities.[131] Colleges and universities are beginning to take advantage of the convenience of cloud computing as they are drawn to its increased efficiency, mobile access, innovation and access to new services.[132] They are moving storage, messaging, video conferencing and computing power to the cloud.[133] Due to the increased popularity of cloud services, Senators Edward J. Markey and Orrin G. Hatch released a draft FERPA amendment that focuses on regulating private parties with access to student data.[134]

---

126. Atria v. Vanderbilt, 142 Fed. App'x 246 (6th Cir. 2005).

127. McFadyen v. Duke Univ., 786 F. Supp. 2d 887 (D.N.C. 2011).

128. 34 C.F.R. § 99.63 (2014).

129. *Id.* at § 99.67.

130. *FERPA at Idaho State University*, IDAHO STATE UNIV., http://www.isu.edu/areg/policy-proc/ferpafacts.shtml (last visited April 18, 2015).

131. Daniel Solove, *FERPA and the Cloud: Why FERPA Desperately Needs Reform*, SAFEGOV (Dec. 10, 2012), http://www.safegov.org/2012/12/10/ferpa-and-the-cloud-why-ferpa-desperately-needs-reform. Cloud computing is a way for colleges and universities to store their data and access programs over the Internet rather than on a hard drive. Eric Griffith, *What is Cloud Computing?*, PC MAG (Mar. 13, 2013), http://www.pcmag.com/article2/0,2817,2372163,00.asp.

132. Scott Cornell, *Why Colleges Are Chasing Cloud Computing*, FARONICS (Apr. 18, 2013), http://www.faronics.com/news/blog/why-colleges-are-chasing-cloud-computing/.

133. *Id.*

134. *Markey and Hatch Release Discussion Draft of Legislation Addressing Student Privacy* (May 14, 2014), http://www.markey.senate.gov/news/press-releases/markey-hatch-release-discussion-draft-of-legislation-addressing-student-

The only section of FERPA applicable to cloud computing notes that if an educational agency discloses information to a third party, that party must "not disclose the information to any other party without the prior consent of the parent or eligible student."[135] The concern is with the institution's control over the personal data turned over to a third party service. FERPA provides only that a college or university must exercise "direct control" over the third party, but doesn't require any specific standards from the third party.[136] These cloud computing services may also fall within the school official exception, which defines school official as people such as "professors; instructors; administrators; health staff; counselors; attorneys; clerical staff; trustees; members of committees and disciplinary boards; and a contractor, volunteer or other party to whom the school has outsourced institutional services or functions."[137] The exception allows a school to designate the cloud provider as an official to facilitate the sharing of information. As a contractor, a cloud computing service could fall under this exception. The exception would allow the service to access information without prior written consent because of a legitimate educational interest in review of the information.[138] If this analysis proves correct, then it would be incredibly easy for cloud computing services to access and use student information without full disclosure to the students.

iii. FERPA and Online Educational Services

Another concern is the increased use of online educational services, including software, mobile applications, and web-based tools created by third parties and used by colleges and universities.[139] Some of these services use FERPA-protected information, while others collect metadata related to that information.[140] If it only involves "directory information", it falls within an exception.[141] It will be important for colleges and universities to assess each online service and determine whether to notify students and identify the information, if any, that falls under FERPA.

---

privacy.

135. 34 C.F.R. § 99.33(a)(1) (2014).

136. Solove, *supra* note 131.

137. *FERPA General Guidance for Students*, U.S. DEP'T. OF EDUC., http://www2.ed.gov/policy/gen/guid/fpco/ferpa/students.html (last visited April 18, 2015).

138. *Id.*

139. *Protecting Student Privacy While Using Online Education Services: Requirements and Best Practices*, PRIVACY TECHNICAL ASSISTANCE CTR. (Feb. 2014), *available at* http://ptac.ed.gov/sites/default/files/Student%20Privacy%20and%20Online%20Educational%20Services%20%28February%202014%29.pdf.

140. *Id.* at 2. The problem with metadata is that it can have "direct and indirect identifiers" that are considered protected information.

141. *Id.* at 3.

c. State Consumer Protection Statutes

Most states have a data breach notification law.[142] While many have broad provisions that hold anyone in possession of personal information liable for a data breach, some of them are considerably narrower in that they only require notification by specific agencies or businesses in the event of a breach.[143] Moreover, states differ as to who must be notified; some require notification only to consumers, while others require entities to notify credit reporting agencies or the government.[144] California and Illinois have broader requirements and represent a majority of the states that require notification of a breach from any business entity (including higher education institutions) that has access to, and maintains, personal information.

i. California

The California Law on Notification of Security of Breach requires notification to the affected individuals when a data breach of personal information occurs.[145] The type of personal information involves name, social security number, driver's license number, and account or credit card number in combination with an access code or password.[146] Notice must be made in "the most expedient time possible and without unreasonable delay."[147] Entities must notify the consumer and the government, but they are not required to notify credit-reporting agencies.[148] There has been litigation under this law as recently as September 2014 when a federal district court in California granted a Motion to Dismiss in a consolidated action against Adobe Systems, a major software company, for a data breach.[149] The court determined that the plaintiffs did not have standing because they "fail[ed]

142. *See, e.g.*, COLO. REV. STAT. §6-1-716 (2014) (Colorado); FLA. STAT. §501.171 (2014) (Florida); 815 ILL. COMP. STAT. 530/1 et seq. (2014) (Illinois); N.Y. GEN. BUS. LAW §899-aa (2014) (New York). New York City even has a regulation specific to the personal information of New York City Residents. N.Y. CITY ADMIN. CODE §20-117 (2014).

143. *See, e.g.*, R.I. GEN. LAWS § 11-49.2-3(a) (2014) (requiring notification only by state agencies that maintain personal information).

144. *See, e.g.*, ALASKA STAT. § 45.48.040 (2014) (requiring entities to notify a credit reporting agency); DEL. CODE ANN. TIT. 6 § 12B-102(a) (2014) (requiring entities to notify only the "affected Delaware resident"); ID. CODE ANN. § 28-51-105(1) (2014) (requiring entities to notify the state attorney general).

145. CAL. CIV. CODE § 1798.82 (2014). Data breach is defined as "the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal informationFalse" *Id.* at § 1798.82(g).

146. *Id.* at § 1798.29(e).

147. *Id.* at § 1798.82(a).

148. *Id.* at §1798.82.

149. In re Adobe Sys. Privacy Litig., No. 13-CV-05226-LHK, 2014 U.S. Dist. LEXIS 124126, at *77 (N.D. Cal. Sept. 4, 2014).

to allege any injury resulting from a failure to provide reasonable notification of the 2013 data breach."[150]

California also has a separate law regarding data protection.[151] The difference between this law and the notification law is that this law covers information about a California resident, regardless of whether the business that owns or licenses the information conducts business in California.[152] The business must "implement and maintain reasonable procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."[153] Personal information includes the same information as outlined in the notification law. Therefore, a college or university outside of California that does not adequately protect information about a student who resides in California could be held liable.

An injured person can bring a civil action to recover damages under either the notification law or the data protection law.[154] They can receive civil penalties for "willful, intentional, or reckless violation[s]."[155]

ii. Illinois

In Illinois, the Personal Information Protection Act covers data collectors, which explicitly includes private and public universities.[156] A breach is defined as an "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information."[157] Notice to affected individuals must be accomplished "in the most expedient time possible and without unreasonable delay."[158] Violating the Act is considered an unlawful practice under Illinois's Consumer Fraud and Deceptive Business Practice Act.[159] Under the Act, only notifi-

150. *Id.* at 38.

151. CAL. CIV. CODE § 1798.81.5 (2014).

152. *Id.* at § 1798.81.5(b). This means that colleges and universities located outside of California may be subject to the law even if they have just one student from California. John L. Nicholson et. al, *Data Privacy Issues – Know Your Rights and Responsibilities*, NACUA (Jun. 22−25, 2008), *available at* http://www.higheredcompliance.org/resources/publications/Data-Privacy-Issues1.doc. North Carolina's notification statute also applies to entities that do not have to be conducting business within the state. N.C. GEN. STAT. § 75-65(a) (2014).

153. *Id.*

154. *Id.* at § 1798.84(b).

155. *Id.* at § 1798.84(c). A willful, intentional or reckless violation can lead to a civil penalty of up to $3,000. *Id.* However, a pure violation can still entitle a victim to up to $500. *Id.*

156. 815 ILL. COMP. STAT. 530/5 (2014).

157. *Id.* The personal information covered is the same as in California, including name, social security number, driver's license number, and credit card information. *Id.*

158. *Id.* at 530/10(a).

159. *Id.* at 530/20.

cation to consumers is required; entities are not required to report to credit reporting agencies or the government.[160]

d. FTC Action

Colleges and universities can fall under the regulatory umbrella of the FTC through the Gramm-Leach-Bliley Act (GLBA)[161] or the Red Flags Rule[162] When colleges and universities participate in financial activities, such as making federal loans, they fall under the regulations of the FTC as a financial institution for purposes of GLBA. GLBA requires an information security program coordinated by the institution, including identification of reasonably foreseeable risks and oversight of service providers.[163] GLBA has a privacy rule that educational institutions are exempt from if they comply with FERPA.[164] This is because the FTC felt that the privacy regulations under FERPA were adequate and FERPA compliance would be equivalent to compliance under GLBA.[165] However, under the Safeguards Rule of GLBA, there is no exemption for institutions that are subject to FERPA, likely because there is no equivalent requirement under FERPA.[166] The Safeguards Rule requires financial institutions to have a written information security program that ensures the safety of customer records, protects against anticipated threats and protects against unauthorized access.[167]

The FTC Red Flags Rule can be applied to colleges and universities.[168] The Red Flags Rule is a part of the Fair and Accurate Credit Transactions Act.[169] The National Association of College and University Business Officers identified several areas of the Rule that can cause colleges and universities to fall under the rule as creditors.[170] This includes institutions that participate in the Federal Perkins Loan program[171], act as a school lender in

160. *Id.* at 530/10(a).
161. 16 C.F.R. § 314.1 (2014).
162. 16 C.F.R. § 681.1 (2014).
163. 16 C.F.R. § 314.4 (2014).
164. *FTC's Gramm-Leach-Bliley Act Safeguards Rule: Guidelines for Compliance*, NACUA (May 16, 2003), http://www.nacua.org/nacualert/docs/GLB_Note_051603i.html.
165. Privacy of Consumer Financial Information, 65 Fed. Reg. 33,648 (May 24, 2000).
166. *Id.*
167. 16 C.F.R. § 314.3(a) (2014).
168. 16 C.F.R. § 681.1 (2014).
169. *Id.*
170. Larry Ladd, *The Red Flags Rule: What Higher Education Institutions Need to Know*, GRANT THORNTON, *available at* http://www.grantthornton.com/staticfiles/GTCom/Advisory/GRC/Red%20Flags%20materials/Red%20Flags%20Rule%20White%20Paper%20(Higher%20Ed)%209_21.pdf.
171. 34 C.F.R. § 674 (2015).

the Federal Family Education Loan Program[172], offer institutional loans, or offer a payment plan for tuition that runs throughout the semester as opposed to requiring a full payment at the start of the semester.[173]

The rule requires a plan to identify, detect, and respond to attempts to use stolen identity information. The plan must include identification of relevant Red Flags, detect Red Flags in the program, respond appropriately to Red Flags to prevent and mitigate identity theft, and ensure periodic update of the program.[174] A Red Flag is defined as "a pattern, practice, or specific activity that indicates the possible existence of identity theft."[175] The Rule provides that after December 31, 2010, any occurrence of identity theft could expose an institution to an FTC investigation.[176] If there is a violation of the rule, institutions are required to submit additional compliance reporting and could be subject to an injunctive compliance order.[177] Further violations can lead to monetary penalties of up to $16,000 per occurrence and a potential civil suit in federal court.[178] Like HIPAA, an individual can use the Red Flags Rule as the standard of care in a private suit.[179]

Like many other colleges and universities, the University of Wisconsin has a policy in response to the Red Flags Rule.[180] The policy requires university personnel who administer covered accounts to take steps to prevent and mitigate identity theft when Red Flags are detected.[181] These steps include: monitoring covered accounts, contacting account holders, changing passwords, notifying law enforcement, and attempting to identify the cause and source of the Red Flag.[182]

The National Association of College and University Business Officers provides sample policies for compliance with the Red Flags Rule.[183] One of these is the policy from the University of California – Los Angeles.[184]

---

172. 20 U.S.C. §§ 1087aa-ii (2012).

173. *Id.* at 2.

174. 16 C.F.R. § 681.1(d)(2) (2014).

175. 16 C.F.R. § 681.1(b)(9) (2014).

176. Ladd, *supra* note 149.

177. *Id.*

178. *Id.*

179. *Id.*

180. *Red Flag Rules*, UNIV. OF WIS., http://www.uwc.edu/money-matters/business-office/red-flag-rules (last visited April 18, 2015).

181. *Id.*

182. *Id.* It is important for personnel to take mitigating steps such as changing passwords, requesting additional documentation, and closing existing accounts if there is any sign of a Red Flag. *Id.*

183. *FTC Red Flags Rule*, NACUBO, http://www.nacubo.org/Business_and_Policy_Areas/Privacy_and_Intellectual_Property/FTC_Red_Flags_Rule.html (last visited Feb. 7, 2015) (linking to sample policies for Red Flags Rule compliance from colleges and universities such as University of Puget Sound and Xavier University).

184. *Red Flag Regulation Implementation at UCLA Student Financial Services*,

The policy requires each manager in Student Financial Services to "maintain responsibility for the implementation and ongoing support of this regulation."[185] It also requires quarterly audits of compliance procedures.[186]

Beyond the regulations that specifically apply to colleges and universities, the FTC has used "its authority to police unfair and deceptive trade practices" to enforce privacy policies.[187] It relies on Section 5 of The Federal Trade Commission Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce."[188] While the FTC very rarely levies fines against violators of Section 5, the FTC can influence reputation by bringing bad press and instilling fear in companies by threatening a lengthy auditing process.[189] When the FTC reasonably believes that Section 5 is being violated, it initiates an enforcement action and investigates the company before issuing a complaint or order that usually ends in a settlement.[190] The FTC currently uses this enforcement power to regulate for-profit colleges and vocational schools, and to ensure that these institutions are not committing unfair trade practices by misleading students as to their accreditation, facilities, qualifications, and employment prospects.[191]

Because the FTC is charged with regulating commerce and profit-making activities, it suggests that the FTC cannot control the actions of colleges and universities that are not for-profit institutions.[192] If this reasoning is correct, then the FTC cannot bring an enforcement action against a college or university for violation of their privacy policy because students are not considered consumers, and nonprofit educational institutions are not considered profit-making institutions. The Department of Education is tasked with regulating privacy in the education context; it is unlikely that the FTC will take over this role despite its ever-expanding role as privacy regulator.[193]

e. Private Causes of Action

It is possible for a student, employee, faculty member, or third party to

---

UNIV. OF CAL. – LOS ANGELES (Jan. 1, 2009), *available at* http://www.nacubo.org/documents/business_topics/UCLA_Redflags.pdf.

185. *Id.*

186. *Id.*

187. Daniel J. Solove & Woodrow Hartzog, *The FTC and The New Common Law of Privacy*, 114 COLUM. L. REV. 583, 585 (2014).

188. 15 U.S.C. § 45(a)(1) (2012).

189. Solove & Hartzog, *supra* note 187, at 604−06.

190. *Id.* at 609.

191. Guides for Private Vocational and Distance Education Schools, 78 Fed. Reg. 68,987, 68, 990 (Nov. 18, 2013).

192. Woodrow Harztog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 G.W. L. REV. (forthcoming 2015).

193. *Id.* at 29–30.

bring an action against a college or university.[194] However, private causes of action are limited when it comes to holding a college or university liable for a data breach. As discussed earlier, FERPA cannot be used to supplement a private cause of action. HIPAA can be used, but only to establish a standard of care. The problem is that, to date, courts have been reluctant to say that institutions have a duty to protect their students from data breaches.

Case law over the past forty years has suggested that colleges and universities, as well as their employees, could have a duty to their students. In *Duarte v. State*, a California court found that a college had a duty to protect students from third-party attack due to its superior control over the residential facility where the attack occurred.[195] The court also noted that the college was responsible for providing adequate security for foreseeable risks.[196] In *Niles v. Board of Regents of the University System of Georgia*, a Georgia appellate court said that a duty to warn or protect a student is dependent "upon the foreseeability of the [danger]" as well as the student's knowledge.[197] Moreover, in *Peschke v. Carroll College*, the Montana Supreme Court found that a college had a duty to provide a reasonably safe environment for its students after a priest's inaction led to an on-campus shooting, but the court did not think that this meant the college was automatically liable for the injury.[198]

While these cases primarily involve physical injury to students, it could be interpreted that colleges and universities also have a duty to protect student information given the level of control these institutions have over the information.

However, an Illinois Appellate Court held that there is no common law duty to safeguard personal information for purposes of a negligence claim in a K–12 setting.[199] In *Cooney v. Chicago Public Schools*, the plaintiffs filed a lawsuit against their employer, Chicago Public Schools, after a printing company mistakenly sent a list including personal information to employees, rather than the intended COBRA Open Enrollment List.[200] The defendant notified the employees of the breach and offered one year of free

194. *See, e.g.*, ABA SECTION OF ANTITRUST LAW, DATA SECURITY HANDBOOK 122 (2008) (detailing a tort theory that plaintiffs could bring regarding data security). As is true of most negligence actions, the tort theory involves a showing that: (1) the defendant had a duty to secure the information, (2) the defendant breached the duty, (3) the breach proximately caused the plaintiff's harm, and (4) the plaintiff suffered actual harm. *Id.*

195. 148 Cal. Rptr. 804, 812 (Ct. App. 1978).

196. *Id.*

197. 473 S.E.2d 173, 175 (Ga. App. 1996).

198. 929 P.2d 874 (Mont. 1996).

199. Cooney v. Chicago Pub. Sch., 943 N.E.2d 23 (Il. App. Ct. 2010).

200. *Id.* at 27.

credit protection insurance.[201] The court determined that there was no common law duty to safeguard information so there could be no negligence claim against the defendant.[202] However, an analysis of the case found that "both the majority and the dissent agreed that a data security statute can be used to establish a duty for negligence purposes even if the underlying statute does not itself provide a private right of action."[203] This supports the assertion that HIPAA, as a data security statute, could serve as the standard of care in the case.

IV. PRIVATE LITIGATION RESULTING FROM DATA BREACHES

There have been over seven hundred data breaches involving educational institutions in the past nine years, some of which have resulted in class action litigation. The following part will highlight recent class action suits against educational institutions, as well as college and university medical centers. While there were a variety of claims brought against these institutions, most ended with a settlement agreement.

a. Class Action Suit Against University of Hawaii

Between April 2009 and June 2011, multiple campuses of the University of Hawaii were accused of releasing the private information of 90,000 individuals.[204] The affected information included names, social security numbers, phone numbers, address, and credit card information.[205] Some of the affected individuals filed a class action complaint against the University.[206] The University settled the lawsuit and provided the free benefits asked for by the class members.[207] The cost of providing all the benefits was approximately $550,000 plus attorneys' fees and costs.[208]

---

201. *Id.*

202. *Id.* at 29.

203. *IL Appellate Court: No Duty Exists to Safeguard SSNs for Purposes of a Negligence Claim*, INFORMATION LAW GROUP (Feb. 3, 2010), http://www.infolawgroup.com/2011/02/articles/lawsuit/il-appellate-court-no-duty-exists-to-safeguard-ssns-for-purposes-of-a-negligence-claim/.

204. *Frequently Asked Questions*, University of Hawai'i Data Breach Settlement, http://uhdatabreachlawsuit.com/?q=node/3 (*last visited* Apr. 14, 2015). The affected campuses included Kapiolani Community College in April 2009, Honolulu Community College in May 2010, University of Hawai'i at Manoa in June 2010, University of Hawai'i at West Oahu in October 2010, and Kapiolani Community College in June 2011. *Id.*

205. *Id.*

206. Complaint at *1, Gross v. Univ. of Hawai'i et al, No. 1:10cv684 (D. Haw. Nov. 18, 2010), ECF No. 1.

207. *Frequently Asked Questions*, *supra* note 204. Class members asked for "Continuous Credit Monitoring Services, Call Center, Consultation Services, and Restoration services" for two years. *Id.*

208. *Id.*

b. Class Action Suit Against Maricopa County Community College District

In 2013, the Maricopa County Community College District experienced a large-scale data breach involving academic and personal data of 2.4 million current and former students, and employees.[209] While the breach occurred in April 2013, students were not notified until November of that year.[210] The compromised information included employee social security numbers, driver's license numbers, bank account information, and student academic information.[211] The Community College District decided to spend $7 million to notify parties and to fund repairs, including the construction of a call center facility.[212]

The victims of the breach filed a class action complaint against the Community College District on April 28, 2014.[213] They allege negligence, negligence per se under two Arizona state statutes, breach of fiduciary duty, bailment, breach of the right of privacy, and violation of a federal statute related to the unlawful disclosure of personal information from a motor vehicle record.[214] The first negligence per se claim was brought under A.R.S. 41-4172 which requires the entity to "develop and establish commercial reasonable procedures to ensure that entity identifying information and personal identifying information. . .is secure and cannot be accessed, viewed or acquired unless authorized by law."[215] The other negligence per se claim was brought under A.R.S. 44-7501, which establishes "a duty of reasonable care to notify in a timely manner if [personal identifying information] or other sensitive information was potentially exposed to unauthorized access."[216] The case has been removed to federal court.

In May 2014, the District had to approve an additional $2.3 million to pay for lawyers' fees, as well as $300,000 for records management, which brought the total amount spent on the breach to $20 million.[217] In order to pay for the data breach, the Maricopa County Community College District

209. Mary Beth Faller, *Maricopa Colleges waited 7 months to notify 2.4 million students of data breach*, ARIZ. REPUBLIC (Nov. 27, 2013), http://archive.azcentral.com/community/phoenix/articles/20131127arizona-college-students-data-breach.html.

210. *Id.*

211. *Id.*

212. *Id.*

213. Class Action Complaint, Roberts v. Maricopa County Cmty. Coll. Dist., No. CV2014-007411 (Ariz. Super. Ct. Apr. 28, 2014).

214. *Id.*

215. *Id.*

216. *Id.*

217. Mary Beth Faller, *Data Breach Costs Approach $20 Million*, ARIZ. REPUBLIC (May 20, 2014), http://www.azcentral.com/story/news/local/phoenix/2014/05/19/data-breach-costs-approach-million/9312729/.

increased the tax levy.[218] The two percent increase will bring in $21 million in revenue, $7.2 million of which will be spent on the information technology department.[219]

Databreaches.net filed a complaint regarding the breach with the FTC in June 2014.[220] The complaint asked that the FTC investigate the District's data practices and security configurations.[221] It also accused the District of failing to "remedy known security vulnerabilities" implementing "the recommendations of its own personnel's strategic plan that had recommended common and industry-standard approaches to good data security."[222] The complainant believed that the District's practices were so inadequate that they had violated the Safeguard Rule[223] and asked that the FTC take action against the conduct.[224]

c. Suit Against Stanford Hospital and Clinics

A business associate of Stanford Hospital and Clinics, located in Palo Alto, California, experienced a data breach when a subcontractor caused a health information breach.[225] Information regarding 20,000 patients treated by the hospital's emergency department was posted on a website, affecting patients treated between March 1, 2009 and August 31, 2009.[226] This information included patient names, medical records, hospital account numbers, emergency room dates, and medical codes detailing the reasons for the visit and billing charges.[227] Despite hospital action to remove the information within twenty-four hours of discovery, the information was posted online for nearly a year.[228]

---

218. Mary Beth Faller, *Maricopa College District Raises Property Taxes*, ARIZ. REPUBLIC (May 28, 2014), http://www.azcentral.com/story/news/local/phoenix/2014/05/28/maricopa-college-district-raises-property-taxes/9677067/.

219. *Id.*

220. Complaint by Dissent, In the Matter of Maricopa County Cmty. Coll. Dist., FTC (Jun. 14, 2014), *available at* http://www.databreaches.net/wp-content/uploads/MCCCD_SafeguardsRule.pdf. The complainant uses Dissent as a pseudonym, and is a privacy advocate and blogger with Databreaches.net. *Id.* at 2.

221. *Id* at 6.

222. *Id*.

223. 16 C.F.R. 314 (2014).

224. *Id.* at 7.

225. Howard Anderson, *Stanford Reports Website Breach*, HEALTHCARE INFO SECURITY (Sep. 9, 2011), http://www.healthcareinfosecurity.com/stanford-reports-website-breach-a-4038?webSyncID=48311491-1e00-80ab-6632-dbb9dbc56bba&sessionGUID=224eea96-7db7-b72e-9ca4-132222770896.

226. *Id*.

227. *Id*.

228. *Id.* The hospital released a statement regarding the actions taken to remedy the breach:

> Stanford Hospital & Clinics has been working very aggressively with the vendor to determine how this occurred in violation of strong contract com-

Some of the victims brought a class action suit against the Medical Center and the vendors.[229] The suit settled for $4 million including attorneys' fees in March 2014.[230] A provision of the California Confidentiality of Medical Information Act allowed the patients to bring an action against the entity seeking minimum damages of $1,000 per person with no proof of actual damage required because the entity negligently released individually identifiable medical information.[231] As part of the settlement, the Health Center agreed to contribute $500,000 to create an educational project managed by the California HealthCare Foundation.[232]

d. Suit Against University of Pittsburgh Medical Center

In 2014, the personal and financial information of 62,000 employees at the University of Pittsburgh Medical Center (UPMC) was compromised in a major data breach.[233] UPMC sent a letter to victims explaining, "[E]mployees were targeted by a fraudulent tax return scheme."[234] In February 2014, some of the victims brought a lawsuit against UPMC following the breach of personal information.[235] The suit claimed that the Medical Center and its payroll processor were negligent in the measures they took to protect employee information.[236] Larry Ponemon, the President and Founder of Ponemon Institute, a cybercrime researcher, said that the average cost of the data breach would be $201 per record, which includes the

---

> mitments to safeguard the privacy and security of patient information. The vendor . . . is conducting its own investigation into how its contractor caused patient information to be posted to the website, and the hospital may take further action following completion of the investigation.

Id. (omission in original).

229. Complaint at *1, Springer v. Stanford Hosps. & Clinics, No. BC470522 (Cal. Super. Ct. Sep. 28, 2011).

230. Marianne Kolbasuk McGee, *Stanford Breach Lawsuit Settled*, DATA BREACH TODAY (Mar. 24, 2014), http://www.databreachtoday.com/stanford-breach-lawsuit-settled-a-6670.

231. *Id.*

232. *Id.*

233. Marianne Kolbasuk McGee, *Victim Tally in UPMC Breach Doubles*, DATA BREACH TODAY (June 2, 2014), http://www.databreachtoday.com/victim-tally-in-upmc-breach-doubles-a-6901.

234. Letter from John P. Houston, Vice President, Privacy and Information Security & Associate Counsel, UPMC, to Employees, *available at* http://www.wtae.com/blob/view/-/25534940/data/1/-/16bay7z/-/Letter-to-UPMC-workers.pdf. The letter notified employees that they would receive identity theft protection services free of charge, and also urged employees to contact credit card companies, the IRS, and banks to notify them of the breach. *Id.*

235. Brian Bowling, *Class-action Lawsuit Targets UPMC, Software Company for Big Data Breach*, TRIBLIVE (May 9, 2014), http://triblive.com/news/adminpage/6086833-74/upmc-software-says#axzz3D2glL6rr.

236. *Id.*

cost of an investigation and a one-year period of credit monitoring for each victim.[237]

The complaint alleged the defendants had a duty to protect the private, confidential, personal and financial information and the tax documents of the plaintiffs.[238] The plaintiffs claimed negligence and breach of contract.[239] The plaintiffs discussed the Federal Trade Commission's guidance on "Protecting Personal Information: A Guide for Business" and argued that because UPMC violated those administrative guidelines by failing to ensure adequate data security, they failed to meet industry standards.[240] The plaintiffs also alleged that UPMC's failure to maintain adequate security practices caused actual damages to the plaintiffs because personal information was used to file fraudulent tax returns.[241] Additionally, the plaintiffs alleged that they were put "at an increased and imminent risk of becoming victims of identity theft crimes, fraud and abuse" and needed to spend "considerable time and money to protect themselves."[242] As of this writing, the case remains unresolved.

V. HOW COLLEGES AND UNIVERSITIES SHOULD PREPARE AND REACT TO BREACHES

As stated earlier, it is rare for colleges and universities to be sued by private plaintiffs for torts such as negligence with regards to data breaches, and governmental action is also rare, but the preceding section shows that, of late, data breach suits have become more common. It is important that colleges and universities take preventive measures to ensure the safety of student, faculty, and employee data. There are also remedial measures that must be implemented immediately when a higher education institution learns of a potential data breach. This part will detail preventive measures such as proper information technology policies, encryption, and insurance. It will also address remedial measures such as timely notification, offering free credit monitoring, and properly defending itself in a class action suit.

a. Information Technology Best Practices & Security Policies

The best way for colleges and universities to ensure that they will not be held liable for a cyber attack is to institute comprehensive information technology policies. Higher education institutions should create a "written information security plan" that "outlines data security methodologies and

237. *Id.* The total cost of the breach could be as much as $5 million. *Id.*

238. Second Amended Class Action Complaint at 4, Dittman v. UPMC, No. GD-14-003285 (Pa. County Ct. June 25, 2014).

239. *Id.* at 13–15.

240. *Id.* at 7–8.

241. *Id.* at 9.

242. *Id.*

gives users insight into their role in data protection."[243] The plan should detail how data is collected, stored and protected.[244] Moreover, there should be an incident response plan in place to complement the information security plan that sets up a clear response in the event of data vulnerability.[245]

An example is Princeton University, which has a detailed information technology policy in place.[246] The policy acknowledges that personal information is "protected by federal and state laws or contractual obligations that prohibit its unauthorized use or disclosure."[247] The University holds employees responsible for assessing the sensitivity of information and ensuring adequate protection for that information.[248] Additionally, the University requires that personally identifiable information not be stored or used unless there is a legitimate business need and there is no reasonable alternative for the information.[249] Perhaps the most important part is that the policy sets out guidelines for employees and contractors alike, requiring third parties with access to confidential information and technology services take the necessary secure steps.[250]

According to the New York Times, some unnamed institutions are being so cautious as to not allow professors to take laptops abroad.[251] This is because a majority of hacks originate overseas, especially in China.[252] When professors visit these countries, the hackers have become advanced enough that they copy the entirety of the professor's hard drive the moment he or she connects to a network.[253] Some of them plant a virus or some other type of malware on the computer that will activate when the computer connects to the home network upon arrival back at the professor's home institution, giving the hackers access to the entire college or university net-

---

243. Deena Coffman, *Managing Data Protection in Higher Education*, RISK MANAGEMENT MAGAZINE (Sep. 1, 2014), http://www.rmmagazine.com/2014/09/01/managing-data-protection-in-higher-education/.

244. *See id.*

245. *Id.*

246. *Information Security Policy*, PRINCETON UNIV. (Nov. 10, 2009), http://www.princeton.edu/oit/it-policies/it-security-policy/#comp0000503ecd50000001f1a12a0c.

247. *Id.* The policy outlines the applicable statutes, including FERPA, HIPAA, the Red Flags Rule, the Electronic Communications Privacy Act, and the Computer Fraud and Abuse Act. *Id.*

248. *Id.*

249. *Id.* This information includes social security number, date of birth, place of birth, mother's maiden name, credit card numbers, bank account numbers, income tax records, and driver's license numbers. *Id.*

250. *Id.*

251. Pérez-Peña, *supra* note 44.

252. *Id.*

253. *Id.*

work.[254]

It would also be good practice for colleges and universities to participate in voluntary self-assessments of information security. There are many ways to review cyber security practices, such as the Cyber Resilience Review or the Cybersecurity Evaluation Tool.[255] One of the difficulties with implementing these assessments is that college and universities are often understaffed in their technology departments.[256] One study found that thirty-nine percent of organizations had inadequate staffing for security and twenty-eight percent claimed that their personnel lacked the proper security skills.[257] Dell Incorporated, a major American computer technology company, suggests that institutions should partner with third-party security services to help prepare and deal with cybersecurity threats.[258] However, as previously discussed, giving third parties access to confidential information creates a different onslaught of issues related to HIPAA and FERPA protections.

b. Encryption

Encryption is defined as "the process of obscuring information to make it unreadable without a decryption key.[259] The goal of encryption is to make sure that "even if sensitive information is compromised, it remains useless to anyone without a key to decrypt it," although some advanced hackers have the ability to override any sort of encryption.[260] The American Bar Association suggests that any organization that collects any kind of sensitive information should create an encryption policy to secure the data in the event that it becomes compromised.[261]

In Texas, a state regulation requires higher education institutions to implement encryption procedures.[262] It requires encryption of confidential information that is transmitted over the Internet or stored in a public location.[263] It also discourages storage of confidential information on portable

254. *Id.*

255. *See* Presentation, Amy Banks & DeShelle Cleghorn, *Integrating Cybersecurity with Emergency Operations Plans (EOPs) for Institutions of Higher Education (IHEs)*, READINESS & EMERGENCY MANAGEMENT FOR SCHOOLS, http://rems.ed.gov/Docs/Integrating_Cybersecurity_with_EOPs_for_IHEs_slides.pdf.

256. *Top 2 Information Security Challenges for Higher Education*, DELL SECUREWORKS, http://www.secureworks.com/assets/pdf-store/white-papers/wp-top-2-info-security-challenges-for-higher-edu.pdf.

257. *Id.* at 2.

258. *Id.* at 3.

259. ABA SECTION OF ANTITRUST LAW, DATA SECURITY HANDBOOK 19 (2008).

260. *Id.*

261. *Id.*

262. 1 TEX. ADMIN. CODE §202.75(4) (2014).

263. *Id.* at § 202.75(4)(A)–(B).

devices and requires encryption if it is used on portable devices.

Although encryption does not insure against data breaches, it is a step in the right direction toward data protection. Encryption protects confidential data by making it more difficult for hackers to discern what the information is and who is belongs to. It is a necessary step for colleges and universities to take to show students and employees that they are serious about data protection.

c. Offsetting Costs with Cyber Insurance

One of the most difficult parts of a data breach is the financial implication for the college or university. Oftentimes, these institutions are not prepared for the high costs of remedying a breach and providing services to victims of the breach.[264] Additionally, few institutions actually have cyber insurance to help offset these costs.[265] Expenses can include "forensics consultants, lawyers, call centers, websites, mailings, identity-protection and credit-check services, and litigation."[266] An intangible expense is the damage to an institution's reputation that occurs when they experience a breach of data security.[267] It can be especially difficult for public institutions that rely on state funding to absorb the costs of a cyber attack.[268]

Data Breach Insurance is available to colleges and universities to help protect them in case a breach occurs.[269] As the threat of cyber attacks increases, so do the number of companies buying cyber insurance.[270] Some insurance carriers are beginning to specifically market cyber insurance for higher education institutions.[271] Insurance can cover both the tangible ex-

---

264. Megan O'Neil, *Data Breaches Put a Dent in Colleges' Finances as Well as Reputations*, CHRON. HIGHER EDUC. (Mar. 17, 2014), http://chronicle.com/article/Data-Breaches-Put-a-Dent-in/145341/ (noting that "[f]ew institutions budget in advance for data breaches").

265. *Id.*

266. *Id.*

267. *Id.*

268. Pérez-Peña, *supra* note 44 (discussing how the University of California – Berkeley has had to double its cybersecurity budget, already in the millions, in response to a huge increase in attempted cyber attacks).

269. *See Data Breach Insurance Protection*, THE HARTFORD, http://www.thehartford.com/data-breach-insurance/ (last visited November 12, 2014). The Hartford offers Data Breach Insurance to companies, providing "access to professionals who can help you comply with regulatory requirements" and "guidance on how to help prevent a data breach and handle a breach crisis if one occurs." *Id.*

270. *See* Deirdre Fernandes, *More Firms Buying Insurance for Data Breaches*, BOSTON GLOBE, Feb. 17, 2014, http://www.bostonglobe.com/business/2014/02/17/more-companies-buying-insurance-against-hackers-and-privacy-breaches/9qYrvlhskcoPEs5b4ch3PP/story.html (discussing how "one in three companies now has insurance to specifically protect" against losing customer information).

271. *See CyberEdge*, AIG, http://www.aig.com/CyberEdge_3171_417963.html (last visited Nov. 13, 2014) (offering cyber security insurance to protect third-party loss

penses as well as efforts to recover any damages to the institution's reputation. The benefits of insurance include protections for breach of contract claims, computer forensics, notification costs, regulatory actions, healthcare protections in the case of an on-campus medical center, and hacker damage.

Unfortunately, cyber insurance is expensive and oftentimes difficult to obtain.[272] Some insurance companies require institutions to have strong security procedures in place in order to be eligible for insurance.[273] If colleges and universities are implementing proper procedures per the FERPA guidelines[274] and the GLBA Safeguard Procedures[275], they should have no problem adhering to the standards set forth by insurance companies.

d. Timely Notification

It is important for colleges and universities to know their state's data breach notification law. Each state's law can vary in the definition of what constitutes a data breach, what timely notification is, and who needs to be notified. Moreover, some states are imposing data protection on out-of-state entities, meaning "physical presence in the state is often not required for an institution to be subject to the law."[276] Therefore, if an institution has students from a wide array of states, they may be subject to the notification requirements of each state.

Timely notification differs by state. In Florida, notification must occur "no later than 30 days following determination of the breach."[277] Some state statutes do not have a set amount of time but rather require notification "in the most expedient time possible and without unreasonable delay."[278] It is in the best interest of colleges and universities to become familiar with the data breach statute of their home state, but also to keep in mind that they might be required to notify students in accordance with the student's home state.[279]

e. Free Fraud Protection

Most colleges and universities deal with breaches by offering free credit

---

resulting from a cyber attack, lost income, and other costs resulting from a breach).

272. O'Neil, *supra* note 264.

273. *Id.*

274. *See supra* Section III(b).

275. *See supra* Section III(d).

276. Nicholson & O'Reardon, *supra* note 73, at 119.

277. FL. STAT. §501.171 (2014).

278. LA. REV. STATS. CH. §51:3074 (2005).

279. For an overview of all state notification statutes, *see State Data Security Breach Notification Laws*, MINTZ LEVIN, http://www.mintz.com/newsletter/2007/PrivSec-DataBreachLaws-02-07/state_data_breach_matrix.pdf (last visited Dec. 4, 2014).

monitoring to the affected students. This involves high costs for the colleges and universities, which might make it more difficult for public entities to fund. Indiana University reacted to a data breach by supplying "Social Security numbers and names of those potentially affected to all three major credit-reporting agencies."[280] California State University East Bay sent a letter to affected parties offering complimentary 12-month credit monitoring services.[281] The University of Maryland offered five years of free credit monitoring.[282]

Offering credit monitoring is a positive response to a data breach that might convince victims not to bring suit and convince the court not to levy too harsh a penalty in the case of a suit.

f. Lack of Standing Argument

One of the most difficult hurdles for class action plaintiffs suing for losses incurred as a result of a data breach is proving that they have standing. Most of the previous cases involving data breaches have settled prior to the class certification stage. The issue is the inability to show a tangible injury. The Supreme Court ruled on Article III standing in federal class action suits in *Clapper v. Amnesty International, USA* in 2013.[283]

The *Clapper* decision involved human rights groups, public interest lawyers, and media organizations that claimed that the wiretapping program under the Foreign Intelligence Surveillance Act affected their work.[284] The question before the court was whether the respondents had Article III standing to seek prospective relief.[285] The respondents asserted that their injury in fact was an "objectively reasonable likelihood that their communications" could be acquired under the Act in the future.[286] The Court determined that this theory was "too speculative to satisfy the well-established requirement that threatened injury must be 'certainly impending.'"[287] In order for the plaintiffs in the underlying litigation to be affected

280. *Indiana University Reports Potential Data Exposure*, IND. UNIV. (Feb. 25, 2014), http://news.iu.edu/releases/iu/2014/02/data-exposure-disclosure.shtml

281. Sample Notice Letter from Brad Wells, Vice President, Administration and Finance & Chief Financial Officer at California State University East Bay, to CA Residents, *available at* http://oag.ca.gov/system/files/California%20State%20University%20East%20Bay%20-%20Sample%20Notice%20Letter%20to%20CA%20Residents%20%285089625x7AB84%29_1.pdf?

282. UMD Data Breach, UNIV. OF MD., http://www.umd.edu/datasecurity/ (last visited Nov. 8, 2014).

283. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013).

284. *Id.* at 1142.

285. *Id.*

286. *Id.* at 1143.

287. *Id.* (*quoting* Whitmore v. Arkansas, 495 U.S. 149, 158 (1990)). In order to establish standing, an injury must be "concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling." Mon-

by the Act, the government would have had to go through a "highly attenuated chain of possibilities" that the court did not find convincing.[288]

The plaintiffs in the underlying litigation also tried to argue that they had standing because they undertook costly measures to avoid being affected by the Act.[289] The Court was unconvinced by the argument that the respondents suffered present costs and burdens as reasonable reaction to a threat of harm because the harm was not certainly impending.[290] The Court held that respondents could not "manufacture standing by incurring costs in anticipation of non-imminent harm."[291] *Clapper* does not carry over to state courts, but colleges and universities should assess the current law of standing in the state where litigation is brought to determine if an injury of the kind experienced in *Clapper* is enough to certify a class.

For colleges and universities facing class action suits stemming from a data breach, it will oftentimes be better to litigate rather than settle because of the plaintiffs' inability to show standing and establish jurisdiction. At the very least, these institutions should move to dismiss data breach class actions on lack-of-standing grounds. It is important for colleges and universities to provide credit-monitoring services immediately upon discovering a breach because that will make it even more difficult for plaintiffs to plead a concrete injury.[292]

The plaintiffs with the best chance of convincing the court to hear their case are those who have actually experienced identity theft and can prove that their injuries occurred directly as a result of the college or university's breach.[293] Therefore, class action plaintiffs seeking redress following a data breach will have to show more than the possibility of identity theft. Even if plaintiffs can show that they suffered identity theft, they have to jump another hurdle and prove that the information stolen directly resulted from the college or university data breach. Considering the wide variety of personal information people give away on a daily basis, it will be difficult for plaintiffs to pinpoint the exact entity that a hacker got their information from.

---

santo Co. v. Geertzon Seed Farms, 561 U.S. 139, 149 (2010).

288. *Clapper*, 133 S. Ct. at 1148.

289. *Id.* at 1150−51.

290. *Id.* at 1151.

291. *Id.* at 1155.

292. Alison Frankel, *Why (Most) Consumer Data Breach Class Actions vs Target are Doomed*, REUTERS (Jan. 13, 2014), http://blogs.reuters.com/alison-frankel/2014/01/13/why-most-consumer-data-breach-class-actions-vs-target-are-doomed/

293. *See id.* Frankel notes that victims of the Target data breach will likely only be able to prove standing if they have actually suffered identity theft as a result of the information stolen from Target, and the information used for the identity theft was actually taken from the Target hacking. *Id.*

VI. POTENTIAL FUTURE REGULATIONS

The Protecting Student Privacy Act of 2014 sponsored by Senator Ed Markey in the United States Senate could become the newest regulation affecting colleges and universities.[294] The proposal would amend FERPA to require institutions to implement information security policies and procedures, and threatens to take away funds if institutions do not comply.[295] The amendment notes that funds will not be available if an educational institution has not implemented information security policies to protect personally identifiable information and require third parties working alongside colleges and universities to have information security policies in place.[296] It focuses on outside parties and requires them to have stronger policies and procedures in place for dealing with student information.[297]

Moreover, Senator Bill Nelson introduced the Data Security and Breach Notification Act of 2015 in January 2015.[298] If enacted, it would preempt all state breach notification laws.[299] The bill has detailed procedures for notification and timeliness, as well as disclosure to the FTC and the Department of Homeland Security.[300] It was referred to the Committee on Commerce, Science and Transportation in January 2015.

Additionally, in 2014, the non-profit Electronic Privacy Information Center released a Student Privacy Bill of Rights that would increase student control over personal information.[301] There are six major features of the Bill of Rights: (1) access to and amendment of student records, (2) focused collection of data, (3) respect for context, (4) security, (5) transparency, and (6) accountability.[302] The focus is on the right to access records, to reasonably limit the amount of data collected and retained, to know what their data is being used for, and to hold institutions and third parties accountable for the way they handle data.[303]

Finally, one article has suggested that colleges and universities need to begin to regulate student social networking in order to reduce the risk of

---

294. Protecting Student Privacy Act of 2014, S. 2690, 113th Cong. (2014).

295. *Id.*

296. *Id.* at (4)(A).

297. *Id.* at (6)(C) (requiring educational institutions to require outside parties to "to have policies or procedures in place regarding information security practices regarding the education records. . .").

298. Data Security and Breach Notification Act of 2015, S. 177, 114th Cong. (2015).

299. *Id.*

300. *Id.*

301. Valerie Strauss, *Why a 'Student Privacy Bill of Rights' is Desperately Needed*, WASH. POST, Mar. 6, 2014, http://www.washingtonpost.com/blogs/answer-sheet/wp/2014/03/06/why-a-student-privacy-bill-of-rights-is-desperately-needed/.

302. *Id.*

303. *Id.*

identity theft.[304] The authors of the article express concern about students' lack of awareness as to the risks of identity theft.[305] Identity theft can affect these students long after they graduate from a college or university, so colleges and universities need to prevent identity theft, as well as discuss remedial measures with victims of identity theft.[306] The primary issue with social networking sites is that they require use of students' real names.[307] The article finds that students should be educated about protecting their own personal data and suggests that this should be mandatory for compliance with regulation.[308]

VII. CONCLUSION

Colleges and universities have seen a dramatic increase in the amount of data security breaches on campuses. These institutions are very susceptible to cyber attacks due to the large amounts of data they store, particularly if they have a medical center on campus. Additionally, they are subject to a multitude of state and federal regulations dealing with everything from data monitoring, protection, and destruction, to breach notification. It is important for these institutions to be aware of the regulations they are controlled by, and how they must shape their practices in accordance with these regulations. It is also necessary that colleges and universities have information security policies in place, and breach response plans to ensure that they will decrease their potential liability in the event of a breach.

304. Jamison Barr & Emmy Lugus, *Digital Threats on Campus: Examining the Duty of Colleges to Protect Their Social Networking Students*, 33 W. NEW ENG. L. REV. 757, 763 (2011), *available at* http://digitalcommons.law.wne.edu/cgi/viewcontent.cgi?article=1673&context=lawreview.

305. *Id.* at 786 (noting that identity thieves can "deduce social security numbers from online data that may be considered innocuous, such as birthdates and hometowns.").

306. *Id.* at 786.

307. *Id.* at 764.

308. *Id.* at 773.