Richmond Public Interest Law Review

Volume 14 | Issue 3 Article 4

1-1-2011

Protecting the Ivory Tower: Sensible Security or Invasion of Privacy

Stephen D. Lichtenstein

PROTECTING THE IVORY TOWER: SENSIBLE SECURITY OR INVASION OF PRIVACY?

Stephen D. Lichtenstein[*]

> *Our beginning point is a recognition that the modern American college is not an insurer of the safety of its students. Whatever may have been its responsibility in an earlier era, the authoritarian role of today's college administrations has been notably diluted in recent decades. Trustees, administrators, and faculties have been required to yield to the expanding rights and privileges of their students. By constitutional amendment, written and unwritten law, and through the evolution of new customs, rights formerly possessed by college administrations have been transferred to students. College students today are no longer minors; they are now regarded as adults in almost every phase of community life.*[1]

I. INTRODUCTION

Notwithstanding the sentiment expressed in the opening quotation, universities[2] should owe a duty to exercise a degree of ordinary care to those with whom they have created a special relationship, including students, faculty, administration, staff, and visitors to the campus. Generally, there is no duty recognized by tort law[3] obligating one party to protect another in the absence of a definite relationship between the parties that would justify on public policy grounds the obligation to protect an individual from the harm of others.[4]

Arguably, the source for this duty and the obligation of the university to protect its students is the educational contract between the student and the university.[5] The essence of the contract is that the student pays tuition and

[*] Professor of Law, Department of Law, Taxation and Financial Planning, Bentley University (Waltham, MA). The author wishes to thank Jonathan J. Darrow, Senior Research Consultant at Bentley University, for his assistance in preparing this manuscript.

1. Bradshaw v. Rawlings, 612 F.2d 135, 138–39 (3d Cir. 1979).
2. The term "universities" as used herein includes colleges and other institutions of higher education.
3. RESTATEMENT (SECOND) OF TORTS § 314 (1965).
4. *Id.*; *see also id.* § 315.
5. Havlik v. Johnson & Wales Univ., 509 F.3d 25, 35 (1st Cir. 2007) (citing Mangla v. Brown Univ., 135 F.3d 80, 83 (1st Cir. 1998) (noting that the student-university relationship is essentially contractual in nature and that the terms of the contract may be stated in handbooks and manuals); *see also* Rendell-

other expenses and the university, in return, provides an education. The university then creates, implements and discloses its policies and rules, as well as the procedures for enforcing those policies and rules, in the context of explaining the rights and responsibilities of the university and its students. These policies may also afford students privacy rights not otherwise available under federal or state laws. The policies are usually disclosed in the student handbook, which is posted on relevant university websites, and available in other forms of university communications.

Courts have granted private universities considerable latitude in drafting the language of their respective handbooks.[6] This latitude is premised on the unique nature of educational contracts that require the terms to be construed so as to allow the university to satisfy its educational obligations.[7]

It would seem that the handbook could serve as a primary source for the university to express its electronic surveillance and other campus monitoring policies. In order to ensure awareness, the university should publicize these policies to the university community and do so in a minimally invasive manner. For example, universities need not list every punishable act that could result in disciplinary action. Rather, the language should be specific enough to indicate that students are expected to respect the rights of others,[8] while fostering an atmosphere that can avoid or limit the types of campus tragedies that are described below.

Ideally, a balance should be struck between creating an atmosphere of safety and security, through the use of best practices or methods (including but not limited to campus surveillance and monitoring), and preserving student privacy and other protected rights. Whatever safety and security measures are taken by the university, there is no guarantee that acts of violence on campus will be prevented in the future. Moreover, such measures cannot end civil suits alleging negligence for failure to exercise ordinary care[9] in taking appropriate precautions, or those alleging unwarranted intrusions into student privacy rights resulting from university actions.

Baker v. Kohn, 457 U.S. 830, 840–41 (1982) (noting that a private school is not fundamentally different from many corporations whose business depends primarily on contracts).

6. Fellheimer v. Middlebury Coll., 869 F. Supp. 238, 242 (D. Vt. 1994).

7. *Id.* at 243.

8. *Id.* at 244–45.

9. RESTATEMENT (SECOND) OF TORTS § 283 (1965) (describing the standard as "that of a reasonable man under like circumstances").

II. INFAMOUS INCIDENTS OF CAMPUS VIOLENCE

It should be noted that the following description of campus tragedies will not focus on the psychological and mental profiles or pathologies of perpetrators and their possible motives. These dimensions have been well-documented and are best left to analysis by experts in the relevant field.[10]

Amy Bishop, a Harvard educated geneticist and assistant professor of biology at the University of Alabama at Huntsville, was denied tenure in early 2009. In appeal of the adverse tenure decision, she armed herself with a gun and appeared before a faculty meeting in February 2010, where she subsequently shot and killed three of her colleagues and wounded three others.[11]

Unfortunately, the incident at the University of Alabama is only one of many similar campus tragedies involving violence and murder. A few of the more infamous of these tragedies are described here. One early example involved Charles Whitman, a twenty-five year old engineering student at the University of Texas in Austin. On August 1, 1966, he armed himself and climbed to the University's observation tower, where he randomly shot and killed thirteen people, wounded thirty-one, and then committed suicide.[12] He had killed his wife and mother only a few hours earlier.[13] On November 1, 1991, Gang Lu, a twenty-eight year old former Ph.D. student in physics at the University of Iowa, entered two campus buildings shooting and killing four faculty members and one student, and wounding another.[14] He was unhappy that his dissertation did not win a prestigious prize.[15]

10. *See* JAMES ALAN FOX ET AL., THE WILL TO KILL: MAKING SENSE OF SENSELESS MURDERS (Allyn & Bacon, 3d ed. 2007); *see also* Jeffrey Kluger, *Inside a Mass Murderer's Mind*, TIME, Apr. 19, 2007, *available at* http://www.time.com/time/nation/article/0.8599.1612368.00.html; Thomas Frank, *Campus Killers' Hints Ignored*, USA TODAY, June 12, 2007, *available at* http://www.usatoday.com/news/nation/2007-06-12-campus-killers_N.htm.

11. Sheila Dewan & Liz Robbins, *A Previous Death at the Hands of Alabama Suspect*, N.Y. TIMES, Feb. 13, 2010, at A20.

12. *See The Madman in the Tower*, TIME, Aug. 12, 1966, *available at* http://www.time.com/time/magazine/article/0,9171,842584,00.html.

13. *Id.*

14. Michael Marriott, *Iowa Gunman Was Torn by Academic Challenges*, N.Y. TIMES, Nov. 4, 1991, at A12.

15. The D.C. Spriestersbach Dissertation Prize, which was awarded each year by the University of Iowa Graduate College to recognize outstanding doctorate-level research. *See* Univ. of Iowa – D.C. Spriestersbach Dissertation Prize, http://www.grad.uiowa.edu/awards/the-dc-spriestersbach-dissertation-prize.

The deadliest campus shooting in modern history[16] occurred April 16, 2007 when Sueng-Hui Cho, a twenty-three year old student at the Virginia Polytechnic Institute and State University (Virginia Tech), shot and killed thirty-two people and wounded another twenty-five before committing suicide.[17] The evidence as to his motive indicate that Cho was patently shy, anti-social, and frequently engaged in aberrant behavior, including the stalking of fellow classmates.[18]

Two additional incidents bear mentioning. The first, and perhaps the most infamous, involved the Columbine High School killing spree in 1999.[19] On April 20, 1999 Eric Harris and Dylan Klebold, two seniors at Columbine High School in Columbine, Colorado, entered the campus armed with an arsenal of weapons. They killed twelve students and one teacher, wounded an additional twenty-three individuals, and then committed suicide. It appears they were influenced by neo-Nazi literature and sought revenge for being socially excluded by other Columbine students.[20]

The second event occurred on April 5, 1986 and involved Jeanne Clery, a twenty-nine year old freshman at Lehigh University who was beaten, raped and murdered while sleeping in her dormitory by another Lehigh student

16. Alessandra Stanley, *Deadly Rampage and no Lose for Words*, N.Y. TIMES, April 17, 2007, at A19.

17. Ian Urbina, *Report on Virginia Tech Shooting Finds Notification Delays*, N.Y. TIMES, Dec. 5, 2009, at A1.

18. *See* VA. TECH REV. PANEL, MASS SHOOTINGS AT VIRGINIA TECH 53 (2007), *available at* http://www.vtreviewpanel.org/report/report/11_CHAPTER_IV.pdf. The report raised questions about Cho's mental stability, which had resulted in a hearing to determine if he should be committed for treatment. *Id.* at 47. Efforts to inform his parents and others at Virginia Tech were impeded by Cho's privacy rights under federal law. *Id.* at 38; *see* Family Educational Rights and Privacy Act (FERPA) of 1974, 20 U.S.C. § 1232g(b) (2006); *see also* Family Educational Rights and Privacy, 34 C.F.R. § 99.5 (2010). If Cho's mental status posed a physical threat to others, concerns for Cho's privacy rights and the confidentiality of his mental condition would be considered in light of *Tarasoff v. Regents of Univ. of Cal.*, 551 P.2d 334 (Cal. 1976), and the holding of the Virginia Supreme Court in *Nasser v. Parker*, 455 S.E.2d 502 (Va. 1995). In *Tarasoff*, the court ruled that where a mentally disturbed patient was in a doctor-patient or hospital-patient relationship, and the patient indicates the intent to harm another, the doctor or hospital is required to warn the intended victim. *Tarasoff*, 551 P.2d at 340. Many states have adopted a similar rule. *See* Charles Patrick Ewing, *Tarasoff Reconsidered*, 36 AM. PSYCHOL. ASSOC. 112 (2005). However, in *Nasser*, the Virginia Supreme Court disagreed with *Tarasoff*, in finding that the duty to warn depends on whether the doctor or hospital has actually taken charge of a mentally disturbed patient rather than whether a doctor or hospital-patient relationship exists at all. 455 S.E.2d at 505. In Cho's case, he had been diagnosed as depressed and a danger to himself. *See* Mike Gangloff & Laurence Hammack, *No Teeth in Virginia Mental Health Laws*, ROANOKE TIMES, May 8, 2007, *available at* http://www.roanoke.com/vtreactions/wb/116052. Accordingly, he was ordered by Virginia Tech health care providers to seek outpatient treatment. *Id.* Unfortunately for the victims of his atrocity, Cho was released but never sought the recommended treatment. *Id.*

19. *See* Michael Janofsky, *Year Later, Columbine Is Learning to Cope While Still Searching for Answers*, N.Y. TIMES, Apr. 17, 2000, at A12; *see also* DAVID CULLEN, COLUMBINE 85–86 (2009).

20. Janofsky, *supra* note 19, at A12.

unknown to her.[21] Following the death of their daughter, her parents, Connie and Howard Clery, discovered that there had been numerous violent crimes committed on the Lehigh campus in the three years prior to their daughter's murder.[22] In the wake of Clery's brutal rape and murder, and concerned with campus security in general, Congress held a number of hearings culminating in the passage of the Student Right-to-Know and Campus Security Act of 1990.[23] In 1998, this Act was renamed the Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act of 1990,[24] to be further discussed below.[25]

It should be emphasized that the above tragic incidents describe the most serious acts of campus violence—those resulting in murder. Federal Bureau of Investigation (FBI) statistics reflect an expanded scope of campus violence by including in their data crimes involving force or the threat of force[26] and non-negligent manslaughter, along with murder, forcible rape, robbery and aggravated assault.[27] Of course, analogous to the general community, numerous other types of crimes are committed on campuses, including but not limited to burglary, motor vehicle theft, stalking, vandalism, and arson.[28] These crimes are serious attacks on person and property, but none is more egregious than the alarming number of sexual assaults and attacks on women like Jeanne Clery that studies reveal pervade university campuses.

Just how pervasive is the problem of sexual assault?[29] The U.S. Department of Justice indicates that one out of every five female university students will be the victim of a sexual assault at one point in a typical five-

21. Mark Fritz, *The Politics of Parental Grieving*, L.A. TIMES, June 6, 1999, at A1.

22. S. Daniel Carter, *Covering Crime on College Campuses*, 88 QUILL 32 (2000).

23. Student Right-To-Know and Campus Security Act, Pub L. No. 101-542, § 204, 140 Stat. 2381, 2385–87 (1990) (codified as amended at 20 U.S.C. § 1092(f) (2006)) (requiring institutions of higher education to collect and make public campus crime statistics, including sex offenses).

24. 20 U.S.C. § 1092(f)(15) (2006).

25. *See infra* Part III.

26. FED. BUREAU OF INVESTIGATION, U.S. DEP'T OF JUSTICE, CRIME IN THE UNITED STATES, 2008-VIOLENT CRIME

(2009), *available at* http://www2.fbi.gov/ucr/cius2008/offenses/violent_crime/index.html [hereinafter VIOLENT CRIME REPORT].

27. *Id.* (follow "Universities and Colleges" hyperlink under "Browse By"; then follow "table 9" hyperlink; then follow "Data Declaration" hyperlink for a general comment regarding nature and extent of FBI data).

28. *See* DIANNA A. DRYSDALE ET AL., U.S. SECRET SERV., CAMPUS ATTACKS: TARGETED VIOLENCE AFFECTING INSTITUTIONS OF HIGHER EDUCATION 6–7 (2010),

http://www2.ed.gov/admins/lead/safety/campus-attacks.pdf.

29. *See* Elizabeth Redden, *Making Women Safer on Campus*, INSIDE HIGHER ED., Sept. 7, 2007, www.insidehighered.com/news/2007/09/07/kentucky.

year matriculation.[30] Equally alarming, approximately 80 to 90 percent of victims will know their assailant.[31] The aftermath of these assaults result in a number of physical and traumatic consequences.[32] The onus to prevent, protect, and educate against these heinous attacks resides primarily with the university. Once again, whatever efforts are employed, universities must be mindful of the balance between the need to create an atmosphere of safety and security while protecting legitimate privacy rights. It should also be mentioned that acts of violence against female students (and others on campuses) include forms of sexual harassment. A 2006 survey conducted by the American Association of University Women Education Foundation (AAUW) found that, in May 2000, nearly two-thirds of female students experienced acts of sexual harassment,[33] one third of which involved physical contact.[34] Universities receiving federal funds are required to implement the provisions of Title IX of the Education Amendments of 1972.[35] The major requirements are to create an effective sexual harassment policy that informs the campus community how and where to file a complaint, as well as the procedure the university will follow to investigate and take appropriate corrective action concerning the allegations. In cases of sexual harassment against a student, whether by another student, faculty member or university employee, the university may be held liable for monetary damages.[36]

30. U.S. DEP'T OF JUSTICE, SEXUAL ASSAULT ON CAMPUS: WHAT COLLEGES AND UNIVERSITIES ARE DOING ABOUT IT 2 (2005), http://www.ncjrs.gov/pdffiles1/nij/205521.pdf; *see also* CTR. FOR PUB. INTEGRITY, SEXUAL ASSAULT ON CAMPUS: A FRUSTRATING SEARCH FOR JUSTICE, (2010), *available at* http://www.publicintegrity.org/investigations/campus_assault/.

31. *Id.*

32. *See* CHRISTOPHER P. KREBS ET AL., U.S. DEP'T OF JUSTICE, THE CAMPUS SEXUAL ASSAULT STUDY, at viii (2007), *available at* http://www.ncjrs.gov/pdffiles1/nij/grants/221153.pdf (reporting that 25-45 percent of rape victims will suffer from non-genital trauma, 19-22 percent will suffer from genital trauma, up to 40 percent will be infected with sexually transmitted diseases, and 1-5 percent will get pregnant).

33. *See* CATHERINE HILL & ELENA SILVA, AM. ASSOC. OF UNIV. WOMEN EDUC. FOUND., DRAWING THE LINE: SEXUAL HARASSMENT ON CAMPUS 2 (2005), *available at* http://www.aauw.org/learn/research/upload/DTLFinal.pdf; *see also id.* at 15 fig.15.

34. *Id.* at 17.

35. 20 U.S.C. § 1681 (2006).

36. *See* Gebser v. Lago Vista Indep. Sch. Dist., 524 U.S. 274, 285 (1998); Davis v. Monroe Cnty. Bd. of Educ., 526 U.S. 629, 633 (1999). The Court in each of these cases limited the liability standards of private actions. *See, e.g.*, *Gebser* at 283; *Davis*, 526 U.S. at 693. For the process to be followed for administrative enforcement of Title IX violations, as contrasted with private actions, see U.S. DEP'T OF EDUC., REVISED SEXUAL HARASSMENT GUIDANCE: HARASSMENT OF STUDENTS BY SCHOOL EMPLOYEES, OTHER STUDENTS, AND THIRD PARTIES, at iii-iv (2001), *available at* http://www2.ed.gov/offices/OCR/archives/shguide/index.html (providing that the process of administrative enforcement require enforcement agencies such as the Office for Civil Rights to inform schools of Title IX violations and to seek voluntary corrective actions before seeking termination of federal funds or other enforcement procedures including referral of complaints for judicial action to the

A. Safe but Not Safe Enough: The Need for Increased Campus Security

Although university campuses may be safe in comparison to urban communities, both evidence and anecdote suggest that the risk to the university community remains unacceptably high. The FBI lists the number and types of campus violent acts known to law enforcement for all public and private universities and colleges in every state.[37] In 2008, the University of Alabama at Huntsville reported one violent act; the University of Texas at Austin, eleven; the University of Iowa, fourteen; Virginia Tech, three; and Lehigh University, five.[38] Of course, the total number for all campuses within the state are significant. For example, for the various University of Texas campuses, the total was 212,[39] while for all Virginia's campuses, it was 113.[40] These statistics coupled with the examples of the campus tragedies described above strongly suggest the need for universities to be proactive in their efforts to protect the campus, while respecting the legal rights of those who are the subject to those efforts.

There are two major means used by universities to protect campus security. In the wake of Columbine, many universities have installed campus video cameras[41] as a means to deter criminal activities and ensure safety and security. A second means is to monitor electronic communications, such as e-mail.

Universities that have their own campus police departments have a responsibility to install and monitor cameras[42] in appropriate public areas without violating privacy rights. These locations include public buildings, such as classrooms, libraries, dining rooms and other common areas. By

U.S. Department of Justice, Civil Rights Division).

37. VIOLENT CRIME REPORT, *supra* note 26 (follow "Universities and Colleges" hyperlink under "Browse By"; then follow "Table 9" hyperlink).

38. *Id.*

39. *Id.*

40. *Id.*

41. *See* Privacy Rights Clearing House, Fact Sheet 29 para. 8 (Nov. 2005), http://www.privacyrights.org/fs/fs29-education.htm#8.

42. *See, e.g.*, SUNY COLL. ONEONTA, ELECTRONIC SURVEILLANCE POLICY 1, *available at* http://www.oneonta.edu/security/documents/SurveillanceVideoPolicy.pdf (last visited Mar. 13, 2011).

> The College at Oneonta reserves the right to place cameras on campus where necessary and appropriate. This policy applies to all personnel, departments, offices, and other subdivisions of the College in the use of electronic recording and surveillance.
> [. . .]
> The College at Oneonta respects the privacy of university community members and is sensitive to balancing that privacy with safety needs on campus.

Id.

contrast, dorm rooms, restrooms, and other private areas where an individual has a "reasonable expectation of privacy"[43] are generally off-limits to surveillance. Exceptions may be made if the purpose of the intrusion relates to a specific threat of imminent and serious crime or to an emergency situation.

In the case of dorm rooms, the university may include in the student housing agreement a provision specifying the reasonable conditions under which an inspection of the room by university officials may occur. For example, Boston College reserves the right for campus officials to enter resident student rooms and conduct a plain view search for reasons of health, maintenance, community standards (including safety and discipline), or inspections.[44] Regular inspections are conducted by staff in all areas.[45] Further, except in cases of an emergency when university officials cannot search the contents of a student's dorm without their consent, a duly authorized search warrant from a local court or issued by the Vice President for Student Affairs may be used.[46] It follows that students would enjoy a reasonable expectation of privacy in their dorm room analogous to what is expected in an apartment or hotel and what can be characterized as the student's "home away from home."[47] However, the ever-present threat of

43. Katz v. United States, 389 U.S. 347, 360 (1969) (Harlan, J., concurring). Katz was convicted of transmitting wagering information across state lines using a telephone in a private phone booth that had been bugged by the FBI with an electronic device placed outside the booth. *Id.* at 348 (majority opinion). The Court held that his Fourth Amendment protection from unreasonable searches and seizures had been violated. *Id.* at 360. In a concurring opinion, Justice Harlan introduced the idea that individuals are entitled to a reasonable expectation of privacy in certain circumstances. *Id.* (Harlan, J., concurring). Justice Harlan opined that there is a twofold requirement for this expectation to apply. *Id.* at 361. First, a person must exhibit an actual (subjective) expectation of privacy and second, that the expectation must be one that society is prepared to recognize as "reasonable." *Id.* While generally a person's home generally is a place where one expects privacy, "objects, activities, or statements that he exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited." *Id.*

44. BOSTON COLL., CONDITIONS FOR RESIDENCY 2007-2008: RIGHT OF ENTRY, *available at* http://www.bc.edu/offices/reslife/lifeinhalls/communityexp/conditions0708.html#RIGHTOFENTRY (last visited Mar. 13, 2011).

45. *Id.*

46. *Id.*

47. Commonwealth v. McCloskey, 272 A.2d 271, 273 (Pa. Super. Ct. 1970); *see also* Piazzola v. Watkins, 442 F.2d 284, 289 (5th Cir. 1971); Morale v. Grigel, 422 F. Supp. 988, 997 (D.N.H. 1976).

recurring acts of campus violence, coupled with the events of September 11, 2001, have reduced the nature and extent of this expectation;[48] though they have certainly not eliminated it.

One critical question with respect to video surveillance is to what degree has the installation of campus cameras reduced the nature, extent, and threat of campus violence? Some pundits assert that there is no conclusive evidence that cameras are a panacea for reducing the incidence of campus violence. For instance, Jim Harper, Director of Information Policy Studies at the Cato Institute,[49] states that security cameras "may be good forensic tools—after something happens, they'll tell you what happened, and in the rare case where a terrorism case fails, they can be useful to help track down the perpetrators. But they do not provide protection against attacks, and that's a key distinction."[50] Others ponder whether the sense of security created by cameras creates an atmosphere of suspicion for some and mistrust for others. In order to foster positive attitudes toward safety measures, universities that use camera surveillance should create and disseminate their privacy and security policies and, at a minimum, describe the rights and responsibilities of students, faculty and other personnel, as well as notify them of the purposes for which the video files can be used, who will have access to the files, how long and where they will be kept and, in the case of faculty or staff, whether the information contained in the files will be used for performance evaluations.[51] The privacy provision within the policy should indicate that the cameras will be used to monitor only suspicious and unlawful activities.

Technological advancements will create new tools for campus video surveillance. One such tool was recently developed by Blackboard, Inc., a company that provides course and classroom management software

48. *See* Robert C. Power, *Changing Expectations of Privacy and the Fourth Amendment*, 16 WIDENER L. J. 43 (2006); *see also* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified as amended in scattered sections of 18 U.S.C., 50 U.S.C., 22 U.S.C., 31 U.S.C., and 47 U.S.C.). The Act contains ten titles and expands the ability of law enforcement agencies to conduct searches of wireless communication and financial or medical records of those suspected of planning or having committed acts of terrorism. *Id.* The Act further enhances the sharing of information among law enforcement agencies. *Id.*

49. Edward H. Crane founded the Cato Institute in Washington, D.C. in 1977 as a non-profit public policy research foundation. For additional information on the Cato Institute, see About Cato, http://www.cato.org/about.php (last visited Mar. 13, 2011).

50. Marcus Barum, *Eye on the City, Do Cameras Reduce Crime?*, ABC NEWS, July 9, 2007, http://abcnews.go.com/US/story?id=3360287&page=1.

51. *Id.* For an example of a more complete surveillance privacy and security policy, see CORNELL UNIV., POLICY 8.1: RESPONSIBLE USE OF VIDEO SURVEILLANCE SYSTEMS (2009), http://www.dfa.cornell.edu/dfa/cms/treasurer/policyoffice/policies/volumes/riskandsafety/upload/vol8_1.pdf.

programs.[52] Blackboard's new service allows campus security officials to view live and recorded video of individuals at the entrance points to certain buildings (dormitories, dining rooms, libraries, athletic facilities, parking lots, and other designated areas) by using entrance activation cards supplied by Blackboard. The service can be added to a university's existing Blackboard software system and also provides an additional means by which to alert the campus of imminent dangers or threats. If a university decides to add this software to its cache of video surveillance tools, notice should be included in its security and privacy policy. This service should only be used for security and protection of the campus and not as a means by which to intrude upon privacy rights.

The second popular method employed by universities to help ensure safety is the monitoring of university-owned computers and other electronic equipment in order to access e-mail, text messages, and other forms of electronic communications.

Every second of every day, huge volumes of instant messages and information are transmitted via e-mail[53] and short message services (SMS) using such devices as mobile phones. One recent survey indicates that the number of text messages sent on a daily basis now exceeds calls made and received by phone.[54] University students engage in these methods of communication in the form of text messages, tweets, chat rooms, web logs ("blogs"), wikis, message boards, and social networks.[55]

52. Posting of Josh Fischman to Chron. of Higher Educ. Blog, http://chronicle.com/blogs/wiredcampus/blackboard-gets-into-video-surveillance/3747 (Mar. 10, 2008, 11:15 EST).

53. The Radicati Group, an independent technology market research firm, estimated 247 billion e-mail messages would be sent worldwide in 2009 and that the number would grow to 507 billion by 2013. Press Release, Radicati Group, E-mail Statistics Report, 2009-2013 (May 6, 2009), *available at* http://www.radicati.com/?p=3237.

54. For the second quarter of 2008, Americans placed and received only 204 calls per month compared to an impressive 357 text messages. *See In U.S., Text Messaging Tops Mobile Phone Calling*, NIELSENWIRE, Sept. 22, 2008, http://blog.nielsen.com/nielsenwire/online_mobile/in-us-text-messaging-tops-mobile-phone-calling/.

In addition, during the first half of 2009, over 822 billion text messages were sent (nearly 5 billion per day); *see also* Press Release, Cellular Telecomm. & Internet Ass'n, The Wireless Association Announces Semi-Annual Wireless Industry Survey Results (Mar. 23, 2010), *available at* http://www.ctia.org/media/press/body.cfm/prid/1936.

55. See generally popular Web sites for doing so, including Facebook.com, YouTube.com, Twitter.com, and Linkedin.com.

How effective a tool is monitoring for providing increased protection and safety? According to a 2009 survey,[56] 46 percent of adult Americans believe that universities do not sufficiently monitor student behavior; 30 percent believe they do, while 45 percent remain undecided.[57] Forty-three percent also believe universities provide sufficient safety measures, thirty-one believe otherwise, while 26 percent are undecided.[58] Statistics such as these suggest broad popular support for an increased role of universities in the protection and safety for the more than 17.8 million undergraduate students.[59]

The rights and obligations associated with the use of university-owned or issued computers and related electronic equipment, including the right of universities to monitor and access the content of electronic communication, are generally governed by a university's terms of use policy. The terms and provisions of a usage policy should clearly indicate what constitutes acceptable use and the circumstances which precipitate a university's right to monitor and access online activities of its students and others within the campus community.[60] Many such policies allow a university to examine a

56. *Forty-Six Percent Say Colleges Don't Monitor Student Behavior Enough*, RASMUSSEN REPORTS, Aug. 18, 2009, http://www.rasmussenreports.com/public_content/lifestyle/general_lifestyle/august_2009/46_say_colleges_don_t_monitor_student_behavior_enough.

57. *Id.*

58. *Id.*

59. DRYSDALE, *supra* note 28, at 5.

60. *See, e.g.*, BENTLEY UNIV., POLICIES GOVERNING TECHNOLOGY RESOURCES AT BENTLEY, http://www.bentley.edu/computing-use/index.cfm (last visited Mar. 13, 2011).

> Bentley reserves the right to examine the contents of personal computers used by faculty, staff and students or other computers attached to our network, without prior consent or knowledge of the individual being investigated. Bentley also reserves the right to confiscate computers used by faculty, staff and students. Cooperation may include, but is not limited to, providing transaction logs, copies of electronic of electronic mail messages, data files, usage records, hardware, account and password information, or other information as required by those authorities. Those who are financially responsible for the perpetrators, such as parents or guardians, may also be held accountable.

Id.; *see also* BENTLEY UNIV., ELECTRONIC MAIL POLICY, http://info-privacy.bentley.edu/policy/electronic-mail-policy.

> Employees and students should be aware that e-mail sent and received using the university's computer resources is neither confidential nor private. . . . The university itself may, upon reasonable grounds, access your e-mail files at any time, without prior notice to the student or employee, but with approval from two vice presidents.
>
> As a general rule, the university will not read or make available the contents of any individual's electronic mail unless there are reasonable grounds to do so. Reasonable grounds for doing so may include but are not limited to: ensuring system integrity (such as tracking viruses or corrupt messages), complying with legal obligations (such as

computer's contents without the prior consent or knowledge of the user.[61] If online activities reveal potential illegal activities involving campus or outside law enforcement, then sufficient probable cause is established for the issuance of a warrant. Otherwise, both the warrant and seizure can be challenged.

For example, in *United States v. Angevine*,[62] the University of Oklahoma's computer terms of use policy provisions prohibited the use of its computers to access obscene material and allowed the University to randomly inspect the files downloaded on computers issued to faculty and others employed by the University.[63] The policy also cautioned that information transmitted on its network either in transit or in storage was not confidential and that any data stored on its computer hardware was property of the University.[64] Angevine was a professor at the University, and with the cooperation of his wife, the Stillwater Police Department was able to obtain a search warrant to search and seize his computer, which ultimately revealed over 3,000 pornographic images of young boys.[65] After Angevine's arrest, he moved to suppress the evidence seized by the police, alleging a violation of his Fourth Amendment rights and claiming a reasonable expectation of privacy in the contents of his computer.[66] The District Court denied the motion, whereupon Angevine conditionally pled guilty to possession of child pornography, retaining his right to further appeal the denial of the motion.[67] Ultimately, the trial court convicted him of possession of child pornography in violation of 18 U.S.C. § 2252(A)(a)(5)(B).[68] On appeal, the Tenth Circuit affirmed the denial of the motion to suppress and found that under the provisions of the computer terms of use policy, Angevine had no reasonable expectation of privacy.[69] Accordingly, the police did not violate his rights under the Fourth Amendment.[70]

> subpoenas) . . . investigating complaints of possible violation of university policy . . . resolving disputes or grievances between individuals at the university . . . conducting judicial review cases . . . [or] continuing business after a person is terminated from their position or leaves Bentley.

Id.

61. *Id.*
62. 281 F.3d 1130, 1132 (10th Cir. 2002).
63. *Id.*
64. *Id.*
65. *Id.* at 1132.
66. *Id.*
67. *Id.*
68. *Id.*
69. *Id.*
70. *Id.*

B. To Search and Seize or Not to Search and Seize, That Is *Calixte*

The amount of credible evidence necessary to satisfy the probable cause requirements for a warrant to search a student's dorm room and to seize his computer and other electronic equipment was addressed in the case of *In re Search Warrant Executed on March 30, 2009 at the Residence of Riccardo Calixte*.[71] *Calixte* also raised privacy issues in light of the relevant laws governing privacy rights related to campus surveillance and monitoring.[72]

Riccardo Calixte, a Boston College student majoring in computer science and an employee in Boston College's Information Technology Department, was having social problems with his ex-roommate Jesse Bennefield.[73] As a result, Bennefield made several serious allegations against Calixte to Kevin Christopher, a detective with the Boston College Campus Police.[74] The most serious of the allegations accused Calixte of having a reputation as a hacker, illegally hacking[75] into Boston College's grading system and changing student grades, illegally downloading movies and music,[76] and using the Boston College computer system to send a mass e-mail in which he stated that Bennefield was gay and participated in a gay dating website.[77] Boston College, however, found no evidence that Calixte changed grades; nor did it find any other evidence to support Bennefield's allegations, except that one of Calixte's e-mail messages sent from his laptop falsely indicated that Bennefield was gay.[78]

Based on this evidence, Christopher and Boston College believed there was sufficient probable cause that Calixte had used technology in violation of Boston College's terms of use policy and Massachusetts laws by

71. *In re* Riccardo Calixte, No. SJ-2009-0212, at 1 (Mass. Dist. Ct. May 21, 2009) (order granting motion to quash search warrant and denying motion to suppress evidence), *available at* http://www.eff.org/files/filenode/inresearchBC/SJCcalixteorder.pdf [hereinafter *In re* Riccardo Calixte].

72. *Id.*

73. *Id.* at 2.

74. *Id.*

75. For a discussion of a hacking incident involving the theft of the personal data of over 160,000 university students contained on the university's server, see Michelle Meyers, *U.C. Berkeley Computers Hacked, 160,000 at Risk*, CNET NEWS (May 8, 2009), http://news.cnet.com/8301-1009_3-10236793-83.html.

76. *In re* Riccardo Calixte, No. SJ-2009-0212, at 1. Universities should include provisions in their computer terms of use policies addressing and prohibiting illegal downloading and file sharing of music, DVDs and other digitally stored information. *See* Jonathan Saltzman, *Student Must Pay $675K for Songs*, BOSTON GLOBE , Aug. 1, 2009, at Metro 1. The $675,000 damage award was subsequently reduced to $67,500. *See* Jonathan Saltzman, *Judge Slashes Downloading Penalty*, BOSTON GLOBE, July 10, 2010, at Metro 1.

77. *In re* Riccardo Calixte, No. SJ-2009-0212, at 3.

78. *Id.*

engaging in fraudulent and unauthorized use of Boston College's computer services,[79] as well as unauthorized access of its computer systems.[80] One of the relevant provisions of Boston College's terms of use for its technology and information resources[81] stated that Boston College would not monitor, access or disclose the contents of a user's electronic data, software and communication files, unless it obtained the proper approval and an urgent and legitimate need existed sufficient to offset Boston College's commitment to protecting the user's privacy.[82] The policy also provided for disciplinary action including criminal prosecution under both state and federal law.[83]

Detective Christopher obtained a search warrant from the Newton District Court.[84] Pursuant to the search warrant, the Campus Police searched Calixte's dorm room and seized his personal laptop, two other laptops

79. MASS. GEN. LAWS ch. 266, § 33A (2010).

> Fraudulent Obtaining of Commercial Computer Services; Penalties: Whoever, with intent to defraud, obtains, or attempts to obtain, or aids or abets another in obtaining, any commercial computer service by false representation, false statement, unauthorized charging to the account of another, by installing or tampering with any facilities or equipment or by any other means, shall be punished by imprisonment in the house of correction for not more than two and one-half years or by a fine of not more than three thousand dollars, or both. As used in this section, the words 'commercial computer service' shall mean the use of computers, computer systems, computer programs or computer networks, or the access to or copying of the data, where such use, access or copying is offered by the proprietor or operator of the computer, system, program, network or data to others on a subscription or other basis for monetary consideration.

Id.

80. MASS. GEN. LAWS ch. 266, § 120F (2010).

> Unauthorized Access to Computer System; Penalties: Whoever, without authorization, knowingly accesses a computer system by any means, or after gaining access to a computer system by any means knows that such access is not authorized and fails to terminate such access, shall be punished by imprisonment in the house of correction for not more than thirty days or by a fine of not more than one thousand dollars, or both. The requirement of a password or other authentication to gain access shall constitute notice that access is limited to authorized users.

Id. "[E]ach unauthorized 'login' to a computer system constitutes a separate offense, and…the number of documents accessed during any given 'login' is not relevant in determining the number of convictions." Commonwealth v. Piersall, 853 N.E.2d 210, 212 (Mass. App. Ct. 2006).

81. *See* BOSTON COLL, PROFESSIONAL STANDARDS AND BUSINESS CONDUCT: USE OF UNIVERSITY TECHNOLOGICAL AND INFORMATION RESOURCES (1995), *available at* http://www.bc.edu/offices/policies/meta-elements/pdf/policies/I/1-100-025.pdf [hereinafter PROFESSIONAL STANDARDS AND BUSINESS CONDUCT].

82. *Id.* The privacy provision of the policy also allows Boston College to monitor, access and disclose contents in order to: maintain system integrity (*e.g.*, track viruses); protect system security; protect University property rights; and meet legal obligations (*e.g.*, respond to a subpoena). *Id.*

83. *See id.* ("Reporting Suspected Violations").

84. *See* Kevin M. Christopher, Application and Affidavit in Support of Application for Search Warrant, No. 0912SW03 (Mar. 30, 2009), *available at* http://www.citmedialaw.org/sites/citmedialaw.org/files/2009-03-30-Application%20for%20Search%20Warrant.pdf.

either belonging to Boston College or other students, two iPods, two cell phones, a digital camera, hard drives, flash drives, compact disks, and other electronic equipment.[85] As a result, Calixte's attorneys along with the Electronic Frontier Foundation (EFF)[86] filed a motion with the Newton District Court to quash the search warrant and to recover his property.[87] The court decided that the allegations and resultant investigation provided sufficient probable cause for the warrant and the motion to quash was denied.[88]

On appeal to the Massachusetts Supreme Judicial Court, the Commonwealth of Massachusetts was ordered to cease any further forensic analysis of the property seized.[89] The court allowed the motion to quash the search warrant and the motion to return the property.[90] The court reasoned that the main focus of the affidavit for the search warrant was the e-mails, which was most likely illegal.[91] Based on the allegations related to the e-mail messages, the search warrant was obtained even though the affidavit failed to indicate the time or origin (e.g., whose computer was used to send) of the alleged illegal e-mail messages and where or when Bennefield witnessed their mailing.[92] The affidavit also failed to substantiate the allegations that Calixte hacked into Boston College's faculty database in order to change grades and to illegally download movies and music files.[93] Apparently, the campus police did not fully investigate the allegations, causing the court to characterize the evidence submitted in the affidavit for the warrant as "sketchy"[94] and "troublingly weak."[95] It further characterized the efforts of the police investigation as "lacking"[96] in that

85. *See In re* Riccardo Calixte, No. SJ-2009-0212, at 3 (Mass. Dist. Ct. May 21, 2009) (order granting motion to quash search warrant and denying motion to suppress evidence), *available at* http://www.eff.org/files/filenode/inresearchBC/SJCcalixteorder.pdf.

86. The EFF was founded in 1990 by Mitchell Kapor, of Lotus Corporation and ON Technology, and John Perry Barlow, a writer and lyricist. EFF's History, http://www.eff.org/about/history (last visited Mar. 14, 2011). EFF is a nonprofit organization whose stated purpose is to "defend[] your rights in the digital world." About EFF, http://www.eff.org/ (last visited Mar. 14, 2011).

87. Brief of Petitioner, *In re* Search Warrant Executed on March 30, 2009 at the Residence of Riccardo Calixte No. SJ-2009-0212 (Mass. Dist. Ct. Apr. 27, 2009) (No. 0912SW03), *available at* http://www.eff.org/files/filenode/inresearchBC/calixteappeal-042709.pdf [hereinafter Brief of Petitioner].

88. *Id.* at 5.

89. *In re* Riccardo Calixte, *supra* note 71, at 10.

90. *Id.* at 11.

91. *Id.* at 6.

92. *Id.* at 6–7.

93. *Id.* at 7.

94. *Id.* at 8.

95. *Id.* at 10.

96. *Id.* at 9.

they failed to establish Bennefield's reliability as a witness despite the fact that he was the named informant in the affidavit. As such, his reliability would be a factor in establishing probable cause for the search warrant to be issued.[97] Simply naming him in the affidavit as the informant was insufficient without more corroboration,[98] and since Calixte worked in Boston College's Information Technology Department, he would have access to computers belonging to third parties. Therefore, the police failed to link the computer used for the alleged illegal activities to Calixte. Finding no nexus between the evidence submitted in the affidavit and the validity of the search warrant, the court reasoned that sending the e-mails from a public e-mail service did not appear to satisfy the elements required to prove the crime of obtaining computer services by fraud or misrepresentation, or the crime of unauthorized access to a computer system.[99] As a result of the unlawful search of Calixte's room and seizure

97. *Id.*

98. *Id.* at 8–9. The court found that the statement in the affidavit indicating Bennefield had been a reliable witness in another investigation was insufficient to evaluate his reliability as a witness for this search warrant. *See* Commonwealth v. Rojas, 403 Mass. 483, 486 (1988).

99. *In re* Riccardo Calixte, *supra* note 71, at 6; *accord* United States v. Drew, 259 F.R.D. 449, 452 (C.D. Cal. 2009). Drew, a forty-seven year old female, created a fictitious social network account on MySpace using the pseudonym "Josh Evans" and, in violation of MySpace's terms of use, Drew posted a picture of a sixteen-year old male without his permission. *Id.* The account of "Josh Evans" was created in order to cyber-bully Megan Meier, who was a thirteen-year-old former friend of Drew's daughter. *Id.* For a number of days, Drew used the "Evans" account to persuade Meier that "Evans" liked her. *Id.* Soon after, "Evans" informed Meier that he was moving, that no longer liked her, and that "the world would be a better place without her in it." *Id.* Meier took the words literally and committed suicide. *Id.* Drew was indicted by a federal Grand Jury and convicted of a misdemeanor under the Computer Fraud and Abuse Act (CFAA) of 1984 (current version at 18 U.S.C. § 1030 (2006)) for using a computer in interstate commerce without authorization and in excess of authorized use. *Id.* at 453. Judge Wu overturned Drew's conviction, opining that

> Treating a violation of a website's terms of service, without more, to be sufficient to constitute "intentionally access[ing] a computer without authorization or exceed[ing] authorized access" would result in transforming [the CFAA] into an overwhelmingly overbroad enactment that would convert a multitude of otherwise innocent Internet users into misdemeanant criminals.

Id. at 466 (citation omitted). In the aftermath of Megan Meier's suicide and the facts surrounding it, the Missouri Legislature expanded its existing laws prohibiting harassment to include bullying via the Internet by means of a computers and other electronic equipment. *See Missouri Lawmakers Pass Bill Against Cyber-harassment After MySpace Suicide Case*, L.A. TIMES, May 17, 2008, *available at* http://articles.latimes.com/2008/may/17/nation/na-suicide17. As of October 2009, twenty other states have enacted similar legislation. *See* Nat'l Coal. Against Censorship, Cyberbullying: Statutes and Policies (Sept. 21, 2009), http://www.ncac.org/List-of-Cyberbullying-Statutes-and-Policies. (listing state statutes that mandate school board to adopt cyberbullying policies). Additionally, in April 2009, U.S. Representative Linda Sanchez (D-CA) introduced the Megan Meier Cyberbullying Prevention Act, H.R. 1966, 111th Cong. (2009). Section 3 of the bill would criminalize cyberbullying. The pertinent part of the proposed bill provides: "Whoever transmits in interstate or foreign commerce any communication, with the intent to coerce, intimidate, harass, or cause substantial emotional distress to a person, using electronic means to support severe, repeated, and hostile behavior, shall be fined under this title or imprisoned not more than two years, or both." H.R. 1966 § 3.

of his personal property, Calixte was deprived not only of his cell phone and other electronic equipment, but also of the use of his computer for academic and other purposes.

One of the most important issues raised in *Calixte* is whether the need for surveillance and monitoring has been appropriately balanced with legitimate student privacy rights. As previously noted,[100] terms of use policies concerning university technology resources generally provide little or no privacy protection for campus e-mail sent using the university's technology resources.[101] The same would be true of phone conversations and text messages transmitted using university networks and other resources.[102]

Beyond the limitations on the expectation of privacy contained in the terms of use policies, federal, state and common laws may provide some guidance for the nature and extent of the privacy rights of students and others where campus surveillance and monitoring occurs. The question surrounding these laws involves a discussion of these rights as they relate to information stored on computers and other electronic devices.

III. FEDERAL PRIVACY LAWS

A. The United States Constitution

The United States' constitutional source of the right to privacy is an implied or penumbral right[103]—rather than an expressed or enumerated right—found in the Fourth,[104] Fifth,[105] Ninth,[106] and Fourteenth[107]

100. *See* PROFESSIONAL STANDARDS AND BUSINESS CONDUCT, *supra* note 81.

101. *See id.*

102. *See id.*

103. Griswold v. Connecticut, 381 U.S. 479, 483 (1965). The Supreme Court declared unconstitutional a Connecticut statute prohibiting the use of birth control devices and the giving of advice regarding their use. *Id.* at 486. The Court further recognized that the Bill of Rights provided us with certain penumbral rights that created "zones of privacy," locations where privacy is expected. *Id.* at 484.

104. U.S. CONST. amend. IV.

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Id.

105. U.S. CONST. amend. V ("No person . . . shall be compelled, in any criminal case, to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law . . . .").

106. U.S. CONST. amend. IX ("The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.").

107. U.S. CONST. amend. XIV, § 1.

Amendments. These rights apply to unwarranted intrusions by the *government* and apply to students attending public or state universities where campus police exercise the same police authority and power as state and local police.[108] In the absence of an exception, these rights do not apply to private universities. An exception may apply if a court determines that the alleged activity of the private university arose out of an act by a private university that was "fairly attributable to the State" (known as the "state action" requirement) and consequently subject to federal law.[109]

Exceptions may also apply where private universities summon local or state police to assist campus police, or where a state statute transfers some of its state police authority and power to private university campus police departments, such as the right to make arrests.[110] Therefore, if a private university's campus police department has been granted this statutory authority and subsequently engages in electronic surveillance, the methods employed should not violate privacy rights protected by the United States Constitution. Even if a student cannot seek redress under the Federal

> No State shall make or enforce any law which shall abridge the privileges and immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.

Id.; *see also* Goss v. Lopez, 419 U.S. 565, 581 (1975) (finding the suspension of nine Ohio public school students for up to ten days without a hearing to be a denial of due process under the Fourteenth Amendment).

108. *See, e.g.*, Arizona State University, ASU Police Officers' Legal Authority and Jurisdiction, http://cfo.asu.edu/police-jurisdiction (last visited May 25, 2010).

> ASU Police Officers are state certified, and have the same powers as any police officer in the State of Arizona. All police officers in the State of Arizona, including ASU police officers, have the authority to enforce state and federal laws within limits imposed by the state and federal constitutions and judicial rulings.

Id.

109. Lugar v. Edmondson Oil Co., 457 U.S. 922, 939–42 (1982); *see also* Zachariah Logodice v. Trs. of Central Maine Inst., 296 F.3d 22, 31 (1st Cir. 2002) (holding that disciplinary actions of the Central Maine Institute, a private high school under contract with the State of Maine, constituted "state action" and were therefore subject to Fourteenth Amendment scrutiny).

110. *See, e.g.*, MASS. GEN. LAWS ch. 22C, § 63 (2010).

> The colonel may . . . at the request of an officer of a college, university, other educational institution or hospital licensed pursuant to section fifty-one of chapter one hundred and eleven, appoint employees of such college, university, other educational institution or hospital as special state police officers. Such special state police officers shall . . . have the same power to make arrests as regular police officers for any criminal offense committed in or upon lands or structures owned, used or occupied by such college, university, or other institution or hospital.

Id.

> The governing board of each private institution of higher education is authorized to establish . . . a campus police department . . . . Except as such provisions apply exclusively to public institutions or employees, the provisions of this chapter shall apply to the appointment and employment of officers, operation, powers, duties and jurisdiction of private campus police departments, and such departments shall be subject to and enjoy the benefits of this chapter.

VA. CODE ANN. §§ 23-232.1 (2010) (citation omitted).

Constitution for the invasion of privacy interests by campus police, he the student may nevertheless find protection under state constitutions and statutes[111] or the common law of torts.[112]

B. Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act of 1990

The essential provisions of the Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act of 1990[113] ("Clery Act") require post-secondary institutions receiving federal student aid to: (1) set policies that warn the campus of potential threats of violence[114]; (2) report annual campus crime statistics to the university community[115]; (3) keep daily campus crime logs[116]; and (4) describe their campus security policies.[117] The Clery Act also contains privacy provisions that prohibit universities from identifying the victims of crimes and persons accused of committing crimes[118] and from disclosing confidential or privileged information.[119]

Additionally, each year, universities must submit a copy of their security report to the Secretary of the Department of Education.[120] The annual security report must include a statement of the university's current policies and procedures for students and other university members to report crimes or emergencies, as well as its policy for responding to such reports. The list of the other required contents of the annual report is quite extensive and relates to additional, mandatory statements and statistics.[121]

If a university fails to file its annual security report, the Secretary is authorized to impose a fine of at least $27,500 for each violation of the

111. *See* MASS. GEN. LAWS ch. 214, § 1B ("A person shall have a right against unreasonable, substantial or serious interference with his privacy. The superior court shall have jurisdiction in equity to enforce such right and in connection therewith to award damages.").

112. RESTATEMENT (SECOND) OF TORTS §§ 652A–E (1997) (describing the torts of "Intrusion upon Seclusion," "Public Disclosure of Private Facts Causing Injury to Reputation," "Publicity Placing Another in a False Light," and "Misappropriation of a Person's Name or Likeness Causing Injury to Reputation").

113. 20 U.S.C. § 1092(f)(15) (2006).

114. *Id.* § 1092(f)(1).

115. *Id.*

116. *Id.*

117. *Id.*

118. *Id.* § 1092(f)(7).

119. *Id.* § 1092(f)(10).

120. *Id.* § 1092(f)(5).

121. *Id.* § 1092(f)(1)(A)–(H).

Clery Act depending upon the seriousness of the violation.[122] For instance, Eastern Michigan University paid a fine of $350,000 in 2008[123]—the largest to date under the Clery Act[124]—for failing to inform the campus of the murder of a student in her dorm room. Exacerbating the violation, Eastern Michigan officials reported[125] that there was no "foul play" involved, and staff members told students there was "no reason to worry."[126] Since 1990, Congress has passed several amendments modifying and expanding the requirements of the annual security report.[127]

C. Electronic Communications Privacy Act of 1986

Two of the most significant federal statutes addressing privacy rights as they pertain to electronic surveillance and disclosure of electronic communications are the Electronic Communications Privacy Act of 1986 (ECPA)[128] and the Family Educational Rights and Privacy Act of 1974 (FERPA).[129]

The ECPA amended existing federal anti-wiretapping statutes in order to expand privacy protections to new electronic communication methods such as cellular phones and e-mail.[130] In general, the ECPA applies to electronic surveillance activities of the government.[131] The ECPA can apply to private

122. *Id.* § 1092(f)(13); Adjustment of Civil Monetary penalties for Inflation, 67 Fed. Reg. 222 (Nov. 18, 2002) (to be codified at 34 C.F.R. pt. 36).

123. *Eastern Michigan University to Pay $350,000 Fine for Clery Act Violation*, CHRON. OF HIGHER EDUC., June 6, 2008, http://chronicle.com/article/Eastern-Michigan-U-to-Pay-/41112/.

124. *Id.*

125. Sara Lipkin, *A University Is Accused of Hushing Up a Murder*, CHRON. OF HIGHER EDUC., Mar. 23, 2007, http://chronicle.com/article/A-University-Is-Accused-of/12175.

126. *Id.*

127. *See, e.g.*, Higher Education Technical Amendments of 1991, Pub. L. No. 102-26, § 10(e), 105 Stat. 123, 125 (changing annual security reporting period from academic year to calendar year); Higher Education Amendments of 1992, Pub. L. No. 102-325, § 486(c), 106 Stat. 448, 621–23 (annual security report must include a statement of the university's policies and provisions for the victims of sexual assaults); Higher Education Amendments of 1998, Pub. L. No. 105-244, § 486(e), 112 Stat. 1581 (expanding the categories of crimes that must be reported); Victims of Trafficking and Violence Protection Act of 2000, Pub. L. No. 106-386, § 1601, 114 Stat. 1464, 1537–38 (universities must make available public sex offender registration information for sex offenders on campus); *see also* New Campus Security Regulations, 34 C.F.R. § 668.46 (2010) (annual security report must include statistics for hate crimes, notification requirements regarding missing students, and a description of the university's emergency response and evacuation procedures).

128. 18 U.S.C. §§ 2510–22 (2006).

129. 20 U.S.C. § 1232g (2006) ("Buckley Amendment").

130. *Compare* Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197, *with* 18 U.S.C. § 2510 (2006).

131. Jamie Lewis Keith, *The War on Terrorism Affects the Academy: Principal Post-September 11, 2001 Federal Anti-Terrorism Statutes, Regulations, and Policies that Apply to Colleges and Universities*, 30 J.C. & U.L. 239, 303–05 (2004).

universities if a court determines that the university engaged in a state action, enlisted the aid of outside law enforcement agencies, or if its campus police department was granted local or state police powers and authority.[132] Recall, for example, that Boston College enlisted the assistance of the Massachusetts State Police to assist in the *Calixte* investigation.[133] State action requirements aside, university counsels have indicated that they will treat the ECPA as if it applies to e-mail and voicemail systems.[134]

Title I of the ECPA[135] prohibits any person from intercepting intentionally or without authorization a wire, oral or other electronic communication[136] affecting interstate or foreign commerce and from disclosing the contents of those communications.[137] The interception under the ECPA must be effectuated simultaneously with the transmission of the communication.[138] This requirement would not apply to interceptions of communications in storage since the transmission would have already occurred.[139] The requirement under Title I that "interception" of an email or other electronic communication be authorized by a search warrant[140] applies to both federal[141] and state[142] law enforcement agencies.

132. 18 U.S.C. § 2511 (2006); *Lugar*, 457 U.S. at 928–29.

133. Brief of Respondent, *In re* Search Warrant Executed on March 30, 2009 at the Residence of Riccardo Calixte No. SJ-2009-0212 (Mass. Dist. Ct. Apr. 27, 2009) (No. 0912SW03), *available at* www.eff.org/files/filenode/inresearchBC/BC-oppositiontomotiontoquash.pdf.

134. *See, e.g.*, Catholic Univ. of Am., Summary of Federal Laws, http://counsel.cua.edu/fedlaw/Ecpa.cfm (last visited Mar. 14, 2011) (stating that "Title18 U.S.C. § 2510(15) extends the Act's protection to university-owned telephone, e-mail and Internet systems," but providing no support for the assertion); Keith, *supra* note 131, at 303–04 n.334 (2004) ("[I]t is prudent for a college or university to interpret the ECPA as applying to all communications on its e-mail and voicemail systems, whether opened or unopened, until otherwise advised by a court that has considered the institution's particular situation.").

135. 18 U.S.C. § 2511 (2006).

136. *Id.* § 2510 ("[A]ny transfer of signs, signals, writing, images, data, or intelligence of any nature by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce."). The most notable exclusions are the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit and any wire or oral communication. *Id.* § 2510(12)(A)-(B).

137. 18 U.S.C. § 2511.

138. Frasier v. Nationwide Ins. Co., 352 F.3d 107, 113 (3d Cir. 2003).

139. *See* Jessica Belskis, *Applying the Wiretap Act to Online Communications After* United States v. Councilman, 2 SHIDLER J. L. COMMERCE & TECH. 18 (2006).

140. *See* 18 U.S.C. § 2518 (2010) (describing the requirements for an application for the search warrant). There is some disagreement about whether communications in electronic storage will trigger the warrant requirement and possible violation of ECPA. *See, e.g.*, United States v. Councilman, 245 F. Supp. 2d 319, 321 (D. Mass. 2003), *aff'd*, 373 F.3d 197 (1st Cir. 2004), *rev'd en banc*, 418 F.3d 67 (1st Cir. 2005) (holding that interception of a communication in storage is an offense under the Wiretap Act).

141. 18 U.S.C. § 2516(1) (2006) ("Authorization for Interception of Wire, Oral or Electronic Communications.").

142. *Id.* § 2516(2).

The prohibition against "interception" contained in Title I potentially applies to a public or private university that intercept and disclose, without proper authorization, the contents of a student's e-mail or other electronic communication to a third party, such as faculty member. If law enforcement seeks to compel a university to disclose the content of an e-mail message stored on its servers, most cases require a search warrant. Civil and criminal sanctions are allowed by the ECPA.[143] Additionally, Title I prohibits an Internet service provider (ISP) from intentionally disclosing the contents of a communication to any person or entity other than the addressee or its intended recipient.[144]

Title II of the ECPA[145] makes it unlawful for a person or entity providing any electronic communication service to the public to knowingly divulge t the contents of a communication while in electronic storage by that service without authorization.[146] This applies to data stored on disks or other storage devices by a person or entity providing they qualify as providing an "electronic communication service"[147] available to the public.[148] Universities that allow students, other members of its community, and the public-at-large to access e-mails through university computers or devices, either on and off the campus, will likely satisfy this qualification; however, relevant case law is sparse.[149] Therefore, it may in some cases be a violation of a student's privacy under the ECPA for a university to access and disclose the contents of a student's e-mail to a third party without proper authorization. Such authorization may derive from the prior express

143. *Id.* § 2511(4)(a). Penalties include fines or imprisonment for up to five years. *Id.*

144. *Id.* § 2511(3)(a).

145. *Id.* §§ 2701–12 ("Stored Communications Act").

146. *Id.* § 2702(a)(1). *See* Andersen Consulting LLP v. UOP, 991 F. Supp. 1041 (N.D. Ill. 1998). UOP hired Andersen to perform a systems integration project in 1992. *Id.* at 1042. During the project, Andersen employees had access to and used UOP's internal e-mail system to communicate with each other, with UOP, and with third parties. *Id.* Dissatisfied with Andersen's performance, UOP terminated the project in December 1993. *Id.* UOP disclosed the contents of Andersen's e-mails to the Wall Street Journal which published them. *Id.* Andersen brought suit under § 2702(a)(1) arguing that UOP provided an electronic communication service to the public making the disclosure of the e-mails unlawful. *Id.* at 1042–43. The court disagreed and dismissed the suit, reasoning that UOP's e-mail system was used solely for internal communications only utilized its e-mail system for internal communications and therefore did not provide a service to the public. *Id.* at 1045.

147. 18 U.S.C. § 2510(15) (2006) (defining "electronic communications service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications").

148. *Id.* § 2702(a)(1); *see* Andersen Consulting LLP, 991 F. Supp. 1041; Robert Konop v. Hawaiian Airlines, 236 F.3d 1035 (9th Cir. 2001).

149. One university attorney concludes that, in light of current uncertainty regarding the applicability of the ECPA to the university environment, "it is prudent for a college or university to interpret the ECPA as applying to all communications on its e-mail and voice-mail systems, whether opened or unopened, until otherwise advised by a court that has considered the institution's particular situation." Keith, *supra* note 131, at 303 n.334.

consent of the student, a clear written policy regarding computer terms of use,[150] or a log-on banner. Disclosure may also be lawful in case of emergency where disclosure is made to a government law enforcement agency.[151] Here, again, the university's terms of use policy should clearly and conspicuously inform the users of its system that the university reserves the right to access stored electronic communications. The sanctions for violations of Title II are similar to those of TitleI.[152]

Title III[153] applies to wiretaps, pen registers,[154] and trap and trace devices.[155] Before law enforcement uses these devices can to collect real time information, a search warrant must be obtained. The order will ordinarily be granted only if the information sought relates to a criminal investigation. As for government access to e-mail and other electronic communications held in storage, the ECPA has a special rule regarding search warrants.[156] To access e-mail that has been in storage for 180 days or less, law enforcement must obtain a search warrant in accordance with the Federal Rules of Criminal Procedure,[157] or its state law equivalent, in order to compel a service provider to disclose the contents of the communication.[158] However, e-mail in storage for more than 180 days is considered stale and thus may be accessed merely by subpoena or court order.[159] Critics of this provision argue that it is outdated, reasoning that Fourth Amendment protection should not depend on the age of e-mail or its status (opened versus unopened).[160] They further argue that since Congress

150. 18 U.S.C. § 2702(b)(1) (2006) ("A provider . . . may divulge the contents of a communication . . . with the lawful consent of the originator or an addressee or an intended recipient of such communication . . . ."); *see also* S. Rep. No. 99-541, at 37 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3591 ("These exceptions permit disclosure . . . with the lawful consent of the sender or the addressee or an intended recipient of such communication . . . .").

151. 18 U.S.C. § 2702(b)(8) (2006) ("A provider . . . may divulge the contents of a communication . . . to a governmental entity if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency."); *see id.* § 2701(c).

152. *Id.* § 2701(a)–(b).

153. *Id.* §§ 3121–3127 ("Pen Register Act").

154. A pen register records phone numbers dialed as outgoing calls. *Id.* § 3127(3).

155. A trap and trace device records the phone numbers from which incoming calls originate. *Id.* § 3127(4).

156. *Id.* § 2703.

157. FED. R. CRIM. P. 41.

158. 18 U.S.C. § 2703(a) (2006).

159. *Id.* § 2703(b), (d); *see* also, United States v. Weaver, 636 F. Supp. 2d 769, 770–71 (C.D. Ill. 2009).

160. James X. Dempsey, *Digital Search & Seizure: Standards for Government Access to Communications and Associated Data*, 970 PRACTICING L. INST. 687, 701 (2009).

passed the ECPA in 1986, technology has advanced to the point where web-based e-mail is stored and saved on third party servers regardless of the e-mail's age or other status.[161]

The September 11, 2001 attack on the United States led to the passage of the USA PATRIOT Act by Congress.[162] This Act and several other federal statutes[163] have amended the ECPA by broadening the surveillance powers of the Federal Government in cases involving suspected threats of terrorism, which effectively reduces the privacy rights provided by the ECPA.[164] Thus, if the government believes a university student or another member of the university community is involved in terrorist activities against the United States or its interests, privacy rights granted under the ECPA may be suspended in the interest of national security.[165]

In addition, there are exceptions to Title I (also applicable to Title II and III)[166] that have possible applications to universities. One exception applies to an ISP[167] and provides that an online operator, officer, employer, or agent of a provider of wire or electronic communication service may, in the ordinary course of its business, intercept, disclose, or use an electronic communication necessary to the rendition of their service or to the

161. *Id.* at 707.

162. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified as amended in scattered sections of 18 U.S.C., 50 U.S.C., 22 U.S.C., 31 U.S.C., and 47 U.S.C.). The USA PATRIOT Act has been the subject of much discussion and, in some cases, criticism regarding its effect on individual privacy. *See, e.g.*, EFF Analysis of the Provisions of the USA PATRIOT Act, Oct. 31, 2001, http://w2.eff.org/Privacy/Surveillance/Terrorism/20011031_eff_usa_patriot_analysis.php.

163. *See*, *e.g.*, Communications Assistance for Law Enforcement Act (CALEA) of 1994, Pub. L. No. 103-414, 108 Stat. 4279 (codified as amended in scattered sections of 47 U.S.C). CALEA further defines the existing statutory obligation of telecommunications carriers to assist law enforcement in executing electronic surveillance pursuant to court order or other lawful authorization. *Id.* The objective of CALEA implementation is to preserve law enforcement's ability to conduct lawfully authorized electronic surveillance while preserving public safety, the public's right to privacy, and the telecommunications industry's competitiveness. *See* About the CALEA Implementation Unit, http://askcalea.net/aboutus.html (last visited Mar. 14, 2011); Foreign Intelligence Surveillance Act (FIFSA) of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (current version at 50 U.S.C. §§ 1801-11 (2006) (establishing procedures for the authorization of electronic surveillance for the purpose of gathering foreign intelligence)).

164. USA PATRIOT Act, § 505, 115 Stat. at 278 (amending § 2516 of ECPA to expand the authority of federal agencies to intercept wire, oral and electronic communications in suspected cases of terrorism). Section 202 of the PATRIOT Act allows interceptions in cases involving computer fraud and abuse. *See id.* § 202.

165. *See, e.g.*, *id.* § 505, 115 Stat. at 365–66 (requiring disclosure of subscriber information or electronic communication transaction records, but not the content of messages themselves, in response to an FBI request); *cf.* John Doe, Inc. v. Mukasey, 549 F.3d 861, 885 (2d Cir. 2008) (partially invalidating 18 U.S.C. §§ 2709(c), 3511(b) (2006)).

166. *See* 18 U.S.C. § 2511(2)(a) (2006).

167. *See id.* § 2511(2)(a)(i).

protection of the rights or property of that service. This exception applies to both internal providers, such as Boston College in *Calixte*, and external providers such as AT&T, Yahoo, AOL, and Verizon. Random observing and monitoring of electronic communications would not be allowed under this exception unless mechanical or quality control was being investigated.[168] This exception could apply to Boston College, since its terms of use policy[169] specifically allows it to intercept and disclose the contents of an individual's electronic data, software, or communication files (including e-mails) where a legitimate or urgent situation exists that is sufficiently strong enough to trump Boston College's commitment to honor the privacy of the members of its community.[170] Such situations include maintaining the integrity of its system (e.g., tracking viruses), protecting system security, investigating possible improper use of its system, protecting property rights, and responding to legal obligations (e.g., subpoenas). It would appear that Boston College's actions would result from an investigation to ensure the security of its electronic communications system. Accordingly, for Boston College to fall within this exception it would have to prove that its access and disclosure of Calixte's e-mails were done to protect Boston College's rights or property interests.[171]

Another relevant exception allows the monitoring and interception of an e-mail or other electronic communication where the originator, addressee, or intended recipient of an electronic communication has given the ISP prior consent to intercept.[172] Such consent could be provided in a computer use policy or a subscription agreement, or may be displayed on a login banner. Boston College's terms of use policy[173] would likely meet the requirements of this exception and would apply to the school's interception and disclosure of Calixte's e-mails. A claim of a violation of privacy rights would be precluded unless the policy contains a term prohibiting "electronic 'snooping' or the use of technological resources for the purposes of satisfying idle curiosity about the affairs of others."[174]

168. *See* United States v. Mullins, 992 F.2d. 1472, 1478 (9th Cir. 1993) (ruling that American Airlines acted as a service provider under this exception when one of its employees investigated discrepancies in reservations made by a travel agent on an online travel reservations system it maintained).

169. *See* PROFESSIONAL STANDARDS AND BUSINESS CONDUCT, *supra* note 81.

170. *See id.*

171. *See id.*

172. 18 U.S.C. § 2511(2)(d), (3)(b)(ii) (2006)).

173. *See* PROFESSIONAL STANDARDS AND BUSINESS CONDUCT, *supra* note 81.

174. *Id.*

A third exception applies to any device, such as an extension telephone or other monitoring device (computers are not mentioned), furnished to ,and used by, a subscriber or user of wire or electronic communications services in the ordinary course of business. [175] It follows that an employer in the ordinary course of its business could use a monitoring device obtained from a telephone company or other ISP to intercept employee communications transmitted in the workplace to determine if they are related to work or business. Prior consent or a monitoring policy of which employees have knowledge would be a prerequisite for this exception. The consent or policy should expressly provide for monitoring of both business and personal calls, otherwise the exception could be limited to communications only of a business nature.[176] Courts have not yet definitively ruled whether this exception would apply to universities intercepting communications of students who, like Calixte, are also university employees. However, as discussed earlier, a university could intercept under other exceptions to the ECPA.

In the recent case of *City of Ontario, California v. Quon*,[177] the U.S. Supreme Court addressed important issues related to privacy protections under the Fourth Amendment and the Stored Communications Act involved in accessing and disclosing the contents of text messages. Although the case involved state action and public employees, the decision could impact private universities that engage in activities that qualify as state actions as discussed earlier.[178]

Jeff Quon was a police officer (SWAT team member) with the City of Ontario Police Department (OPD).[179] Quon, along with other police officers and City employees, were issued alphanumeric pagers to send and receive text messages.[180] The City's terms of use policy allowed it to monitor and log all e-mail and Internet usage with or without notice.[181] It also informed City employees that they would have no expectation of privacy or confidentiality when using Ontario's computers or technology

175. 18 U.S.C. § 2510(5)(a).

176. *See* Watkins v. L.M. Berry & Co., 704 F.2d. 577 (11th Cir. 1983) (where the employer's policy applied only to business-related calls, intercepting the personal call made by the employee to a friend violated the Federal Wiretap Act); *see also* Fischer v. Mt. Olive Lutheran Church, Inc., 207 F. Supp. 2d 914 (W.D. Wis. 2002).

177. 130 S. Ct. 2619 (2010).

178. *See supra* note 108 and accompanying text.

179. *Quon*, 130 S. Ct. at 2624.

180. *Id.* at 2625.

181. *Id.*

resources.[182] Although text messages were not expressly included in the policy, the City informed its employees, including its police, that text messages would be treated similar to e-mails and thus subject to audit.[183]

The City's contract with Arch Wireless, its ISP, limited the number of text messages employees could send and receive per month.[184] Exceeding the limit would result in additional fees.[185] Quon and other officers were aware of the terms of use policy but were informally told that as long as they paid overage to the City, they could send and receive personal texts without being subject to audits.[186] Quon continuously exceeded the contract allowance and reimbursed the City for the overage.[187]

Nevertheless, the OPD Chief of Police obtained the transcripts of Quon's text messages stored with Arch without a search warrant to determine if the limits were too low and if Quon was paying for work-related rather than personal messages.[188] The transcripts revealed that of the 456 messages sent or received by Quon in one month, fifty-seven were work-related while the others were personal in nature.[189] As a result, Quon was disciplined.[190] He filed suit in federal district court and alleged violations of his privacy rights under the Fourth Amendment of the U.S. Constitution, the California Constitution, and the Stored Communications Act for releasing the stored transcripts and their contents to the OPD without Quon's consent.[191] A jury decided that since the Chief's purpose in obtaining the transcripts was to determine the efficacy of the limits and not whether Quon was involved in misconduct, the search was reasonable.[192] Relying in part on *O'Connor v.*

182. *Id.*

183. *Id.*

> In this case, for instance, an email sent on a City computer was transmitted through the City's own data servers, but a text message sent on one of the City's pagers was transmitted using wireless radio frequencies from an individual pager to a receiving station owned by Arch Wireless. It was routed through Arch Wireless' computer network, where it remained until the recipient's pager or cellular telephone was ready to receive the message, at which point Arch Wireless transmitted the message from the transmitting station nearest to the recipient. After delivery, Arch Wireless retained a copy on its computer servers. The message did not pass through computers owned by the City.

Id.

184. *Id.*

185. *Id.*

186. *Id.*

187. *Id.*

188. *Id.* at 2626.

189. *Id.*

190. *Id.*

191. 445 F. Supp. 2d 1116, 1128 (C.D. Cal. 2006), *rev'd*, 529 F.3d 892,899 (9th Cir. 2008).

192. *Quon*, 529 F.3d at 899 (9th Cir. 2008), *rev'g*, 445 F. Supp. 2d 1116, 1128 (C.D. Cal. 2006), *rev'd*, 130 S. Ct. 2619 (2010).

Ortega,[193] the Ninth Circuit reversed and held that Quon had a reasonable expectation of privacy in the text messages and that the scope of the search was unreasonable under the Fourth Amendment.[194]

The U.S. Supreme Court unanimously reversed and remanded, finding the search of Quon's text messages was reasonable and did not violate the Fourth Amendment.[195] According to the Court, the search was motivated by a legitimate work-related purpose and was not excessive in scope.[196] The Court assumed without deciding that Quon had a reasonable expectation of privacy in his text messages.[197] As for private universities and its employees, the Court also concluded that the search would be regarded as reasonable and normal in the private-employer context.[198] Seemingly, this would include universities like Boston College and student employees like Calixte.

D. Family Educational and Privacy Rights Act of 1974

The Family Educational and Privacy Rights Act of 1974 (FERPA)[199] applies to both public and private colleges and universities receiving federal funds.[200] It is to be noted that once a child is eighteen years old and a student at a university, the rights under FERPA benefit the student rather than the parent or guardian.[201] FERPA prevents disclosure of information contained in a university student's education records.[202] Education records are defined to include any document that contains information directly related to a student that is maintained by or on behalf of an educational

193. O'Connor v. Ortega, 480 U.S. 709, 719 (1987) (holding that public employees have a reasonable expectation of privacy in their desks, file cabinets and other work-related areas subject to Fourth Amendment protection). The Court noted that "[t]he operational realities of the workplace . . . may make *some* employees' expectations of privacy unreasonable . . . [and] may be reduced by virtue of actual office practices and procedures, or by legitimate regulation." *Id.* at 717. The Court further noted that given the variety of environments in which employees work, whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis. *Id.* at 718.

194. *Quon*, 529 F.3d at 908–09.

195. Quon, 130 S. Ct. at 2633.

196. *Id.* at 2632.

197. *Id.* at 2633.

198. *Id.* (citing O'Connor, 480 U.S. at 732) (Scalia, J. concurring).

199. 20 U.S.C § 1232g (2006); see 34 C.F.R. § 99.1 (2010). FERPA is also known as the Buckley Amendment and is named after Senator James Buckley of New York, one of its sponsors. *See e.g.,* Elec. Privacy Info. Ctr., Family Educational Right to Privacy Act (Buckley Amendment), http://epic.org/privacy/education/ferpa.html (last visited Mar. 13, 2011).

200. 20 U.S.C. § 1232g(a)(1)(A) (2006).

201. *Id.* § 1232h(c)(5)(B).

202. *Id.* § 1232g.

institution.[203] Absent a student's written consent,[204] information contained in a student's education records cannot be disclosed to others, subject to certain exceptions.[205]

However, records of incident reports created and maintained by campus police for law enforcement purposes are not part of a student's educational records and constitute a major exception to FERPA.[206] Consequently, these reports may be shared with external law enforcement agencies without posing issues of student privacy under FERPA. Since Boston College's campus police were investigating the allegations against Calixte to determine whether he was engaged in criminal activity, it is likely that Boston College did not violate his privacy rights under FERPA by disclosing the evidence to the Newton police without his permission.

Also recall that officials at Virginia Tech were prevented by FERPA from informing Cho's parents about his precarious mental stability.[207] Cho's written consent was required before his condition could be disclosed to his parents. Arguably, even if they were informed, it probably would not have prevented his actions.

FERPA allows a university to disclose information about a student if ordered to do so by a court or valid subpoena, provided that the student is notified of the order or subpoena in advance of compliance by the university.[208] An exception to the consent requirement arises where the issuing court orders non-disclosure of the contents, which could be the case with a grand jury subpoena.[209] The same would be true for investigations or prosecutions of terrorism under the USA PATRIOT Act.[210] FERPA would also allow disclosure of contents if a "health or safety emergency" exists and "knowledge of the information is necessary to protect the health and safety of the student or other persons.[211] Thus, if Calixte presented a threat

203. *Id.* § 1232g(a)(4)(A).
204. *Id.* § 1232g(a)(6)(b)(1).
205. *Id.* § 1232g(a)(6)(b)(1)(A)-(J).
206. *Id.* § 1232g(a)(4)(B)(ii).
207. *See supra* note 18 and accompanying text.
208. 20 U.S.C. § 1232g(b)(2)(B) (2006).
209. *Id.* § 1232g(b)(1)(J).
210. Pub. L. No. 107-56, § 507, 115 Stat. 272 (2001) (amending FERPA to allow the U.S. Attorney General to obtain, upon application to a court of competent jurisdiction, education records relevant to an investigation or prosecution of domestic or foreign acts of terrorism).
211. 20 U.S.C. § 1232g(b)(1)(I).

to the safety of Bennefield, and there was information in Calixte's education records that could protect Bennefield from harm, Boston College could disclose it to Bennefield.[212]

If a university violates FERPA, the U.S. Secretary of Education has the authority to withhold funds under any applicable program, issue a cease and desist order compelling compliance, or terminate funding for further non-compliance.[213] Furthermore, FERPA does not provide students with a private cause of action for violation of its provisions.[214] Instead, students who believe they have a claim for a FERPA violation must file a complaint with the Secretary of Education in whom FERPA vests the power to enforce its regulations.[215]

IV. STATE PRIVACY LAWS

State privacy laws grant rights similar to those provided by the federal laws discussed above. For example, Article IV of the Massachusetts Declaration of Rights provides rights similar to those provided by FERPA and the Fourth Amendment with respect to search and seizure privacy in the context of education and academic records, searches of dorm rooms, computers and electronic communications.[216] Massachusetts also protects individuals against "unreasonable, substantial or serious interference" with their privacy.[217]

212. *Id.*

213. *See id.* § 1232g(b)(7)(f); *see also* 34 C.F.R. § 99.67 (2010).

214. *See* Gonzaga Univ. v. Doe, 536 U.S. 273, 273–74 (2002). The respondent, a student at Gonzaga, wished to become an elementary school teacher. *Id.* at 277. One of the requirements was for him to obtain an affidavit of good moral character from Gonzaga University. *Id.* Gonzaga's teacher certification specialist overheard one student tell another that the respondent had engaged in sexual misconduct, whereupon the University prompted an investigation, contacted the state agency in charge of certification, and identified the respondent by name, all of which resulted in the respondent not receiving the necessary affidavit. *Id.* He brought suit claiming the information released without his consent violated FERPA under Section 1232g. *Id.* The Court held that there is no private right of action under the provisions of FERPA. *Id.* at 289.

215. 20 U.S.C. § 1232g(a)(7), (f)-(g).

216. MASS. CONST. art. XV (2010).

> Every subject has a right to be secure from all unreasonable searches and seizures of his person, his houses, his papers, and all his possessions. All warrants, therefore, are contrary to this right, if the cause or foundation of them be not previously supported by oath or affirmation; and if the order in the warrant to a civil officer, to make search in suspected places, or to arrest one or more suspected persons, or to seize their property, be not accompanied with a special designation of the persons or objects of search, arrest, or seizure: and no warrant ought to be issued but in cases, and with the formalities prescribed by the laws.

Id.; *see* MASS. GEN. LAWS ch. 214 § 1B (2010).

217. MASS GEN. LAWS ch. 214 § 1B.

California law provides comparable rights. A provision of its Education Code requires schools to give written notice to parents of their rights and responsibilities with respect to school records.[218] In addition to other rights, the California Constitution recognizes an "inalienable right" to privacy.[219]

States also afford universities the right to adopt and implement their own student privacy rules and policies, especially as they relate to dorm rooms, educational records, electronic communications, and the use of university resources. Recall the discussion above concerning the contract between the university and the student and the importance of the student handbook as a source for identifying student privacy rights.

V. COMMON LAW TORTS FOR INVASION OF PRIVACY

> Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone."[220]

When this quotation was written by Samuel Warren and Louis Brandeis in their 1890 article "The Right to Privacy," there were no laws or constitutional provisions that were considered to recognize an individual's "right to privacy." However, Warren and Brandeis may have been prophetic when they alluded to the significance of "recent inventions and business methods."[221] They may have envisioned a time when those "inventions and business methods" would create an environment where private and personal information are shared via e-mail, text messages, social networks,[222] blogs, and other means of electronic communications, thus necessitating laws designed to protect privacy when threatened or invaded.

The federal and state laws discussed herein may not be sufficient for such purposes. Recall that privacy rights implied in the U.S. Constitution generally apply only to government intrusions, except where private entities engage in "state action," and FERPA does not provide a private cause of action. Consequently, students like Calixte who believe their right to privacy has been violated must pursue alternative legal theories. One set of

218. CAL. EDUC. CODE § 49063 (2009).

219. CAL. CONST. art. I, § 1 ("All people are by nature free and independent and have inalienable rights. Among these are . . . pursuing and obtaining . . . privacy.").

220. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).

221. *Id.*

222. For a discussion of the privacy controversy involving social networks, including those of Facebook and Google, see Jennifer Martinez, *Lawmakers Grill Internet Firms over Privacy Protection*, L.A. TIMES, July 28, 2010, http://articles.latimes.com/2010/jul/28/business/la-fi-tech-hearing-20100728; *see also* Posting of Jennifer Valentino DeVries to Wall St. J. Blog (July 21, 2010, 17:56 EST), http://blogs.wsj.com/digits/2010/07/21/facebook-touts-its-500-million-friends/.

possible theories includes the four common law intentional torts for invasion of privacy found in the Restatement (Second) of Torts[223] and advanced by Professor Prosser in his seminal article on privacy.[224]

These intentional torts include: Intrusion upon Seclusion;[225] Misappropriation of a Person's Name or Likeness Causing Injury to Reputation;[226] Publicity Given to Private Facts;[227] Publicity Placing Another in a False Light.[228] The following discussion describes the elements required for each of these torts and their viability as legal theories for students seeking to hold a university liable for invasion of privacy. It should be emphasized that the first requirement in all such suits is to establish the existence of a reasonable expectation of privacy.

A. Intrusion Upon Seclusion

Intentionally intruding, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns may give rise to liability to the other for invasion of privacy if the intrusion would be highly offensive to a reasonable person.[229] The tort of intrusion upon seclusion usually involves entering a private room or area without authorization, opening private personal mail, searching a safe or wallet, examining a private bank account or compelling by a forged court order to permit inspection of one's personal documents.[230] As discussed above, absent an emergency or other exception, a university cannot search the contents of a student's dorm room without obtaining a duly authorized search warrant from a local court.[231] In *Calixte*, Boston College seemingly obtained an authorized search warrant from the Newton District Court that was subsequently held to lack sufficient probable cause.[232] Since there are no cases on point, it is mere speculation as to what would be the result if Calixte sought to hold Boston College liable for intrusion upon his seclusion and a violation of his privacy resulting in damages. At a minimum, he would need to prove that (1) he held a reasonable expectation

223. RESTATEMENT (SECOND) OF TORTS §§ 652 B–E (1977).
224. William Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960).
225. RESTATEMENT (SECOND) OF TORTS § 652B (1977).
226. *Id.* § 652C.
227. *Id.* § 652D.
228. *Id.* § 652E.
229. *Id.* § 652B.
230. *Id.* § 652B cmt. b.
231. *See infra* Part II.A.
232. *In re* Riccardo Calixte, No. SJ-2009-0212, *supra* note 71, at 11.

of privacy in his dorm room and in his electronic communications,[233] (2) that the warrant obtained was invalid notwithstanding that its duly authorization, and finally, (3) that Boston College's intrusion was intentional and would be highly offensive to a reasonable person.[234]

To avoid possible liability for intrusion upon seclusion, universities employing campus cameras are cautioned to avoid surveillance of dorm rooms and other private areas, absent a legal justification, and to limit the use of tracking or monitoring devices (web-bugs, "spy ware" or e-mail wiretaps) of university-owned electronic equipment to its terms of use policy or other applicable laws.[235]

B. Misappropriation of a Person's Name or Likeness Causing Injury to Reputation

Misappropriation of a person's name or likeness occurs when one uses the name or likeness of a living person without their permission, and where such use results in damage to the person's reputation. This tort usually involves using another's picture or likeness without their permission for commercial or non-newsworthy purposes.[236] Consequently, this tort would

233. *See* Biby v. Bd. of Regents, 419 F.3d 845, 851–52 (8th Cir. 2005) (dismissing invasion of privacy claims brought by a state university employee against the university after the latter searched the office computer of the former, in light of the university's computer terms of use policy which the court found to negate any reasonable expectation of privacy).

234. RESTATEMENT (SECOND) OF TORTS § 652B (1977).

235. *See* Hamberger v. Eastman, 206 A.2d. 239, 242 (N.H. 1964) (awarding damages for intrusion upon seclusion where a landlord installed a hidden camera in his tenant's room and recorded private conversations).

236. *See* Howard Stern v. Delphi Internet Servs. Corp., 626 N.Y.S. 2d 694 (N.Y. Sup. Ct. 1995). This case involved a plaintiff—the famous radio shock-jock Howard Stern—who ran for Governor of New York as a publicity stunt. *Id.* at 695. As part of his "campaign," Stern posed for a photograph in which he exposed his buttocks. *Id.* Defendant Delphi Internet Services (Delphi), an online news provider, published Stern's picture without his permission on its online news bulletin board with his buttocks exposed. *Id.* Delphi claimed it did so to promote its news-related products. *Id.* at 700. Stern sued for invasion of privacy alleging that since Delphi published the picture without permission, it resulted in a misappropriation of his name and likeness thereby causing him injury. *Id.* at 695. The court disagreed declaring Stern a public figure whose candidacy was newsworthy with no reasonable expectation of privacy existed given the facts. *Id.* at 700. Therefore, the Defendant had a First Amendment right to publish Stern's name and picture in order to advertise or promote its news-related products. *Id; see also* Felsher v. Univ. of Evansville, 755 N.E.2d 589 (Ind. 2001). Felsher, a French professor at the University of Evansville, was fired in 1991 and, six years later, he set up websites and e-mail addresses that included parts of the names of three university officials, as well as the letters "UE." *Id.* at 591. He posted articles in which he alleged that the three were guilty of wrongdoings. *Id.* He then sent e-mails to other universities nominating the three university officials for certain teaching positions. *Id.* He then directed interested universities to visit his websites, where they could read the articles and the allegations that he posted. *Id.* The three officials and the University of Evansville sued Felsher alleging invasion of privacy. *Id.* The Court found Felsher guilty of misappropriation of the official's names and enjoined him from using the three names along with the letters "UE." *Id.* at 600. However, the

have limited relevance in suits against a university for alleged invasions of privacy.

C. Public Disclosure of Private Facts Causing Injury to Reputation

The public disclosure or transmission of highly private or personal information about another that causes damage to reputation can also give rise to liability. "Public" disclosure implies publicizing a private fact to a significant number of individuals rather than to one or a mere few individuals. The facts made public must be offensive and objectionable to a reasonable person and of no concern to the public.[237] Although this tort would not apply to Boston College's role in *Calixte*, it could apply to Bennefield were he to claim that visits to gay websites were an intimate or private activity made public in Calixte's e-mails, thereby deeming the e-mails offensive and highly objectionable to Bennefield and to a reasonable person in the same or similar circumstances.

D. Publicity Placing Another in a False Light

One who gives publicity to a matter concerning another that presents that person to the public in a false light is subject to liability to the other for invasion of his privacy.[238] Liability for this tort requires the publicity to be highly offensive to a reasonable person, and the defendant must have knowledge of, or act in reckless disregard as to, the falsity of the publicized matter and the false light in which the other would be placed.[239] Proof of actual damages is not required.[240] Instead, the focus is on whether the false depiction of the plaintiff by the defendant subjected the plaintiff to ridicule, contempt, or hatred. The requirement of knowledge of or recklessness as to the truth or falsity of the matter publicized would probably eliminate Boston College from any liability for this tort, unless a court were to describe Boston College's investigations of Bennefield's allegations as, "sketchy"[241] and "troublingly weak,"[242] as the Massachusetts Supreme Judicial Court described, and interpret those descriptions as "reckless" behavior resulting in a disregard as to the truth or falsity of the allegations.

injunction did not prohibit future nominations Felsher might send in his own name. *Id.*

237. RESTATEMENT (SECOND) OF TORTS § 652D (1977).

238. *Id.* § 652E.

239. *Id.*

240. *Id.*

241. *In re* Riccardo Calixte, No. SJ-2009-0212, *supra* note 71, at 8.

242. *Id.* at 10.

Nevertheless, few cases involving universities and false light claims have been successful.[243] Accordingly, the relative value of these torts in cases against universities for invasion of privacy rights is limited.

VI. CONCLUSION

Short of making the Ivory Tower into an educational fortress, no combination of precautions and methods exists that would ensure complete campus safety. Beyond video surveillance and monitoring of campus electronic technology usage by students, additional methods that have been suggested for keeping campuses safe include concealed carry provisions, the use of metal detectors, and the implementation of criminal background checks.

A. Concealed Carry

The majority of four-year universities allow their campus police to carry firearms while opposition has been raised at some smaller institutions.[244] Would allowing students and faculty to carry concealed weapons enhance safety or create potentially dangerous situations ending in injury or deaths? Although there are no statistics arguing for or against arming students and faculty, the issue is controversial with arguments both in favor and against. Those in favor argue that it could reduce deaths caused by the acts resembling those at Virginia Tech, while others emphasize the infrequency of such incidents combined with the dangers of placing guns in the hands of students who are drunk or emotionally upset or depressed.[245]

Utah is the only state that allows those twenty-one years of age or older, including students, to carry concealed weapons on campus at all public and private universities.[246] Other state legislatures have proposed statutes that

243. *See* Collins v. Purdue Univ., 703 F. Supp. 2d 862, 880 (N.D. Ind. 2010) (holding that plaintiff failed to state a claim for false-light invasion of privacy where Purdue published accurate statements that a former university student had been charged with an illegal act); Maes v. Folberg, 504 F. Supp. 2d 339, 347 (N.D. Ill. 2007) (finding that state university employee enjoyed a reasonable expectation of privacy in her workplace computer absent a terms of use policy indicating otherwise); Anderson v. Vanderbilt Univ., 2010 U.S. Dist. LEXIS 52381, at *46 (M.D. Tenn. May 27, 2010) (holding that claim for false-light invasion of privacy fails where a notation that a student cheated on an exam was placed on his transcript indicating an honor code violation).

244. Marcella Bombardieri, *Campus Police Renew Call to Carry Arms*, BOSTON GLOBE, Apr. 28, 2007, at A1.

245. Pat Doyle, *More Guns, Safer Campus?,* STARTRIBUNE, Apr. 16, 2008, http://www.startribune.com/politics/state/17833874.html.

246. *See Utah Only State to Allow Guns at Colleges*, MSNBC, Apr. 28, 2007, http://www.msnbc.msn.com/id/18355953/.

would allow students to carry concealed firearms on campus, but none have been successful.[247] Students for Concealed Carry on Campus (SCCC) is a student organization with over sixty chapters in the United States with a membership of over 42,000 students, professors, and parents/guardians of university students.[248] The SCCC strongly advocates allowing students who are trained in the use of guns to carry them on campus.[249] SCCC lists twenty-four states "that expressly prohibit carrying concealed guns on campuses" and fifteen "Right-to-Carry" states "that leave the decision of concealed carry on entirely to each college/university."[250] Of these fifteen universities, Colorado State University in Fort Collins and Blue Ridge Community College in Weyers Cave, Virginia allow concealed carry on campus.[251]

B. Metal Detectors

The use of metal detectors as a deterrent to violence on campus also raises controversial issues concerning their effectiveness.[252] Although commonplace at many urban high schools, their use on university campuses has generally been limited to campus events such as concerts, dances and parties, rather than classrooms, other buildings and dorms.[253] Those favoring metal detectors argue that they are effective in detecting firearms and knives and may discourage carrying weapons at these events, leading to fewer acts of violence.[254] They point to incidents such as that which took place at a Duquesne University student union dance. In that case, the use of

247. THOMAS HARNISCH, AM. ASS'N OF STATE COLLS. & UNIVS. CONCEALED WEAPONS ON STATE COLLEGE CAMPUSES: IN PURSUIT OF INDIVIDUAL LIBERTY AND COLLECTIVE SECURITY 1 (2009), *available at* http://www.aascu.org/media/pm/pdf/pmdec08.pdf. ("[L]awmakers in 17 states have introduced measures seeking to relax concealed weapons restrictions on college and university campuses."); Derek P. Langhauser, *Gun Regulation on Campus: Understanding* Heller *and Preparing for Subsequent Litigation and Legislation*, 36 J.C. & U.L. 63, 83 (2009) ("[T]wenty states in 2009 considered various reforms to campus weapon laws . . . ."); *see also* Janet Elliot, *Texas Senate OKs Guns on College Campuses Bill Today*, HOUS. CHRON.. May 20, 2009, *available at* http://www.chron.com/disp/story.mpl/metropolitan/6432279.html.

248. About Students for Concealed Carry On Campus (SCCC), http://www.concealedcampus.org/aboutus.php (last visited Mar. 14, 2011).

249. *Id.*

250. State-by-State, SCCC, http://www.concealedcampus.org/ (last visited Mar. 14, 2011).

251. *Id.*

252. Bill Schackner, *Colleges Disagree on Use of Metal Detectors*, PITT. POST-GAZETTE, Sept. 20, 2006, *available at* http://post-gazette.com/pg/06263/723346-298.stm.

253. *See* Mass. Inst. of Tech. Event Regulations – Metal Detectors, http://web.mit.edu/eventguide/eventregulations/metaldetectors.html (last visited Mar. 14, 2011).

254. *See* Alfonso Jimenez, *Metal Detection Worth Its Mettle*, CAMPUS SAFETY, Nov. 1, 2006, *available at* www.campussafetymagazine.com/Articles/Default.aspx?ArticleID=64.

metal detectors may have prevented a gunman, who was in attendance at the dance, from shooting and wounding five Duquesne University basketball players following an argument that began at the dance.[255] Those opposing of the use of metal detectors respond that metal detectors are not foolproof, especially on university campuses where most buildings have numerous entrances and exits. The use of security professionals properly trained in the use of metal detectors is also imperative. Professionals should be able to distinguish between a gun or knife and other heavy metal objects such as a belt buckle. Metal detectors also raise issues of constitutionality and privacy.

C. Criminal Background Checks

Many universities informally ask incoming students questions on their admission applications, including "The Common Application,"[256] regarding whether they have been subject to prior disciplinary actions or criminal convictions (other than traffic violations), and whether they are on probation or suspension from another university.[257] Some universities conduct a formal and extensive criminal background check as a condition for acceptance and enrollment of incoming students, new faculty and administration, and new hires.[258] Many universities offering degrees and

255. Jim Ritchie, *Five University of Duquesne Basketball Players Shot*, PITT. TRIB. REV., Sept. 17, 2006, *available at* http://www.pittsburghlive.com/x/pittsburghtrib/news/mostread/s_470982.html.

256. *See* Allen Grove, The Common Application, About.com, http://collegeapps.about.com/od/glossaryofkeyterms/g/CommonApp.htm (last visited Mar. 14, 2011).

> The Common Application is used for undergraduate admissions by roughly 350 colleges and universities. Only schools that evaluate applications holistically are allowed to use the common application; that is, the admissions staff must take into consideration things like letters of recommendation and the application essay. If a college bases admission solely on GPA and test scores, they can not be members of the Common Application. The Common Application covers several areas: personal data, educational data, standardized test information, family information, academic honors, extracurricular activities, work experience, a short answer essay, a personal essay, and criminal history.

Id.

257. Mary Beth Marklein, *Should College Applicants Get Background Checks?*, USA TODAY, Apr. 4, 2007, *available at* http://www.usatoday.com/news/nation/2007-04-17-blcover_N.htm.

258. *See, e.g.*, Yale Univ. Staffing & Career Development – Background Checks, http://www.yale.edu/hronline/careers/screening/index.html (last visited Mar. 14, 2011).

> [A]ll offers of employment extended to external candidates have been contingent upon successful completion of a background check. This includes candidates for management and professional (M&P) positions, clerical and technical (C&T) positions and service and maintenance (S&M) positions. Beginning January 1, 2010 the background verification process was expanded to include postdoctoral/postgraduate fellows and associates, casual employees, and temporary employees.

Id.; UCLA Human Resources, Procedure 21: Appointment, http://map.ais.ucla.edu/go/1001618 (last visited Mar. 15, 2011) ("All critical positions are subject to a criminal background check.").

programs related to law enforcement, medicine and health also require criminal background checks for incoming students, including the Virginia Tech Carilion School of Medicine and Research Institute,[259] even though Virginia Tech does not support criminal background checks for other undergraduate applicants.[260] A few objections against such background checks include privacy concerns, negligence in checking, flawed or incorrect data and discrimination in the form of profiling those with negative background checks.[261] Perhaps if criminal background checks had been in place at Virginia Tech and the University of Alabama they would have raised warnings about Seung-Hui Cho and Amy Bishop, respectively. As a result of these incidents, more universities are considering criminal background checks for all incoming students.[262]

Other suggestions for protecting the Ivory Tower include but are not limited to:

- Engaging medical and mental health professionals with expertise in identifying and monitoring "at risk" students as well as training of faculty and staff in the danger signs manifested by such students;
- Creating and implementing emergency notification systems and response programs using a variety of methods to alert the campus, including messages via e-mail, cell phone, text, and other devices;
- Displaying warnings or notifications on campus media such as strategically placed large screen plasma televisions;
- Providing surveillance and monitoring of entrances to dorms;
- Impressing upon students the need to lock their rooms and windows;
- Utilizing campus police patrols;
- Creating student escort services to accompany students to seeking to return to dorms or other buildings;
- Providing safety seminars and training sessions to students;
- Cultivating mutually beneficial relationships with local and state police, other emergency agencies, and neighboring universities.

259. *See* Va. Tech. Carilion Sch. of Med. & Res. Inst., Criminal Background Check and Drug Screening, http://www.vtc.vt.edu/education/admissions/background_check_drug_screening.html (last visited Mar. 15, 2011) [hereinafter Va. Tech. Carilion Background Checks].

260. Sarah Watson, *Tech Will Not Support Background Checks on Prospective Students*, COLLEGIATE TIMES, May 26, 2010, *available at* http://www.collegiatetimes.com/stories/15505/tech-will-not-push-for-background-checks-on-prospective-students.

261. *Id.*

262. *See* Va. Tech. Carilion Background Checks, *supra* note 259.

As additional security precautions are implemented, the campus community should also be apprised of its privacy rights. To this end, universities should ensure that policies regarding issues of computer usage, monitoring and privacy are disseminated to all members of the campus community. In addition, universities should obtain consent before conducting criminal background checks and adhere to all pertinent laws such as FERPA, the Clery Act, and other privacy laws.

No security measure or combination of measures can serve as a panacea for preventing acts of campus violence, which can occur irrespective of the most intensive prevention efforts. Furthermore, although security should be appropriate to the level of risk, universities must at the same time strive to preserve and cultivate the sense of "community." The efforts employed by universities directed at providing campus safety and protection should be viewed as prescriptions for prevention of the Virginia Tech-type atrocity. Despite challenges, universities that are vigilant and persistent in their efforts can simultaneously respect individual privacy while ensuring a safe educational environment.