UNC SCHOOL OF LAW

NORTH CAROLINA LAW REVIEW

Volume 81 | Number 3 Article 12

3-1-2003

FERPA in the Age of Computer Logging: School Discretion at the Cost of Student Privacy

Jennifer C. Wasson

FERPA in the Age of Computer Logging: School Discretion at the Cost of Student Privacy?

> All of us involved in providing and supporting information resources on our campuses must constantly remind ourselves of the ultimate objective of what we are doing, namely, facilitating the scholarship of students and faculty. Except in a very few disciplines, technology is not an end in and of itself—it is the means to achieve some other scholarly aim. Technology, however, has an allure and a seductiveness that occasionally catches all of us, and we forget the original goal as we become captivated with the process.[1]

Technology is a part of life for students at virtually every American university. Students log onto a campus computer network to use e-mail, check grades, post papers for classes, surf the Web, and conduct other academic and non-academic affairs. Pajama-clad in their dorms or tucked into a corner of a computer lab, many students using the network may assume their information is protected from the invasion or abuse[2] occurring on college campuses more frequently than ever.[3] Similarly, many undergraduates rely on the technology behind their student identification cards to perform many campus activities with little awareness of the data collected from their card

---

1. BRIAN L. HAWKINS, ORGANIZING AND MANAGING INFORMATION RESOURCES ON CAMPUS 11 (1989).

2. *See* Tyler Boersen, *"U." Seeks to Protect Students' Online Privacy*, MICH. DAILY, Mar. 7, 2002, http://www.michigandaily.com/vnews/display.v/ART/2002/03/07/3cb2fb609df77 (on file with the North Carolina Law Review) ("Most students are under the assumption that (this information) [sic] can only be accessed by themselves. They operate under the assumption of *privacy*, but it is not always the truth.").

3. *See* United States v. Machado, 195 F.3d 454, 455 (9th Cir. 1999) (affirming the conviction of a University of California student who used the university network to send e-mails threatening to kill fifty-nine Asian students); Virginia Rezmierski & Aline Soules, *Security vs. Anonymity: The Debate over User Authentication and Information Access*, EDUCAUSE REV. 22, 26 (Mar.–Apr. 2000) (illustrating the types of tampering that can result from unauthorized and unmonitored computer usage); Paul T. Rhinehart, *The Use of Electronic Data Interchange Under the Family Educational Rights and Privacy Act*, CAUSE/EFFECT, Spring 1996, at 34, 37 (describing the vulnerability of computer systems against deliberate tampering); Beth Kormanik, *Internet Poses New Worry for Colleges: More Use Can Mean More Illegal Use*, FLA. TIMES-UNION, Nov. 6, 2002, at B1, http://www.jacksonville.com/tv-online/stories/110602/met_10891343 (on file with the North Carolina Law Review) (focusing specifically on intellectual property theft by university students).

use.[4] At colleges and universities across the country, students may not realize the extent to which information regarding their computer use, daily activities, and whereabouts may be appropriated without their knowledge or consent.[5] Four scenarios[6] provide telling examples:

> I. *The Curious Dean.* The dean of a small university receives a complaint about a student, so he contacts the systems administrator[7] of the university network and asks

---

4. *See infra* notes 11–15 and accompanying text.

5. *See* Arthur Miller, *Computers, Data Banks and Individual Privacy: An Overview*, 4 COLUM. HUM. RTS. L. REV. 1, 10 (1972) (noting that even at an early time in technological history "the centralized quality and compactness of a computerized dossier create [sic] an incentive to invade it because the payoff for doing so successfully is [large]"). Despite the threat of invasion, students often are uninformed about the privacy of their computer information. *See* Katherine Kelman, *Stanford Students Raise Privacy Awareness*, STANFORD DAILY, Nov. 28, 2001, http://daily. stanford.edu/tempo?page=content&id=6929&repository=001_article# (on file with the North Carolina Law Review) (citing a pilot study of 120 Stanford students in which most knew "very little" about privacy rights on Stanford's campus); Kelli Shillito, *Release of Student Records Creates Privacy Concerns*, OSU DAILY BAROMETER, via University Wire, June 6, 2002, LexisNexis Academic Universe (stating that students may not know exactly who has access to their records); *see, e.g.*, ACLU Freedom Network, *Ask Sybil Liberty About Your Right to Keep Your School Records Private*, *at* http://archive.aclu.org/students/slrecord.html (last visited Feb. 21, 2003) (on file with the North Carolina Law Review) (informing students about their right to educational privacy, but never mentioning logging or technology awareness issues). Students also may have little knowledge about information collected from campus identification cards. *See* University of Michigan, *Standard Practice Guide for Identification and Access Control Cards*, *at* http://spg.umich.edu/pdf/601.13.pdf (revised Oct. 1, 2001) (on file with the North Carolina Law Review) (describing student cardholders' responsibilities but never indicating who may access information generated from cards or how identification card information is used and stored); C. Barry Weiser, *Who's Wandering the Hallowed Halls?*, SECURITY MGMT., Aug. 1, 1999, at 57, 1999 WL 14496633 (discussing Princeton students' outrage upon learning that the university's new card access system included tracking features). Administrators "seriously underestimated the negative reaction the students would have" when the system's tracking function was revealed to them. *Id.*

6. These scenarios are loosely based on fact patterns from the Logging and Monitoring Privacy ("LAMP") Project. *See* FINAL REPORT: NSF LAMP PROJECT, IDENTIFYING WHERE TECHNOLOGICAL LOGGING AND MONITORING FOR INCREASED SECURITY END AND VIOLATIONS OF PERSONAL PRIVACY AND STUDENT RECORDS BEGIN: A REPORT TO THE DIGITAL GOVERNMENT PROGRAM OF THE NATIONAL SCIENCE FOUNDATION 2001, at 5.1, 5.1–5.6 [hereinafter LAMP PROJECT]. This project sought to determine more information about logging activity and policy on college campuses. *Id.* at iii.

7. This Recent Development will use the term "systems administrator" to describe school personnel who manage the university computer network and have access to the student information it contains. In reality, these officials' titles may range from "computing manager" to "information technology officer" and beyond, and their educational backgrounds may range from high school to doctorate levels. *See id.* at 3.1.

her to track the student's user ID,[8] discovering which Web sites the student visits,[9] how long the student is on the network, and when and to whom the student sends e-mail.[10] The systems administrator easily collects this information and transfers it to the dean for his perusal.

II. *ID Card Tracking.* University students often are assigned identification cards ("student IDs" or "ID cards") upon enrollment.[11] Students use these cards to enter dorms and campus buildings, eat meals, park in campus lots, use vending machines and laundry facilities, and make purchases at the campus bookstore, student store, and local eateries.[12]

---

8. According to a National Science Foundation report, forty-two percent of systems administrators surveyed logged information about specific individuals without the individuals' knowledge or permission. *Id.* at 6.2.

9. For example, this type of Web site monitoring occurs at the University of Michigan, which collects data on Web site visits to determine computer usage rates. *See* Boersen, *supra* note 2.

10. When surveyed, four of eight current and former employees of the University of Nebraska at Omaha's computer services department acknowledged they had been asked to read student e-mail and report the results to administrators or that administrators had intercepted student e-mail directly. Two others had not witnessed this but had secondhand knowledge that it was occurring. Katherine Stoltzfus, *Someone May Be Reading Your Email*, UNO GATEWAY, Mar. 29, 1994, *at* http://www.eff.org/CAF/news/apr_03_1994 (on file with the North Carolina Law Review). School officials also may misappropriate confidential student information for other purposes. For example, Yale recently accused Princeton of using the names, birthdates, and Social Security numbers of its applicants to hack into Yale's confidential online admissions Web site. Pamela Ferdinand & Michael Barbaro, *Yale Tells FBI of Rival's Breach of Web Site: Princeton Suspends Admissions Official over Snooping into Student Files*, WASH. POST, July 26, 2002, at A2. Florida A&M also misappropriated student data by disclosing personal student information to its employees. *See* Melanie Yeager, *Audit of Florida A&M University Uncovers Several Flaws*, TALLAHASSEE DEMOCRAT, June 4, 2002, at B1 (reporting that a state audit of the Florida A&M Financial Aid Office revealed that student names, Social Security numbers, and bank account numbers were used without permission as examples in the university's procedural manuals).

11. Approximately 1,300 of the 3,500 four-year colleges and universities in America have implemented a multi-use identification card system. Richard R. Holley III, *One-Card 101: Wachovia Hits the Pit and Becomes the Partner of the UNC One-Card*, 4 N.C. BANKING INST. 371, 371 (2000). Industry journal *Security* estimates that there are currently fifteen to twenty million magnetic stripe cards in use. Deborah L. O'Mara, *Full Steam Ahead for Multi-Function Cards*, SECURITY, July 1, 2000, at 55, 2000 WL 14261690.

12. *See* Shang-Lin Chuang, *Card Keys Sometimes a Problem*, THE [M.I.T.] TECH, Nov. 18, 1994, *at* http://the-tech.mit.edu/V114/N57/keys.57n.html (on file with the North Carolina Law Review) (detailing the use of the ID card at M.I.T. for dormitory entry; meal plan, student store, and vending machine purchases; parking; and laundry services); *see also* CORNELL UNIVERSITY OFFICE OF THE UNIVERSITY REGISTRAR, CORNELL IDENTIFICATION CARD POLICY STATEMENT, Aug. 2002, *at* http://www.sas.cornell.edu/OUR/Grades/PDF/Cornell_ID_Policy.pdf (detailing use of identification card for access to dorms, libraries, dining halls, parking, fitness centers, and athletic events) (on file with the North Carolina Law Review); Diebold, Card Systems Products, http://www.diebold.com/opccsol/Products/CSProducts.htm (last visited Feb. 21, 2003) (on file with the North

Because the ID cards, when used, send information to a central database,[13] university officials can determine when students enter dorms and other buildings, enter or exit a campus parking lot, eat meals, and purchase items with their cards.[14] The director of a campus office notices that a student employee has not come to work that morning. Seeking to discover the student's whereabouts, the director uses payroll records to obtain the student's identification number, then calls the systems administrator to request the student's ID card information for the past three hours.[15]

Carolina Law Review) (advertising Diebold's campus card system, which allows students to "positive[ly identify themselves], pay fees, purchase books and meals, access buildings and events, withdraw money and much more"). In the future, these cards also may be used to access computer networks in place of passwords. *See* O'Mara, *supra* note 11.

13. Chuang, *supra* note 12 (noting that a central computer periodically communicates with M.I.T. card-key readers to facilitate dorm entry); *see also On Campus, Student Cards Do It All*, SECURITY, Jan. 1, 1994, at 13, 1994 WL 14083480 (noting that Texas A&M upgraded to a centralized computer system with a multi-use identification card program); Lisa Otteson & Mark Fallowes, *Graduating to Higher Security*, SECURITY MGMT., Apr. 1, 1998, 1998 WL 10740297 (explaining in detail the operation of the centrally-controlled card access system at Wake Forest University); Diebold, *supra* note 12 (advertising its identification card system as offering an "integrated total solution").

14. *See* Diebold, CS Housing, http://www.diebold.com/opccsol/roducts/cshousing/cshousing.htm (last visited Feb. 23, 2003) (on file with the North Carolina Law Review) (advertising Diebold's CS Housing Card System, which integrates with other campus applications and permits "real-time updates" on card use, "streamlines data capture for persons in dozens of categories, including demographic, special needs, preferences, and interests," and has "unlimited and multiple adjacent room fields incorporated for roommate and suitemate determination"); *see also* Otteson & Fallowes, *supra* note 13 (noting that a systems administrator can determine when a student's card is used and can retrieve and view a student's photograph anytime the card is activated); Robbin M. Rittner-Heir, *The Revolution in I.D. Cards*, SCHOOL PLAN. & MGMT., http://www.peterli.com/plegarchive/spm/227.htm (last visited Feb. 21, 2003) (on file with the North Carolina Law Review) (noting that even ID card systems used in middle schools can generate reports on the location of card use, the time of use, and the identity of the card user). Wake Forest University also has considered installing a camera surveillance system to complement its card system. Otteson & Fallowes, *supra* note 13. The University of North Carolina at Chapel Hill allows students to track their card purchases through a secure Web site. The transaction history the University receives shows each transaction date, time, and location, as well as the amount of each purchase and the current balance. *See, e.g.*, Transaction History for Aug. 25, 2002–Nov. 13, 2002 for Jennifer Wasson, *at* https://www-s3.ais.unc.edu/OneCard/TransView.jsp. (on file with the North Carolina Law Review).

15. System use for non-emergency reasons may not be so uncommon. For example, the director of the Computing and Data Communications Department at the University of Nebraska at Omaha violated federal law by obtaining a student employee's grades without authorization and then sharing them with other department members, apparently out of concern that this student was working too much. Stoltzfus, *supra* note 10; *see* Ann Longmore-Etheridge, *Keyless but Not Clueless*, SECURITY MGMT., July 1, 2001, 2001 WL 23143408 (discussing Mount Holyoke College's use of identification card logs to track a student for "an urgent phone call"); O'Mara, *supra* note 11 (noting that in high schools

III. *Hacking Alert.* A systems administrator has observed an increase in hacking over the past few months. Suspecting a few computer science students who previously have boasted about their hacking skills, he secretly monitors[16] their personal computers periodically to check for abusive behavior.[17]

IV. *Print Use Records.* A student working at the computer lab information desk has access to printing records. These records display the names or user identifications of students sending print jobs to the university printers, the number of sheets printed, and the specific machine from which the jobs were ordered. The printing records are used to cut school overhead costs, and bills for individual print jobs exceeding a specified limit are sent to the students.[18]

These scenarios are all examples of "logging," the process by which a systems administrator collects data about a computer network and the individuals using it.[19] All of the above scenarios,

---

with card systems, administrators can stop a student in the hall, ask where he or she is going, then return to the office and verify the student's whereabouts using the card records).

16. *See infra* note 19.

17. This type of troubleshooting is often a main task of systems administrators. LAMP PROJECT, *supra* note 6, at 6.2. *See generally* Kormanik, *supra* note 3 (interviewing a computer systems control specialist at Florida State University about monitoring to prevent computer misconduct on campus); Stoltzfus, *supra* note 10 (quoting a posting from Bradley University Systems Administrator Jeff Hibbard discussing the discovery and punishment of hacking and chain letter violations).

18. The College of William and Mary has a print system that operates in this manner. Undergraduate students are allowed 400 free pages from the university printer, then are charged $.05 per page for print jobs exceeding this limit. *See* E-mail from Tech Support Services, The College of William and Mary, to Jennifer Wasson (Oct. 7, 2002, 16:38:49 EDT) (on file with the North Carolina Law Review).

19. LAMP PROJECT, *supra* note 6, at 1.2. University networks may be configured to record students' user identifications, Internet addresses, and other personal information once students log on. *See* Dan Carnevale, *Network Practices Can Endanger Students' Privacy, Report Warns*, CHRON. HIGHER EDUC., Nov. 23, 2001, at A30. Logging can be performed in a variety of ways: by tracking the student's user ID number or name (which can identify all of the computing transactions associated with that user), date and time stamps (used to determine a user's location, length of time on the network, and changes made to programs or applications), IP address (which is the name given to a specific computer and used to trace transactions back to it), or domain name (which is the name given to that section of the network of which a specific computer is a part). LAMP PROJECT, *supra* note 6, at 4.3–4.4. Systems administrators may log this information by relying on a default function in the system that automatically collects the desired information or by writing "scripts," instructions that customize searches for specific data, individuals, or machines. *Id.* at 4.2–4.3. According to a 2001 survey of university systems administrators in post-secondary schools of varying size, ninety-six percent of systems administrators responding logged computer data, and more than half of the respondents wanted to increase current levels of logging. *Id.* at 4.3. This attitude is likely a result of

however, raise significant concerns about the use of technology to monitor private life.[20]

To what extent do students have a privacy interest in the logged records of their activities? The Family Educational Rights and Privacy Act,[21] or "FERPA," is the principal law on student privacy.[22] FERPA governs the use and dissemination of student information.[23] To protect the private nature of education records, FERPA prohibits federal funding for any institution with a policy or practice[24] of denying students access to their education records[25] or disclosing

---

the primary purpose that systems administrators serve—to ensure the network is accessible and safe for all users. *See id.* at 6.2 (noting that systems administrators primarily log for network maintenance, security, and operations reasons); *see also supra* note 17 (discussing computer monitoring to prevent misconduct).

20. "The freedom of the individual to pick and choose for himself the time and circumstances under which, and most importantly, the extent to which, his attitudes, beliefs, behavior, and opinions are to be shared or withheld from others" is part of the essence of individual privacy. Charles R. Tremper & Mark A. Small, *Privacy Regulation of Computer-Assisted Testing and Instruction*, 63 WASH. L. REV. 841, 846 (1988) (quoting Oscar Ruebhausen & Orville Brim, *Privacy and Behavioral Research*, 65 COLUM. L. REV. 1184, 1189 (1965)). Because college students may be especially sensitive about personal information such as their ethnic backgrounds, bodies, or economic statuses, "[p]roviding an environment where ... information about themselves can be controlled eases one of the many pressures of campus life." CAUSE TASK FORCE, PRIVACY AND THE HANDLING OF STUDENT INFORMATION IN THE ELECTRONIC NETWORKED ENVIRONMENTS OF COLLEGES AND UNIVERSITIES 4 (1997).

21. Education Amendments of 1974, Pub. L. No. 93-380, § 513, 88 Stat. 484, 571–74 (1974) (codified as amended at 20 U.S.C. § 1232g (2000)).

22. *See* American Association of Collegiate Registrars and Admissions Officers, SPECIAL REPORT: EDUCATION RECORDS AND PRIVACY RIGHTS: A NEW BATTLEGROUND FOR THE INFORMATION REVOLUTION?, Apr. 2002, at 1 (noting that FERPA is the primary law in regard to student records).

The Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2522 (2000), was enacted to protect e-mail communication from government surveillance. The effect of this law on student e-mails sent through the university network is not clear, as students may waive their right to protection from data interception merely by signing onto the network. *See infra* note 48. State laws also may provide limited protection to student privacy. *See infra* note 36. For an overview of other laws pertaining to specific student records, see generally Lynn M. Daggett, *Bucking up* Buckley I, *Making the Federal Student Records Statute Work*, 46 CATH. U. L. REV. 617 (1997).

23. *See* 20 U.S.C. § 1232g (2000).

24. In its most recent FERPA case, the Supreme Court emphasized that FERPA provisions have "an aggregate focus," pointing to the "policy and practice" language in the statute. Gonzaga Univ. v. John Doe, 122 S. Ct. 2268, 2278 (2002). However, a university may violate FERPA each time it releases education records absent an explicit statutory exception or student consent in writing. *See, e.g.*, Letter of Finding to Henry County (KY) Public Schools Regarding Disclosure to Media, FERPA Online Library, Mar. 10, 1999, *at* http://www.ed.gov/offices/OM/fpco/docs/henry_co_ky.html (on file with the North Carolina Law Review) (finding that a school district violated FERPA when it released a student's disability records to a newspaper).

25. § 1232g(a)(1)(A)–(B).

student information without authorization.[26] FERPA is administered by the Family Policy Compliance Office ("FPCO"), which hears complaints, answers schools' questions, and enforces the statute through advisory letters.[27] Unfortunately, however, neither the statute nor FPCO has addressed the technology issues presented in the scenarios above.[28]

Enacted in 1974, FERPA was created when "the model for academic recordkeeping was very much a paper model."[29] Thus, the statute is no longer adequate to guide schools through the complicated educational privacy issues of the new century.[30] This Recent Development argues that to preserve student privacy in an increasingly "wired" environment, Congress should amend FERPA to encompass technology issues such as logging.[31] Until Congress acts to update this outdated statute, however, FPCO can and should entitle student logging information to a high degree of protection by legitimately defining computer logs as "education records" under the existing statutory scheme.[32] FPCO should further apply a primary purpose analysis to delineate proper and improper uses of such information.[33] In this way, schools can effectively manage the benefits of technology without compromising student privacy.

---

26. *Id.* § 1232g(a)(1)(A).

27. *Id.* § 1232g(g) (enabling the Secretary of Education to create a compliance and review office). The Family Policy Compliance Office ("FPCO") is the complaint-hearing and enforcement arm of FERPA. Family Educational Rights and Privacy, 34 C.F.R. §§ 99.63–99.67 (2002) (describing guidelines for FERPA's application). For more information about FPCO, see its Web site at http://www.ed.gov/offices/OM/fpco/ (last visited Feb. 21, 2003) (on file with the North Carolina Law Review); *see also infra* note 36 (discussing FPCO's investigation process for FERPA complaints).

28. *See generally* § 1232g (making no mention of computer records such as logs); Family Educational Rights and Privacy, 34 C.F.R. § 99 (2002) (providing guidelines on the application and purpose of FERPA, some relevant definitions, the rights of parents and students, notification regulations, and law enforcement provisions).

29. Carnevale, *supra* note 19.

30. Marcia Coyle, *Court Faces First School Records Case: Privacy Case Could Have Wide Impact*, NAT'L L.J., Nov. 19–26, 2001, at A1 (quoting Julie Lewis, staff attorney to the National School Boards Association, as stating that "[FERPA] seems a straightforward statute, but it has become cumbersome with implementation, particularly with the evolution of technology"); *see infra* notes 48–74 and accompanying text.

31. "[FERPA] needs an electronic overhaul to bring it into compliance with modern electronic systems." Robert F. Curran, *Student Privacy in the Electronic Era: Legal Perspectives*, CAUSE/EFFECT, Winter 1989, at 14, 18; *see* William Hillison et al., *Confidentiality of Student Records in the Electronic Frontier: Professors' and Administrators' Obligations*, 18 J. ACCT. EDUC. 301, 309 (2000) (discussing FERPA's inadequacy in regard to records' security).

32. *See infra* notes 82–100 and accompanying text.

33. *See infra* notes 116–33 and accompanying text.

FERPA governs students' access to their records[34] as well as the release of those records to third parties.[35] The Act is Spending Clause legislation that conditions schools' federal funding on compliance with its provisions.[36] Section (b)(1) states: "No funds shall be made

34. *See* 20 U.S.C. § 1232g(a)(1)(A)–(B) (2000) (prohibiting federal funding for education institutions that deny students the right to review their records).

35. *See id.* § 1232g(b) (prohibiting education institutions from disclosing education records without first obtaining the student's written consent, subject to several exceptions).

36. *See id.* § 1232g (denying federal funding to schools that fail to comply with FERPA). FERPA violations may be enforced by written complaints to FPCO, which investigates the complaints and, if appropriate, issues notices outlining measures the institution must take to comply with FERPA. Family Educational Rights and Privacy, 34 C.F.R. § 99.64–99.66 (2002). If the institution does not comply, the Secretary of Education may then refuse to grant federal funding or may terminate existing funding. *Id.* § 99.66–99.67. There are multiple problems with this enforcement scheme. First, the injured student is given no direct relief; the school is merely ordered to comply after the violation has taken place. *See, e.g.*, Letter to Dr. John R. Leitzel, President, University of New Hampshire, from LeRoy S. Rooker, Family Policy Compliance Office (Jan. 31, 2001) *at* http://www.ed.gov/offices/OM/fpco/ferpa/library/unh.html (on file with the North Carolina Law Review) (finding a FERPA violation for releasing student education records to a prior employee and merely asking the school to notify its officials of FERPA policies as the remedy). Second, the loss of funding for egregious violations does not solve the problem adequately; instead, an elimination of funds harms students by reducing their educational opportunities. For a judicial exposition of this view, see *United States v. Miami Univ.*, 91 F. Supp. 2d 1132, 1140 (S.D. Ohio 2000). Moreover, commentators believe that no school actually has been punished with termination of funding because it is such a drastic remedy. *See* Dixie Snow Huefner & Lynn M. Daggett, *FERPA Update: Balancing Access to and Privacy of Student Records*, 152 W. EDUC. L. REP. 469, 475 (2001); Virginia de Leon, *Student Privacy Extensive; Even Parents Can Be Kept from Information*, SPOKANE SPOKESMAN-REVIEW, Dec. 9, 2001, at A1. Thus, a student who is injured in a situation like the Curious Dean scenario or the Keycard Tracking scenario has little remedy under FERPA. The student's complaint and a subsequent letter from FPCO are, in reality, the statute's remedy for university privacy violations. Further, the student may not have a Fourth Amendment claim because of his or her explicit consent to the collection (the search and seizure) of this information. *See infra* note 48. State privacy laws, however, may provide another avenue of relief to students. *See, e.g.*, ARIZ. REV. STAT. ANN. § 15-141 (West Supp. 2002) (allowing a state law action in addition to a federal action); CAL. EDUC. CODE § 49070 (West Supp. 2002) (allowing a state law action in addition to a federal action); ME. REV. STAT. ANN. tit. 20-A, § 6001 (West Supp. 2002) (reaffirming that federal law governs privacy of student records but setting up a commission to investigate complaints); OHIO REV. CODE ANN. § 149.41 (Anderson 2001) (allowing a state law action in addition to a federal action). Students also may petition the court to enjoin schools from further disseminating their records. *See, e.g.*, United States v. Miami Univ., 294 F.3d 797 (6th Cir. 2001) (issuing a permanent injunction to keep a newspaper from accessing student disciplinary records); Krebs v. Rutgers, 797 F. Supp. 1246, 1259 (D.N.J. 1992) (enjoining disclosure of students' Social Security numbers to campus post office personnel). Previously, FERPA violations also could be remedied through private causes of action against schools under 42 U.S.C. § 1983 (2000). However, the Supreme Court recently precluded a private cause of action to enforce FERPA's provisions. *See* Gonzaga Univ. v. Doe, 122 S. Ct. 2268, 2279 (2002) (holding that FERPA

available . . . to any educational agency or institution[37] which has a policy or practice of permitting the release of education records (or personally identifiable information contained therein other than directory information . . .) of students without [their][38] written consent . . . ."[39] Before seeking student consent, the school must notify the student of "records to be released, the reasons for such release, and to whom" the records will be given.[40] The school also must provide students with a copy of the requested records if desired.[41] Under FERPA, schools must document requests for an individual student's records and maintain a list of these requests in the student's file.[42] This list must specify the legitimate interest that each requester has in obtaining the information and must be accessible to the student upon demand.[43]

To be entitled to these safeguards, student information must be classified as "education records." The statute defines "education records" as "those records, files, documents, and other materials which contain information directly related to a student; and are

---

does not create individual rights that may be enforced through § 1983). The lack of a private suit leaves injured students without redress.

37. FERPA defines "educational agency or institution" as "any public or private agency or institution which is the recipient of funds under any applicable program." 20 U.S.C. § 1232g(D)(3). Thus, a private university still may be subject to FERPA if it receives any federal assistance.

38. Students eighteen years of age or older or in attendance at a post-secondary institution are accorded all rights of disclosure, inspection, and consent afforded to parents of minor children under the statute. *Id.* § 1232g(d).

39. *Id.* § 1232g(b)(1).

40. *Id.* § 1232g(b)(2)(A). The statute excepts persons issuing subpoenas, the Comptroller General, the Secretary of Education, and state auditors from the notification requirement. *Id.* § 1232g(b)(2)(B)–(b)(3).

41. *Id.* § 1232g(b)(2)(a). Education records may be excepted from the consent requirement if the person requesting them meets one of twelve exemptions: (1) school officials with "legitimate educational interests," *see infra* notes 102–07; (2) officials of other school systems when the student transfers; (3) representatives of the Comptroller General, the Secretary of Education, federal auditors, and the Attorney General; (4) officials in connection with a student's application or receipt of financial aid; (5) state or local officials given access under a state statute if the disclosure concerns the juvenile justice system and the nondisclosure to third parties is certified in writing; (6) organizations conducting studies for the purpose of developing predictive tests or improving education; (7) accrediting organizations; (8) appropriate persons in connection with an emergency to protect the health or safety of the student or others; (9) officials in connection with a subpoena; (10) and the student's parents. *See* § 1232g(b)(1)(A)–(J).

42. § 1232g(b)(4)(A).

43. *Id.* The school also must take steps to ensure that the requester will not disclose a student's education records to third parties. *Id.* § 1232g(b)(4)(B) (conditioning a third party's access to student records on a promise not to disclose the records to others and prohibiting schools from releasing any other education records for five years to a requester who violates this promise).

maintained by an educational agency or institution or by a person acting for such agency or institution."[44] Excluded from this broad definition are teacher's notes for class preparation, law enforcement records, employee records, psychiatric treatment records for students over age eighteen, and alumni records.[45] FERPA also excludes "directory information," which it defines as the student's name, "address, telephone listing, date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, and the most recent previous educational agency or institution attended by the student."[46] In contrast to the protections afforded education records, directory information may be disclosed after the school gives public notice of its intent to disclose and allows students a reasonable time to request withholding of their individual directory information.[47] Thus, if student information is covered under FERPA, it is either classified as "directory information" and given little protection from disclosure, or as "education records" and given much greater protection.

Under this scheme, the question then becomes whether the school personnel in the Curious Dean, ID Card Tracking, Hacking Alert, or Print Use Records scenarios above invaded educational privacy under FERPA.[48] The answer is unclear.[49] Because FERPA leaves much to individual schools' discretion, systems administrators

---

44. *Id.* § 1232g(a)(4)(A)(i)–(ii).

45. *See id.* § 1232g(a)(4)(B)(i)–(vi). Recently the Supreme Court also has excluded peer grading practices from the definition of "education records," finding that the graded sheet is not "maintained" by the student grader and thus does not conform to the statute's two prong definition. *See* Owasso Indep. Sch. Dist. No. I-011 v. Falvo, 534 U.S. 426, 436 (2002).

46. § 1232g(a)(5)(A). This list is not exhaustive, but illustrative.

47. *Id.* § 1232g(a)(5)(B).

48. In situations pertaining to computer logging, students may waive their rights to the collection of personal information every time they log onto a network computer or use their identification cards. *See, e.g.*, ATN Onyen Policy, The University of North Carolina at Chapel Hill, *at* http://www.unc.edu/policy/onyenpol.html (last visited Feb. 21, 2003) (on file with the North Carolina Law Review) (warning that students' activity on the network may be traced back to them); DePaul University, Student Computer Lab Policies, *at* http://service.depaul.edu/labs/new/policies.htm (last visited Feb. 21, 2003) (on file with the North Carolina Law Review) (noting that the university reserves the right to review user files on campus computers). Consent to collection is not equivalent to consent to improper use and dissemination, however. *See infra* notes 65–69 and accompanying text.

49. Huefner & Daggett, *supra* note 36, at 479 (questioning whether school e-mail systems constituted FERPA records); *see infra* notes 50–63 and accompanying text (detailing the confusion school personnel face when dealing with education privacy issues).

and registrars often may not consult the statute[50] or may be confused as to what is appropriate under FERPA in regard to computer logging.[51] In fact, when given scenarios substantially similar to those detailed above, systems administrators, university registrars, and even FPCO experts differed when asked whether these types of situations violated FERPA or even qualified for coverage under the statute.[52] On a few occasions, because the statute allows these tough questions to be determined by school officials,[53] experts from FPCO could not decide what the appropriate policy should be.[54]

Lacking policy from FPCO or Congress, school officials have little statutory guidance on computer logging. FERPA contains no statement of purpose, has little legislative history to guide administrators,[55] and has never been amended to address technology issues.[56] Consequently, many schools have not updated their FERPA

50. *See* CAUSE TASK FORCE, *supra* note 20, at 3 ("It is easier to combine databases, to perform automated search and sorting processes, to use data for secondary purposes with no human authorization, and to instantly transport data over electronic networks from one location to another—perhaps without a moment's reflection on the privacy implications of such actions.").

51. According to the LAMP Project, "[There is] confusion and uncertainty [among systems administrators] regarding whether sharing of the logged data constitutes a violation under FERPA." LAMP PROJECT, *supra* note 6, at 5.5.

52. *Id.* at 5.2 (demonstrating results as to agreement/disagreement with statements concerning FERPA on six factual scenarios related to logging).

53. *See* 20 U.S.C. § 1232g(a)(5)(B) (2000) (allowing schools to designate categories of directory information in accordance with FERPA); New FERPA Final Regulations, 65 Fed. Reg. 41,852, 41,855 (July 6, 2000) (noting that "the examples of 'directory information' listed in the regulations are not intended to be exhaustive"); *id.* at 41,863 (referencing permissible disclosures under 34 C.F.R. § 99.31(a)).

54. LAMP PROJECT, *supra* note 6, at 5.1.

55. FERPA was passed as an amendment to the 1974 Education Act and, as such, it has little legislative history. *See* H.R. REP. NO. 93-1056 (1974) and S. CONF. REP. NO. 93-1409 (1974), *reprinted in* 1974 U.S.C.C.A.N. 6779. Furthermore, "[l]ike Congress, litigants also treat [FERPA] largely as an afterthought ... [and] the legal system has largely ignored [FERPA]." Daggett, *supra* note 22, at 618.

56. FERPA was amended four times in the 1990s, with the amendments primarily concerning student safety from crime. Crime Awareness and Campus Security Act of 1990 of the Student Right-to-Know and Campus Security Act, Pub. L. No. 101-542, § 203, 104 Stat. 2381, 2384–87 (1990) (permitting disclosures concerning violent criminal activity); Higher Education Amendments of 1992, Pub. L. No. 102-325, § 1555, 106 Stat. 448, 840 (1992) (amending language regarding law enforcement records); Improving America's Schools Act of 1994, Pub. L. No. 103-382, § 249, 108 Stat. 3518, 3924–26 (1994) (permitting disclosure for subpoenas and student emergencies); Higher Education Amendments of 1998, Pub. L. No. 105-244, §§ 951–52, 112 Stat. 1581, 1835–36 (1998) (broadening definition of officials who may access student records and adding language regarding disclosure of disciplinary proceedings for sex offenders). For a summary of these amendments and their effects, see Daggett, *supra* note 22, at 620–22. FERPA also has been amended in this century, most recently to permit disclosures to the Immigration and Naturalization Service and to the Attorney General to combat terrorism. USA

policies to reflect technological changes in the last five years.[57] In a recent survey, sixty-five percent of systems administrators polled admitted that their schools did not have any formal policies concerning the collection, appropriate use, authorization levels, or disposal of logged computer data.[58] Furthermore, schools that attempt to delineate a technology policy under FERPA are faced with many questions,[59] including whether the value of access is more important than the risk of a privacy violation.[60]

PATRIOT Act, Pub. L. No. 107-56, § 507, 115 Stat. 367–68 (2001) (codified as amended at 20 U.S.C.A. § 1232g(j) (West 2000 & Supp. 2002)); *see* Paula T. Kaufman & Peter M. Siegel, *9/11 Legislation and Technology: The Academic Impact*, EDUCAUSE REV., Sept.–Oct. 2002 at 86 (discussing the impact of the USA PATRIOT Act on school use of technology).

57. Hillison et al., *supra* note 31, at 302 n.3 (discussing a study in which twelve schools out of 100 surveyed in 2001 had not updated their FERPA policies).

58. LAMP PROJECT, *supra* note 6, at 4.7. The absence of formal policies may create many problems. CAUSE TASK FORCE, *supra* note 20, at 3 ("New technologies are exposing campus administrators to a barrage of inquiries, demands and complaints .... Without comprehensive, carefully considered policy, the need for case-by-case decision-making will turn into an impossible burden."); Boersen, *supra* note 2 (quoting Jim Secreto of University of Michigan's campus ACLU: "[U]nless there is a specific policy in place, there is always the opportunity for invasion of a constitutional right to privacy."); Jeffrey Young, *Montana Allows Public Colleges to Monitor Computer Use*, CHRON. HIGHER EDUC., June 14, 2002, at A31 (quoting a policy officer in Cornell's information technology office: "In the heat of the moment, people sometimes do rash things unless guided by policy.").

59. Existent policies vary widely among schools. *Compare* Bob Anez, *Regents Approve Policy for Tracking Higher Ed Computer Use*, ASSOC. PRESS ST. & LOC. WIRE, May 24, 2002 (detailing a new Montana University computer monitoring policy that "should spell out more clearly who has authority to monitor use," "permits monitoring by information technology staff, administrators, and supervisors," and has no "hard-and-fast requirements for judging what is inappropriate"), *with* The University of North Carolina at Chapel Hill, Electronic Mail and Electronic Transfer of Information Policy, *at* http://www.unc.edu/policy/emailprivacy.html (last modified Dec. 13, 2002) (on file with the North Carolina Law Review) (delineating seven instances when a systems administrator may access student personal information and further defining which instances need provost or legal counsel's prior approval). *See also* Michael J. Kleckner, *U. Oregon Users Lack Internet Protection*, OR. DAILY EMERALD, Jan 25, 2002, http://www.dailyemerald.com/vnews/display.v/ART/2002/01/25/3c5187393c6b6 (on file with the North Carolina Law Review) (comparing the University of Oregon, which has no computer privacy policy, to the University of California, which has a comprehensive "Electronic Communications Policy").

60. Policy considerations may include: How sensitive are student e-mail records or Web site visits? Is protection a high priority, or should schools assume that students know that many Internet transactions are not private? How sensitive is a student file stored online? Should an individual's school photograph be categorized as "directory information" if it is posted on the Internet and can be accessed worldwide? Susan K. Ferencz & C.W. Goldsmith, *Privacy Issues in a Virtual Learning Environment*, CAUSE/EFFECT, Vol. 21, No. 1, 1998, at 5, 9–10, *available at* http://www.educause.edu/ir/library/pdf/cem981w.pdf.

Unfortunately, in many instances, the systems administrator must answer these questions himself and ultimately decide the extent and value of students' privacy regarding computer records.[61] In addition to possibly having no written policies to follow, few systems administrators have been informed about FERPA or student educational privacy.[62] The result may be that "the responsibility for technology applications rests with people who have not had to be concerned with privacy and compliance issues."[63]

Students also are ill-equipped to provide a check on unauthorized use of their personal computing or identification card information. University students' expectations of privacy may differ from those of other computer and ID card users, such as employees. For example, many employees use company-owned computers and networks primarily for work purposes, and their e-mail communications and other computer activities are often not private.[64] In contrast, students use the university network not only in academic buildings, but also in their own "homes"—student dorms.[65] Many undergraduates rely on the campus network for all their computer needs, from doing research on a university-owned computer in the

61. *See id.* at 10; *supra* notes 16–17, 19, and accompanying text.

62. LAMP PROJECT, *supra* note 6, at 3.3 (noting that only twelve percent of systems administrators responding to the nationwide survey had received training in fair information practice or data access, and none had taken a FERPA course). Further, many university personnel may have access to confidential student data but are not recognized as persons needing FERPA training or given background checks to ensure the security of the information. *See* Yeager, *supra* note 10.

63. CAUSE TASK FORCE, *supra* note 20, at 3. Ferencz and Goldsmith, *supra* note 60, note that more harm to student privacy is done through ignorance of FERPA and school policy than through intentional activity. *Id.* at 9; *see, e.g.*, Linda H. Fleit, Self-Assessment for Campus Information Technology Services, CAUSE White Paper, 1994 (on file with the North Carolina Law Review) (providing a policy guide for campus network administrators, but failing to address student privacy issues).

64. According to a recent American Management Association report, over three quarters of major U.S. companies monitor their employees' computers. *See* 2001 AMA SURVEY, WORKPLACE MONITORING & SURVEILLANCE, SUMMARY OF KEY FINDINGS, *at* http://www.amanet. org/research/pdfs/ems_short2001.pdf (last visited Feb. 25, 2003) (on file with the North Carolina Law Review); *see also* United States v. Angevine, 281 F.3d 1130, 1135 (10th Cir. 2002), *cert. denied*, 123 S. Ct. 182 (2002) (finding that an employee did not have a reasonable expectation of privacy in computer files and logs on computers issued for work purposes).

65. *See* Susan C. Thomson, *More Students Are Opting for the Campus Life*, ST. LOUIS POST-DISPATCH, Aug. 18, 2002, at D1 (finding that commuter colleges are less prevalent now than even a few years ago because an increasing number of students wish to live on-campus). Though some undergraduate students choose to live off-campus, this Recent Development focuses specifically on students residing in campus housing, where the university network often serves both personal and academic functions. *See infra* note 66 and accompanying text.

library to chatting with their friends at 2 a.m. on individually-owned personal computers in their dorms.[66] Further, unlike employees, students often pay for their network use through technology fees included in tuition or room and board charges.[67] Thus, students may conclude that their school would not monitor their computer or card use in the same way that an employer would monitor an employee.

Expectations of privacy in other facets of campus life also may cause students to assume their log information is protected. Students do not expect a dean or faculty member to intercept their phone calls,[68] which are often facilitated through the university's phone system, or to invade their dorm rooms or lockers, which are provided by and ultimately belong to the university. Correspondingly, students likely do not expect school personnel to access the contents of their personal e-mail messages or determine their whereabouts through the university's network.[69] Relying on these expectations, students may not realize that their personal information may be accessed or disclosed.[70] To compound the problem, students who are concerned

66. *See Class Is In Session: A 'Pop Quiz' to Find the Right Computer for School*, PR NEWSWIRE, Aug. 19, 2002, LexisNexis Academic Universe (offering advice on student computers, which have become "as commonplace as spiral notebooks and pencils"); Palmer Houchins, *Laptop Requirement a Reality for Some*, DAILY MISSISSIPPIAN, Sept. 12, 2002, http://www.thedmonline.com/vnews/display.v/ART/2002/09/12/3d80416097435 (on file with the North Carolina Law Review) (citing a survey by The University of Mississippi that found that eighty-five percent of incoming freshmen in 2002 were planning to bring a computer to school); Grant Smith, *Students Say They Would Be Lost Without Computers: Technology Plays an Ever-Increasing Role in College Life*, CHARLESTON DAILY MAIL, Sept. 21, 2002, at 8A, LexisNexis Academic Universe (interviewing students about computer use in their dorms).

67. While it is true that students may use their own Internet service providers, those students living on campus have little incentive to do so. *See* William & Mary Information Technology Homepage, Network/Internet, *at* http://www.wm.edu/IT/index.php?id=109 (last visited Feb. 21, 2003) (on file with the North Carolina Law Review) (noting that students who previously have used a telephone modem "will discover that the [William & Mary residential network] connection is about twenty times as fast as a modem and there is no monthly fee [because] students pay for their Internet connection ... through the Technology Fee, which is part of [their] room and board charges.").

68. *See* Randolph S. Sergent, Note: *A Fourth Amendment Model for Computer Networks and Data Privacy*, 81 VA. L. REV. 1181, 1196–97 (1995) (arguing that though the telephone company may record conversations just as a systems administrator may review user files, both the telephone user and the computer user retain an expectation of privacy).

69. The computing use policy of The Ohio State University makes clear the similarity between the university network and other school-owned facilities that students use for personal reasons. It affords file space the same status as private library carrels, dormitory rooms, and gym lockers, which OSU owns but enters only for "administrative" purposes such as building maintenance. Electronic Frontier Foundation, *Computers and Academic Freedom: Frequently Asked Questions*, *at* http://www.eff.org/CAF/faq/email.policies.html (last visited Feb. 21, 2003) (on file with the North Carolina Law Review).

70. *See supra* note 5.

about the privacy of their records do not always have viable options for protecting them.[71] Finally, when students discover that their computer records or online information have been misappropriated, they have little remedy under the statute due to the Supreme Court's recent interpretation of FERPA,[72] the Act's toothless enforcement penalties,[73] and congressional deference to the school's discretionary decision making.[74]

The current, uncertain status of computer logging and the absence of adequate safeguards to protect logged information may allow school officials to misappropriate student data either inadvertently, through ignorance or confusion,[75] or intentionally, because no guidelines are in place to stop them.[76] Because student privacy may be seriously at risk if schools decide logging issues ad hoc,[77] Congress should amend FERPA to clarify school policy on computer logging. To adequately guard student privacy until

71. At some schools, flexible options regarding what information should and should not be released are not available. For example, at the University of Texas, use of the Blackboard system, an online teaching tool for posting assignments and class discussions, was conditioned on the release of student directory information. A student-led initiative sought to allow students to choose which parts of their directory information would be kept confidential without denying them use of Blackboard. *See* Claire Harlin, *U.T. Directory May Offer Privacy Options for Students*, DAILY TEXAN, Sept. 23, 2002, LexisNexis Academic Universe ("The students wanted to protect themselves [from release of directory information], however, it was more important for them to be able to participate in class and Blackboard like the rest of the class, and making directory information publicly available was the only choice." (quoting Donald Dumtra, Graduate Student Assembly Representative)); *see also* Mary Dimeglio, *Web Confidentiality Concerns Penn State Students*, DAILY COLLEGIAN, Apr. 22, 2002, LexisNexis Academic Universe (discussing the "all or nothing" nature of student information disclosure at Penn State University and the push to allow students to individually specify what information they would like to release and withhold).

72. In *Gonzaga University v. Doe*, 122 S. Ct. 2268 (2002), the Supreme Court held that FERPA does not grant individual rights enforceable through a § 1983 action. *Id.* at 2282. *But see id.* at 2282 (Stevens, J., dissenting) (arguing that FERPA's language does create a "presumptively enforceable right") (internal quotations omitted). As a result of *Gonzaga University*, students may not sue schools for FERPA violations, but instead must file complaints with FPCO. *Id.* at 2279.

73. *See supra* note 36.

74. *See supra* note 53.

75. *See, e.g.*, *Indiana State U. Mistakenly Posts Students' Personal Information Online*, ASSOC. PRESS, May 21, 2002 (noting that the university accidentally posted 10,000 students' personal information, including Social Security numbers, online for two weeks). The dean of Kent State also recently violated FERPA by obtaining oral but not written permission from students before posting their names and grades online. Jason Gallagher, *Kent State U. Dean Violates Law by Posting Grades Online*, DAILY KENT STATER, via University Wire, Apr. 22, 2002, LexisNexis Academic Universe.

76. *See supra* notes 5, 55–60 and accompanying text.

77. *See supra* notes 7–18 and accompanying text.

Congress acts, FPCO must establish unequivocally that computer log records are covered under FERPA.[78]

If computer logging is unambiguously covered under FERPA, it must be classified into one of the statute's two categories of student information: "directory information"[79] or "education records."[80] At first blush, log information about a student's personal computer use or whereabouts does not resemble a traditional education record. Logs often contain a broader scope of information than that typically found in a registrar's filing cabinet, and logs may at times have little to do with a student's literal education, as they track social as well as academic activities.[81] FPCO should, and legitimately could, however,

78. Many systems administrators and registrars believe that data collected from computer logs constitute some kind of student record under FERPA. *See* LAMP PROJECT, *supra* note 6, at 5.5. This opinion, however, is not universal. *See* Joe Penepinto, *Who Owns Your Email?*, 12 TELEMATICS & INFORMATICS 125, 127 (1995) ("The interpretation ... suggests E-mail files should be treated as just another form of student record. However, that fails to recognize the personal nature of E-mail files and does not clearly delineate who 'owns' E-mail files .... Clearly this interpretation should be challenged.") In addition, to date, no court has decided whether computer log information is covered under FERPA. FPCO is poised to fill this void in student security.

79. 20 U.S.C. § 1232g(a)(5)(A) (2000).

80. *Id.* § 1232g(a)(4)(A)(i)–(ii).

81. *See* Panepinto, *supra* note 78, at 127 (citing a study concluding that student e-mail messages are more likely to contain personal, "purely social," concerns instead of work or study concerns). Likewise, logs of identification card use track students not only as they move from class to class, but also when they leave campus for an afternoon at the beach or return to their dorms after a weekend party. *See supra* notes 11–15 and accompanying text. Some courts have held that school records are not "education records" unless they pertain to academics or other information directly related to a student's education. *See, e.g.*, Red & Black Publ'g v. Bd. of Regents, 427 S.E.2d 257, 261 (Ga. 1993) (permitting disclosure of hazing charges against University of Georgia fraternities because they did not involve academic activities); Kirwan v. Diamondback, 721 A.2d 196, 205 (Md. 1998) (allowing parking ticket violations of University of Maryland athletes to be disclosed to the student newspaper because the violations do not relate to "individual student academic performance, financial aid, or scholastic probation"). These cases, however, appear to illustrate the minority view and have been the subject of considerable criticism. *See* United States v. Miami Univ., 91 F. Supp. 2d 1132, 1149 n.17 (S.D. Ohio 2000) (including disciplinary records as education records and criticizing *Kirwan* and *Red & Black Publishing* because "[n]one of the above decisions provided any reasoning for their narrow interpretation of FERPA, and this Court fails to see how such a limited meaning of 'education records' can be discerned from the plain language"); Lynn M. Daggett & Dixie Snow Huefner, *Recognizing Schools' Legitimate Educational Interests: Rethinking FERPA's Approach to the Confidentiality of Student Discipline and Classroom Records*, 51 AM. U. L. REV. 1, 32 (2001) (noting "*Red & Black* and similar decisions are wrongly decided as a matter of FERPA's current, plain language"); Toni A. Roth, *The Maryland Survey: 1998–1999 Recent Decisions*, 59 MD. L. REV. 1053, 1078–80 (arguing that the court incorrectly interpreted "educational records" under *Kirwan*). The Supreme Court has not defined education records so narrowly, but merely has recited the two-prong definition in the statute as the basis for analysis. *See* Owasso Indep. Sch. Dist. No. I-011 v. Falvo, 534 U.S. 426, 431–34 (2002).

classify computer logs as education records under a variety of rationales.

First, computer logs fit the statutory definition of education records—"records which contain information directly related to a student and are maintained by an educational agency."[82] The Supreme Court recently used this definition as the primary determinant of FERPA qualification.[83] In February 2002, the Court held that the peer grading process, by which each student grades another's test or quiz, fails FERPA's two-prong definition of "education record" because the grade is not a record "maintained" by the student grader.[84] The Court noted that "[t]he word 'maintain' suggests FERPA records will be kept in a filing cabinet in a records room at the school or on a permanent secure database."[85] Under this analysis, computer logs conform to the statutory definition of education records: they contain information directly related to a student and are maintained on a database by systems administrators. Lower courts also have interpreted the two-prong definition to protect nontraditional records under FERPA's "education records" provisions,[86] and one lower court has already concluded that e-mail messages sent to a professor are "education records" under FERPA.[87]

In addition to conforming to the two-prong definition, computer logs fit within FERPA's original definition of education records. When first enacted, FERPA's delineation of "education records" was an exhaustive list of "any and all official records, files, and data directly related to [students] . . . and specifically including, but not limited to, identifying data, academic work completed, level of achievement, attendance data . . . and verified reports of serious or recurring behavior patterns."[88] Computer logging produces data that

82. § 1232g(a)(4)(A)(i)–(ii).

83. *Falvo*, 534 U.S. at 431–33.

84. *Id.*

85. *Id.* at 433.

86. For example, in *MR v. Lincolnwood Board of Education*, 843 F. Supp. 1236 (N.D. Ill. 1994), the court implicitly found that a videotape of a handicapped student was an education record under FERPA because the court permitted disclosure of the tape under the "legitimate educational interest" exception to FERPA. *Id.* at 1239; *see also* Warner v. St. Bernard Parish Sch. Bd., 99 F. Supp. 2d 748, 752 (E.D. La. 2000) (classifying a mother's letter in a student's file as an education record and holding that the school violated FERPA by disclosing its contents to the media).

87. Bates College v. Congregation Beth Abraham, No. CV-01-02, 2001 WL 1671588 (Me. Sup. Ct. Feb 13, 2001).

88. Education Amendments of 1974, § 513, Pub. L. No. 93-380, 88 Stat. 484, 571, 572 (current version at 20 U.S.C. § 1232g (2000)).

directly relate to a student's computer usage,[89] identifies student users, and is by its very nature intended to track and verify recurring behavior patterns.[90] Thus, logs likely fit the definition of education records according to Congress's original legislative scheme.

Characterizing computer logs as education records is also compatible with FERPA's meager but clear legislative history. Senator James L. Buckley, who introduced the bill as an amendment to the Education Amendments of 1974, noted, "There has been clear evidence of frequent, even systematic violations of the privacy of students and parents by the schools through unauthorized collection of sensitive personal information and the unauthorized, inappropriate release of personal data ...."[91] Representative Jack Kemp also concluded:

> [T]here is growing concern over the potential abuse and improper disclosure of information now maintained and used by the public and private school systems .... [School records contain] extensive information on the social and economic background, attitudes and behavior, performance and ability, and health of pupils within those systems .... Because the information stored in these elaborate systems follows the student as he or she goes through the learning process ... and because this information is subjective and involves the most sensitive of data which can be ascertained about an individual, we must come to grips with the potential abuses which can arise from the disclosure of this information.[92]

89. *See supra* notes 8–10.

90. *See supra* notes 16–17.

91. 121 CONG. REC. 13,991 (1975). One impetus for FERPA was a nationwide survey conducted by the Russell Sage Foundation that found very few guidelines in place regarding school recordkeeping. *See* RUSSELL SAGE FOUNDATION, GUIDELINES FOR THE COLLECTION, MAINTENANCE, AND DISSEMINATION OF PUPIL RECORDS: REPORT OF A CONFERENCE ON THE LEGAL AND ETHICAL ASPECTS OF SCHOOL RECORD KEEPING (1970) (reporting inconsistency and a lack of guidance among schools maintaining student records); *see also* Rios v. Read, 73 F.R.D. 589, 598–99 (D.C. N.Y. 1977) (reviewing the legislative history of FERPA).

92. 120 CONG. REC. 9633 (1974); *see also* Kelly A. Nash, *Peer Grading Outlawed: How the Tenth Circuit Misinterpreted the Family Educational Rights and Privacy Act in* Falvo v. Owasso Independent School District, 229 F.3d 956 (10th Cir. 2000), 25 HAMLINE L. REV. 479, 500 n.81 (2002) (quoting 120 CONG. REC. 9633 (1974)).

FERPA was enacted to allow parents[93] of students "access to education records and to protect [students'] right to privacy by limiting the transferability of their records without their consent."[94] By classifying logs as education records, FPCO can continue to effectuate FERPA's original goals.

Additionally, even if computer logs do not fit squarely into traditional notions of education records, they are more similar to education records than they are to directory information. As enumerated in the statute, "directory information" is student information that is relatively impersonal—information (such as address, birthdate, and field of study) that may be found in a campus phone book.[95] In contrast, computer logs of e-mail contents, Web site visits, and identification card use may reveal much more personal information about a student than would be readily available in a public directory.[96] In fact, in its *Comments and Analysis of the 2000 Final Rule on changes to FERPA*, FPCO announced that student e-mail addresses could be classified as directory information, but that class rosters and schedules could not be, because this classification "may lead schools to disclose sensitive information . . . [that] would be harmful or an invasion of privacy."[97] If class rosters, which merely connote students' presence in a class, constitute sensitive information about a student's activities, then Web site visits, e-mail traffic, and identification card information may constitute a similar and greater threat to student privacy if deemed directory information.

Finally, public policy also warrants defining logged data as education records. If logs are deemed directory information, a blanket notice in the student handbook would suffice to notify students of the school's unfettered ability to release their computer information unless they actively protest.[98] Furthermore, once the

93. Before students turn eighteen, parents have the right to access education records. After a student has reached eighteen years of age, however, only the student retains rights in his education records. *See* 20 U.S.C. § 1232g(d) (2000).

94. 120 CONG. REC. 39,862 (1974) (Joint Statement of Senators Buckley and Pell).

95. *See supra* note 46 and accompanying text.

96. *See supra* notes 8–18 and accompanying text.

97. New FERPA Final Regulations, 65 Fed. Reg. 41,852, 41,855 (July 6, 2000).

98. *See supra* note 47 and accompanying text. *But see* Kestenbaum v. Mich. State Univ., 327 N.W.2d 783 (Mich. 1982). In *Kestenbaum*, the Michigan Supreme Court affirmed the Michigan Court of Appeals's holding that the university's refusal to release a computer tape containing students' names and addresses to a political campaign for mass mailings was consistent with FERPA even though the university published a notice about directory information in the student handbook. *Id.* at 789–90. The plaintiff posited that the medium of computer tape made no difference to the designation of the information as directory information. *Id.* The Michigan Supreme Court, however, distinguished the

information is deemed "directory" or is not covered under FERPA at all, there is little to stop a school from profiting by selling records of student Internet use to commercial entities hungry to capitalize on it.[99] Thus, if logs are not classified as education records, students' privacy may be jeopardized by school officials with unauthorized or illegitimate access[100] as well as by the transfer of personal data to commercial and other entities ready to bombard students with unwanted solicitations.

FPCO can better safeguard student information by classifying computer logs as education records. However, log data may not be protected from all potential abuses because of an exception to the student notification requirement that precedes disclosure of education records.[101] Though in general students must consent in writing to the release of their education records, FERPA excepts from this requirement "school officials, including teachers within the educational institution or local educational agency, who have been determined by such agency or institution to have legitimate educational interests, including the educational interests of the

---

directory information in the computer files from the paper directory, noting that "[c]omputer information is readily accessible and easily manipulated .... [I]t does not follow that students should have known that an efficient and intrusive computer mailing system already was available to anyone for a nominal sum." *Id.* *See generally* William Bradley Colwell & Brian D. Schwartz, *Student Handbooks: A Significant Legal Tool for the 21st Century*, 154 Educ. L. Rep. 409 (2001) (detailing the use of student handbooks to insulate a school from liability).

99. Campus ID Report, *April 1996: Article Summaries: Understanding the Buckley Amendment: Is Your Card Program Violating Student Privacy Laws?*, *at* http://www.campusid.com/april16.html (last visited Nov. 13, 2002) (on file with the North Carolina Law Review) (offering advice to schools whose card program vendors seek student information for marketing purposes). The ACLU has alleged that the University and Community College System of Nevada violated FERPA by selling students' and alumni's personal information to a credit card company. *See* Elaine Goodman, *Credit Card Operation: ACLU Says Universities Violating Privacy Rules*, RENO GAZETTE-J., Jan. 23, 2002, 2002 WL 15177494; Letter from Gary Peck, Executive Director, ACLU of Nevada, and Ann Beeson, Staff Attorney, ACLU, National Legal Department, to Jane Nichols, Chancellor, University of Nevada, Jan. 22, 2002, http://archive.aclu.org/news/2002/n012202b.html (on file with the North Carolina Law Review); *see also* CAUSE TASK FORCE, *supra* note 20, at 20 (noting "the sale of student mailing lists by an institution to generate a revenue stream ... might tempt some campuses in times of fiscal constraint"); Susan E. Gindin, *Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet*, 34 SAN DIEGO L. REV. 1153, 1157–61 (1997) (discussing commercial Internet providers' sales of logged data about users and the public outrage accompanying it). The argument that computer data are owned by the owner of the computer or network has been deemed "specious" by one court in upholding the private nature of logs from computers available for public use at libraries. Quad/Graphics, Inc. v. S. Adirondack Library Sys., 664 N.Y.S.2d 225, 228 (1997).

100. *See supra* notes 7–15.

101. *See* 20 U.S.C. § 1232g(b)(4)(A)–(B) (2000).

[student] for whom consent would otherwise be required."[102] Thus, if a professor, campus employer, or other school official can contrive a colorable "legitimate educational interest" for accessing a student's education records, the official may obtain the data without the student's knowledge or consent.[103] Further, FERPA grants schools the discretion to define a "legitimate educational interest."[104] Accordingly, policies vary. Some schools simply define this term according to the Department of Education's ambiguous Final Rule, which states that a school official has a legitimate educational interest if the official needs to review an education record "in order to fulfill his professional responsibility."[105] One school has expanded its definition of "legitimate educational interests" to encompass "interests essential to the general process of higher education including ... general counseling, ... academic assistance activities, [and] experiential learning activities."[106] Another school has shortened its definition to "a legal right to know."[107] Because policies are not uniform, systems administrators are largely untrained, and

---

102. *Id.* § 1232g(b)(1)(A).

103. *Id.*

104. *Id.* The 1994 amendments to FERPA noted that the student's educational interest should be taken into account when determining a "legitimate educational interest," but neither the Act nor FPCO has elaborated on the degree to which this element is to be followed. Improving America's Schools Act of 1994, Pub. L. No. 103-382, § 249, 108 Stat. 3518, 3924–25 (1994).

105. Department of Education, FERPA Final Rule, 61 Fed. Reg. 59,297 (Nov. 21, 1996). The University of Colorado at Boulder is just one school that follows this definition. *See* The University of Colorado, *Student Records Policy*, *at* http://www.registrar.colorado.edu/facstaff/FERPA (last visited Oct. 27, 2002) (on file with the North Carolina Law Review). The University of North Carolina similarly characterizes a legitimate educational interest as one that "is in the educational interest of the student ... or if it is necessary or desirable for the official to obtain the information ... to carry out his or her official duties or to implement the policies of The University of North Carolina." *See* Offices of the University Registrar, The University of North Carolina at Chapel Hill, *Family Educational Rights and Privacy Act Notice*, *at* http://regweb.oit.unc.edu/official/FERPA/notice.html (last visited Feb. 21, 2003) (on file with the North Carolina Law Review). In regard to personal information such as e-mail messages, this definition is too vague.

106. Michigan Technological University Office of Student Records and Registration, *Privacy and Release of Student Educational Records*, *at* http://www.admin.mtu.edu/em/students/policies/privacy.php (last visited Feb. 21, 2003) (on file with the North Carolina Law Review).

107. Catholic Univ. of America, Office of General Counsel, *Of Counsel—A Bulletin on Legal Issues at CUA—November 1997: Questions and Answers About FERPA*, *at* http://counsel.cua.edu/OC/FERPA/question.html (last visited Sept. 30, 2002) (on file with the North Carolina Law Review). *But see* Catholic Univ. of America, Office of General Counsel, *FERPA*, *at* http://counsel.cua.edu/FERPA/questions/ (last revised Dec. 19, 2002) (on file with the North Carolina Law Review) (revising definition to include tasks related to job description as well as tasks related to students' education, discipline, and safety).

schools are not held accountable, school discretion in defining legitimate educational interests may undermine student privacy.

Not surprisingly, schools' interpretations of the legitimate educational interests exception have been at issue in some FERPA controversies. In *Krebs v. Rutgers*,[108] for example, a university attempted to characterize its disclosure of students' Social Security numbers to campus post office personnel as a "legitimate educational interest."[109] The United States District Court for the District of New Jersey enjoined the practice, noting that "the regulations do not suggest, and it is far from clear, that distribution of social security numbers . . . serves a 'legitimate educational interest.' "[110] In contrast, in *Achman v. Chicago Lakes Independent School District No. 2144*,[111] a Minnesota federal district court held that the supervisor of the school's detention room had a legitimate educational interest in accessing the disciplinary records of a student she monitored.[112] In another FERPA case from 1987, the Wisconsin Court of Appeals found that a school official who requested students' education records to defend against her pending criminal charges did not have a legitimate educational interest in the records.[113] Finally, in another instance that some commentators have deemed "an egregious example of when disclosure serves no legitimate educational interest,"[114] a substitute teacher told her class that a student had HIV and classmates should not share lip balm with him.[115]

The meager case law regarding a school's "legitimate educational interests" appears to delineate between appropriate disclosures, which directly relate to the student's educational experience, and inappropriate disclosures, which serve a secondary, more remote

108. 797 F. Supp. 1246 (D.N.J. 1992).

109. *Id.* at 1259.

110. *Id.*

111. 45 F. Supp. 2d 664 (D. Minn. 1999).

112. *Id.* at 669; *see also* Tyler v. Poway Unified Sch. Dist., 2002 Cal. App. Unpub. LEXIS 2903, at *10 (Cal. Ct. App. Mar. 19, 2002) (finding that a school district's practice of transferring student records to a special education expert for help in a mediation was not incompatible with FERPA's legitimate educational interest provision); E. Conn. State Univ. v. Freedom of Info. Comm'n, 1996 WL 580966, at *3 (Conn. Super. Ct. Sept. 30, 1996) (finding that a teacher had a legitimate educational interest in tapes of a student's disciplinary hearing because the teacher filed the initial complaint leading to the hearing).

113. Rathie v. Northeastern Wis. Tech. Inst., 419 N.W.2d 296, 299 (Wis. Ct. App. 1987). In another FERPA case, teachers' use of homeroom lists for mailings pertaining to a collective bargaining agreement did not constitute a legitimate educational interest. Bd. of Dir. of the Palmyra Area Sch. Dist. v. Palmyra Area Educ. Ass'n, 644 A.2d 267, 270 (Pa. Commw. Ct. 1994).

114. Huefner & Daggett, *supra* note 36, at 469, 478.

115. *Right to Privacy*, EDUC. WK., May 22, 1996, at 4.

purpose. FPCO can utilize this framework to define a "legitimate educational interest" in logged information as an interest which furthers the primary purpose for which log data was collected, that is, to maintain safe and efficient access to campus computer systems and to facilitate entry into campus buildings and activities.[116] FPCO also should mandate that due to the sensitive nature of computer log information, school officials' requests for such information must be recorded and kept in the student's file in the same way that an outside request would be.[117] Under this scheme, when systems administrators use log information to maintain the network and investigate security breaches,[118] these actions constitute legitimate educational interests because they are designed explicitly to protect students, their records, and the network.[119] Accordingly, the systems administrator's monitoring in the Hacking Alert scenario[120] and the student worker's access to printer usage logs in the Print Use Records scenario[121] likely

116. Ferencz and Goldsmith have advocated this approach, asserting that "when personal information is gathered from a student, it should be used only for the purpose for which it was collected." Ferencz & Goldsmith, *supra* note 60, at 8. This Recent Development suggests that FPCO should adopt a primary purpose analysis in its guidelines for defining school officials' legitimate educational interests. Clearly, some kind of monitoring is necessary given the high incidence of computer security breaches on college campuses. For example, the Computer Emergency Response Team Coordination Center, which tracks computer security on major corporate and university networks, received 43,136 reported security violations in the first six months of 2002. Kelly Heyboer, *'Ivygate' a Wake-up Call to Nation's Campuses*, NEWHOUSE NEWS SERV., Aug. 2, 2002, LexisNexis Academic Universe. Monitoring also may be necessary to protect students from crime and robbery. *See* Randy I. Atlas & Stanley A. Young, *Planting and Shaping Security Success*, 46 SECURITY MGMT. 71 (2002), 2002 WL 23073167 (describing how Barry University's crime rate dropped twenty-five percent after an identification card access system was installed); John F. Kirch, *Drawing the Right Card*, 41 SECURITY MGMT. 62 (1997), 1997 WL 9533066 (noting that Duke University students and employees feel safer with an identification card system for building access); Weiser, *supra* note 5 (reporting that Princeton University's theft, burglary, and sexual assault rates have declined since an identification card system was installed). However, without more guidance from FPCO, some schools may not temper their monitoring with adequate privacy safeguards. *See supra* notes 57–60, 75 and accompanying text.

117. *See supra* notes 40–43 and accompanying text. In this way, a student may access his file and be better able to investigate or contest inappropriate uses by school officials.

118. *See* LAMP PROJECT, *supra* note 6, at 4.2 (detailing the three primary purposes for which systems administrators were logging); *supra* note 8 (discussing the troubleshooting tasks performed by systems administrators).

119. This means that a school could use computer usage logs to punish a student for maintaining an illegal business, possessing or trafficking in child pornography, sending a mass mailing or a disruptive chain letter, or pirating information in violation of the copyright laws. Identification card logs may be used to track stolen cards and to sound an alarm when a stolen card is used to attempt dorm entry. *See* Lisa Arbetter et al., *All in One*, SECURITY MGMT., Jan. 1, 1994, 1994 WL 2823140.

120. *See supra* notes 16–17 and accompanying text.

121. *See supra* note 18 and accompanying text.

would be acceptable uses of logged information because such uses serve the primary purpose for which the logs were created. In contrast, the dean in the Curious Dean scenario[122] and the campus employer in the ID Card Tracking scenario[123] likely would have a secondary purpose for the information—neither is performing routine system maintenance or stopping an immediate threat to the network. Accordingly, their interests in the information would not qualify as "legitimate educational interests" under the primary purpose analysis. Consequently, before log information could be released to the dean or employer in these scenarios, the systems administrator would be obligated under FERPA to notify the student and obtain her written permission.[124] Systems administrators could further enforce this policy by disabling any logging function not necessary to maintain network safety.[125] Moreover, if there were a serious need for the logged information that greatly outweighed the need for student privacy, the dean or guidance counselor likely could invoke FERPA's emergency exception, which provides that schools may disclose information to "appropriate persons if the knowledge of such information is necessary to protect the health or safety of the student or other persons."[126]

---

122. *See supra* notes 7–10 and accompanying text.

123. *See supra* notes 11–15 and accompanying text.

124. *See supra* notes 37–43 and accompanying text; *see also* Ferencz & Goldsmith, *supra* note 60, at 8 (noting that if student data is used for "non-routine purposes," school officials should obtain student consent).

125. *See* Rezmierski & Soules, *supra* note 3, at 24 ("Generally, security professionals need to look only at basic machine-identification information and network time-stamps to discern the source of abuse and who was using the source machine at that time. They are not interested in what a particular individual was accessing or reading when an abuse was committed."). The LAMP Project provides a schema for levels of security commensurate with levels of logging. *See* LAMP PROJECT, *supra* note 6, at 6.5. The report recommends that most logging functions be disabled from identifying specific users. *Id.* It also advises that logging functions that identify users be closely monitored by those trained in FERPA who have high-level authorization. *See id*; *see also* UNIVERSITY OF MICHIGAN STANDARD PRACTICE GUIDE, PRIVACY OF ELECTRONIC MAIL AND COMPUTER FILES AT THE UNIVERSITY OF MICHIGAN, Dec. 1, 1993, http://spg.umich.edu/pdf/601.11.pdf (on file with the North Carolina Law Review) (recommending protections such as encryption, filters, and user permission when performing network maintenance that compromises privacy). Schools also may keep curious personnel from tracking students by allowing only the campus police or public safety department to access identification card logs. The College of William and Mary protects student privacy in this way. *See* E-mail from Carolyn Burks, The College of William and Mary, to Jennifer Wasson (Nov. 13, 2002, 13:24:47 EDT) (on file with the North Carolina Law Review); *see also* Arbetter et al., *supra* note 119 (noting that the identification card access system is controlled by public safety personnel at Pepperdine University).

126. 20 U.S.C. § 1232g(b)(1)(I) (2000). An example of tracking to investigate a serious infraction occurred at Duke University after a student planted a homemade bomb in the

The primary purpose framework will help to ensure student privacy while protecting network security. First, it properly balances students' privacy rights with the need for secure and efficient school operations. Second, the method aligns with students' expectations: though students may realize that their identification card information goes "somewhere" and that the network is monitored to protect against abuse,[127] they likely do not expect that their personal information will be used to satisfy curious, suspicious, or concerned school personnel,[128] or be misappropriated for other purposes, such as raising revenue for the school.[129] Furthermore, students likely are aware that their grades and Social Security numbers cannot be disclosed,[130] and they probably would expect highly personal information such as that detailed in logs to be treated similarly.[131]

---

registrar's office. *See* Kirch, *supra* note 116. Campus police examined logs of entry into the registrar's office and other buildings where debris was found as well as logs of purchase information for the bomb's contents from the student store to find the student responsible for the crime. *Id. But see* Weiser, *supra* note 5, (noting that Princeton University officials, seeking to preserve student privacy, denied log information to police officers investigating vandalism). Though FERPA's emergency exception may prevent or alleviate serious harm, this provision likely needs more clarity and tweaking as well. For an example of how a school may have used its discretion and the emergency exception of FERPA to a student's peril, see Denise Lavoie, *MIT Sued in Wrongful Death Suit*, ASSOC. PRESS, Jan. 29, 2002, http://news.findlaw.com/ap_stories/other/1110/1-29-2002/20020129 1012307103.html (on file with the North Carolina Law Review) (noting that M.I.T. officials failed to warn a suicidal student's parents of her condition, citing FERPA as authority for their non-disclosure). Until FPCO or Congress revises FERPA's emergency provision, schools should clarify what constitutes an "emergency" and make specific provisions in regard to student tracking. *See, e.g.*, Weiser, *supra* note 5 (detailing the authorized and unauthorized uses for logged data in the Princeton University privacy policy).

127. *See supra* notes 48, 59.

128. *See supra* note 5 and accompanying text.

129. *See supra* note 99. "It would appear reasonable to expect that a government agency, to which a citizen is required to submit certain materials, will use those materials solely for the purposes intended and not disclose them to others in ways that are unconnected with those intended purposes." Commonwealth v. Buccella, 751 N.E.2d 373, 383 (Mass. 2001).

130. *See* Andrea Foster, *ID Theft Turns Students into Privacy Activists*, CHRON. HIGHER EDUC., Aug. 2, 2002, at 27 (discussing student pressure on university officials to remove Social Security numbers from identification cards to prevent identity theft); Dave Katzman, *Student ID Numbers Found in Garbage*, SIUC DAILY EGYPTIAN, May 2, 1996, *at* http://www.dailyegyptian.com/spring96/050296/security.html (on file with the North Carolina Law Review) (reporting students' shock and outrage when a former student found a list with Social Security numbers and addresses in a dumpster on school grounds and found a discarded list of student ID numbers and phone charges behind a campus building).

131. *See* Boersen, *supra* note 2 (noting that many students believe their computer records are private); Shillito, *supra* note 5 (explaining that some students do not know how

The primary purpose analysis also conforms with FERPA's foundational purpose of protecting students' rights to privacy by limiting the transferability of their records without their consent.[132] This analysis affords students all protections under the Fair Information Practices Guidelines,[133] written by the Department of Health, Education, and Welfare at the time of FERPA's enactment, to ensure that information about an individual is not maintained without his knowledge and ability to control its use and contents. Most importantly, this characterization preserves students' rights to discover and contest uses that exceed mere system maintenance and security.

Finally, this categorization of computer logs is practical and workable. It solves the basic problems of maintaining network security and operations for all users, protecting students from unauthorized invasions into their accounts. At the same time, it ensures that highly personal student data are not used for secondary, and often improper, purposes.

Judging from the varied policies,[134] confusion among registrars and systems administrators,[135] and student ignorance of data collection and use,[136] student privacy rights in computer log information are at serious risk of abuse by school administrators and others. To correct and prevent these abuses, Congress should amend FERPA to address logging issues specifically. Until then, the Family Policy Compliance Office should clarify FERPA policy on computer logging. This can best be done by explicitly providing for computer logging in the regulations accompanying FERPA, by categorizing computer data as "education records" under the statute, and by delineating primary versus secondary purposes as the determinant of "legitimate educational interests."

JENNIFER C. WASSON

much of their personal information is revealed to outsiders through the university network).

132. *See* 120 CONG. REC. 39,858–66 (1974) (Joint Statement of Sens. Buckley and Pell).

133. *See* U.S. DEP'T OF HEALTH, EDUC., AND WELFARE REP., RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS (1973) (recommending a federal code of fair information practices governing both public and private record keeping systems).

134. *See supra* note 59 and accompanying text.

135. *See supra* notes 58–63 and accompanying text.

136. *See supra* notes 2, 5, and accompanying text.