

The Federal Role in Student Privacy – FERPA and Beyond

**© Dana Walker
May 2000**

The Federal Role in Student Privacy – FERPA and Beyond

A Washington, DC mother is denied access to psychological tests, which indicate to school officials that her child should repeat kindergarten. A new teacher receives this summary of a student's previous classroom performance: "A real sickie—absent, truant, stubborn, and very dull. Is verbal only about outside, irrelevant facts. Can barely read (which was a huge accomplishment to get this far). Have fun." A New York landlord gains access to his youthful tenant's college financial records. The secretary of a private tutoring agency calls a public junior high school to inquire about a child's reading level and is in turn also briefed about the child's bedwetting history and her mother's alcoholism. (George, 1978)

The value of privacy, or as Justice Brandeis argued in his dissenting opinion in *Olmstead v. U.S.*, the "right to be left alone – the most comprehensive of rights, and the right most valued by a free people," has long been an important right to the U.S. public. With the horror stories above, it is easy to imagine that concern about privacy and confidentiality abuses as related to student records swelled in the early 1970s. But concerns about privacy abuses were not limited to students. The late 1960s and early 70s saw a tremendous amount of activity regarding privacy, both in the legislative and judicial arenas.

In response to the increasing concerns raised by privacy advocates, Congress passed the Freedom of Information Act in 1966 as a way for citizens to request information about the operation of the government. The next year, in 1967, the Supreme Court reversed the famous *Olmstead v. U.S.* case and declared that the government must have a warrant to wiretap (*Katz v. U.S.*). In 1970, Congress passed the Fair Credit Reporting Act that gave consumers the right to request and correct information kept by credit bureaus. The Supreme Court, in 1973, ruled on *Roe v. Wade* which limited the ability of the government to regulate abortion, in part because it saw that regulation as an infringement on privacy. In 1974, Congress passed the overarching Privacy Act that regulated the collection, maintenance, use and dissemination of personal information by federal agencies (O'Brien, 1979; see also Privacy Protection Study Commission, 1977).

History of FERPA Legislation

It was in this environment of general concern about privacy and confidentiality¹ that Senator James L. Buckley of New York introduced his floor amendment to the General Education Provisions Act of 1974. Citing the "many absurd and sometimes tragic examples of abuses," (Buckley in George, 1978, p. 25) Buckley introduced the legislation to protect student records and to curb what he saw as educators usurping parental authority (Cudlipp in U.S. Congress, 1976). FERPA covers elementary and secondary educational institutions as well as postsecondary institutions. However, FERPA was primarily designed to address problems in elementary and secondary schools, applying it to higher education institutions was an afterthought (Privacy Protection Study Commission, 1977).

As noted, privacy legislation and case law were not new to the legislative and judicial arenas of the early 1970s. The Buckley Amendment was another attempt, although sector specific, at privacy protection. Nevertheless, the legislation had a rocky start. Buckley was criticized for the way he introduced the bill – a last-minute floor amendment to the General Education Provisions Act – because it did not allow for the usual committee and public hearing process. Even after passage on the floor, the legislation was not afforded a tremendous amount of support in conference. Passage was aided by the highly controversial busing issue that was associated with the 1974 General Education Bill (George, 1978). House and Senate conservatives were not necessarily concerned with student records policy. They were, however, concerned with the psychological and behavioral testing that was occurring in elementary and secondary schools. In essence, adding an educational privacy amendment made the pro-bussing provision more acceptable to congressional conservatives (George, 1978).

The Family Educational Rights and Privacy Act of 1974 (§ 513 of P.L. 93-380 – the Education Amendments of 1974) was signed into law by President Ford in August 1974 and was codified at 10 U.S.C. § 1232g. Initially, few educators were aware of its passage. As soon as the implications of the legislation became apparent, educational institutions and organizations began to express their many concerns en masse. “The initial reaction of many sectors of the education community was one of alarm. They professed a fear of endless red tape and court suits which would interfere with legitimate educational functions.” (Buckley in U.S. Congress, 1976) A compromise measure, known as the Buckley/Pell Amendment, was signed into law in December 1974 and made retroactive². The compromise addressed a number of the ambiguities and concerns identified by the educational community, especially policies regarding letters of recommendation, parental financial records, grades and test scores (U.S. Congress, 1974).

FERPA: The Federal Role as Protector of Student Privacy

The overall goal of FERPA was to balance the institution’s need to maintain information about an individual with the obligation to protect the individual’s rights regarding the collection, maintenance, use and dissemination of personally identifiable information. FERPA, like virtually all privacy policy and law in the U.S., including the omnibus Privacy Act of 1974, is framed after a concept known as the “Code of Fair Information Practices³.” To summarize, the code – first developed by the Department of Health, Education, and Welfare’s Advisory Committee on Automated Data Systems – states that when an individual gives personally identifiable information to an organization two things happen: the organization takes on an obligation and the individual is granted some rights (Rotenberg, 1998).

The law creates a minimum standard for the protection of records. Broadly stated, FERPA protects educational records at both the elementary/secondary level and postsecondary level. This particular paper will focus only on postsecondary institutions. The law has three basic policy objectives: (1) to grant students (or their parents if the student is under age 18) access to their education records⁴; (2) to grant students the right to seek amendment of their education records; and (3) to grant students some control over the disclosure of their education records⁵.

FERPA is a “spending clause” statute - the statute does not specifically prohibit the disclosure of covered records, but unauthorized disclosures can result in a cut-off of federal funds to the institution. The law has been interpreted and implemented broadly to cover all student-connected records. Institutions, overall, have created relatively complex bureaucracies to administer the regulations.

For the purposes of the law, personally identifiable information is split into two categories. The first, the so-called directory information⁶, is information that is generally not considered harmful or an invasion of privacy if disclosed (e.g. name, address, phone, date and place of birth, dates of attendance, etc.). Students have the choice of opting-out of disclosure of directory information. If the student has not opted-out, then prior written consent is not required to disclose directory information. The second, non-directory information, is all other information contained in the educational record. Prior written consent is required before this information can be disclosed. There are, however, 14 exceptions to the prior written consent rule⁷. Furthermore, FERPA requires that institutions annually notify students of their rights, including what is considered directory information and methods for opting-out.

25 Years Later – Student Privacy Today

Despite its rough beginnings, FERPA did initially accomplish its goals. The law forced educational institutions to consider their policies and practices regarding student records and to understand their responsibilities in regard to those records. Before its passage, school record laws varied widely among states. Only 24 states provided some form of parental or student access to records, of those only five

explicitly granted the right to contest or correct information and nine prohibited release of information without consent (Cudlipp in U.S. Congress, 1976).

Importantly, the legislation affirmed that the federal government was fundamentally interested in two things when it came to student information. First there was a set of minimum standards, a code of fair information practice, necessary to protect the confidentiality and privacy of student information and educational institutions had the obligation to meet those standards. Second, students had some rights regarding their own information. A student had the right to notification, to inspection, to amendment and to nondisclosure.

It is arguable that 25 years after its enactment, FERPA is not meeting its goals. Institutions have created systems, sometimes elaborate bureaucracies, to comply with FERPA regulations. But those regulations are simply the outer layer of an outdated system. The interior is no longer serving the needs of students or educational institutions.

What happened? It is not that privacy issues are new, the individual right to privacy has been debated in the U.S. since the country's founding. Information collection and storage aren't new either. What is new is that privacy issues have become more complex. Today the challenge to all privacy law, including FERPA, is that the dawn of the "Information Age" has re-framed the privacy debate. The number of databases storing personal information has grown exponentially – the techniques for constructing those databases are not new, but the techniques for using them have multiplied. Furthermore, it is now easier to merge databases, which enables users to mine data and create new information. And the new networked technology infrastructure allows data gatherers to track the movements of people and things (Agre and Rotenberg, 1998).

To say that educational information practices in the year 2000 are different than 1974 is overly simplistic, but true. In 1974, student records were limited to grades, transcripts and class selections. The focus was on centralized data collection – records were generally contained in a single office or a single database or file. Data was under the specific responsibility of a known individual – record stewardship was under the authority of the registrar or bursar. The collection of personal information was labor intensive and its centralized storage made it more difficult to widely distribute.

In 2000, institutions have taken advantage of emerging technologies to improve student service, efficiency, accountability and instruction. They have converted to networked databases, have created student service systems on the Internet, and have become increasingly dependent on email, data warehouses and electronic data exchange. The drafters of FERPA could not have foreseen these changes. Technology has made it possible to capture, store, and access a student's medical information, digitized images, building usage, library usage, dining habits, computer log-on and usage, purchases, and money card usage (CAUSE, 1997).

The Privacy Balancing Act

New technology has been both a bane and a blessing (CAUSE, 1997). There is a delicate balance between an institution's obligation to protect its students' privacy and the responsibility to provide effective service and public accountability. In their 1995 book *The Right to Privacy*, Alderman and Kennedy wrote, "Whenever an invasion of privacy is claimed, there are usually competing values at stake. Privacy may seem paramount to a person who has lost it, but that right often clashes with other rights and responsibilities that we as a society deem important."

Policymakers face a significant dilemma when creating privacy policies appropriate for the year 2000. Should student's privacy dictate the policy? Should institutional needs be more important? Is there a place in the middle?

Privacy is a value. It is not an absolute. A company called KinderCam claims to be the industry leader in “childcare viewing systems.” KinderCam works with childcare providers to place cameras in the childcare center. Parents, while working or at home, can jump on the Internet and see live video of their children at play. Parents seem to be happy about the opportunity to view their children from afar, they can follow their daily routines, watch them interact with others and keep up with their development. These same parents, however, are less than happy about the concept of cameras in their own workplace. “KinderCam reversed.” (Brin, 1998)

What in one situation may be considered acceptable or even essential (KinderCam) may be an infringement on privacy in a different context (KinderCam reversed). If the right to privacy is a balancing act, then the protection policies must be as well.

Beyond FERPA - Toward a New Student Privacy Policy

There is no turning back from the explosion in technology. How, then, do decision-makers develop effective and balanced policies to protect student privacy? If FERPA isn’t working, then what will?

In this new landscape, new questions arise:

- What is considered proper notification when student data is being stored and transported among different offices on a continual basis? Should privacy policies include an opt-in selection instead of the current opt-out policy?
- If an institution is required to collect data for Accountability Study A, can the institution also collect some additional information that *may* be needed for the future Accountability Study B? After the data is collected, should it be stored, deleted or disseminated?
- Is it appropriate to collect some data anonymously?
- If the public is supporting higher education through tax dollars, should that student data be used for secondary purposes if it helps further institutional and student accountability?

The development of privacy policy balances on the question of who decides. When does a student’s individual right supersede the institution’s need? When does the institution’s need supersede the student’s right to privacy? In order to get to a policy that is balanced, flexible and appropriate in a networked world, privacy policy must be based on two things: (1) It must continue to be founded on a strong ground of enforceable fair information practices - in an updated form; and (2) a good privacy policy must promote technologies, known as privacy-enhancing technologies (PETs), that will protect the disclosure of personal information.

It is a mistake to assume that a good privacy policy can be based on one and not the other. Institutions too easily believe that if the data is kept confidential, through secure technology, that they have upheld their responsibility to protect privacy. True, confidentiality is a means to protect privacy by keeping information safe from unauthorized disclosure. But confidentiality is only relevant *after* the data has been collected (Cavoukian, 1996).

Real privacy, based on fair information practice, allows an individual to consent to the collection of data. The Germans have referred to this as “informational self-determination.” As Marc Rotenberg, a leading privacy advocate stated, “Where once individual *consent* was central to the disclosure of personal information, now the focus is on individual *choice* for a range of disclosures. Where privacy techniques focused on the means to protect identity, now the focus is on means to obtain information.” (Rotenberg, 1998)

New Fair Information Practices for a New Landscape

The drafters of FERPA based the original law on a foundation of fair information practice. However, the regulations have not kept pace with technology. FERPA does not address new security issues, proper notification or access, or new secondary use issues. So how could an institution employ a privacy practice that was based on fair information practice as well as privacy-enhancing technology?

Let's say an institution is looking to market to new students and wants to perform a study regarding the financial background of its financial aid students.

Scenario 1: Institution A knows that the data is already available because it was collected when the student submitted her application for financial aid. The institutional research office, in the interest of time and ease (and uninformed about the institution's privacy policy), compiles the already existing data and uses it for the study.

Scenario 2: Institution B will collect the data by notifying each student of the purpose of the data collection (market study) and will affirm that the data will not be used for a secondary purpose. The data is stored using the student's identification number and the researchers compile the study.

Scenario 3: Institution C will notify and collect the data in the same manner as Institution B, but decides to secure the data by putting it behind a firewall. Only a single researcher will be able to access the data. The researcher compiles the study.

Scenario 4: Institution D will notify students in the same manner as Institutions B and C, but will collect the data anonymously through blind signatures. The data is authentic and accurate, but cannot be linked to a particular person. The study is completed.

In all four scenarios the institution performs the study, but clearly, Scenario 4 provides the most privacy protection to the student. How is it done? By combining fair information solutions with privacy-enhancing technology solutions.

Solution 1: Minimization/Collection Limitation

The fair information practice of data minimization is one of the most important for higher education institutions. When faced with ever-increasing demands for accountability assessments, institutions are collecting more and more data. In 1977, the Privacy Protection Study Commission raised concerns about this trend.

Educational institutions make and keep more records about students than ever before. More people participate in making and keeping education records, and more people outside the educational system want access to them for other than educational purposes. Moreover, the emphasis in educational record keeping has shifted from reporting progress to parents and making decisions about students to serving not only as a management tool but also as a means of justifying an educational institution's actions and budget. (Privacy Protection Study Commission, 1977, p. 394)

The challenge to an institution is to identify data that is truly the minimum needed and to avoid collecting data for collection's sake or for potential future use (CAUSE, 1997). Each additional piece of personally identifiable information that is stored can lead to a potential abuse of individual privacy. Educational policymakers should question if they really need to know or store information about where students eat, at

what time they access a building and what they buy at the campus bookstore. If the information is mission-critical can it be collected anonymously? Are there ways that information can be retrieved later on an as-needed basis?

Federal and state policymakers need to grapple with the same minimization standards. As Henderson in his 1999 book, *Privacy in the Information Age*, argues, “The government is in a paradoxical position with regard to privacy. On the one hand, legislatures and courts have provided a growing number of guarantees of privacy rights in some areas. On the other hand, the government is itself the single largest gatherer and user of information about individuals.” (Henderson, 1999, p. 31) Since the 1960s, the federal government has increased its involvement in higher education. With such a tremendous investment of taxpayer resources, the public has a right to hold higher education institutions accountable for those dollars. However, federal policymakers need to ask themselves the same tough questions – does the public need information on athletes’ completion and transfer-out rates⁸ or detailed statistics on arrests or persons referred for campus disciplinary actions for liquor law violations, drug-related violations or weapons possession⁹? Each additional piece of data requested increases not only administrative burdens, but also increases the amount of personally-identifiable information that is tied to a particular person.

Solution 2: Anonymous Collection

To the extent that data collection can be minimized, privacy interests will be advanced. If the information is mission critical and should be collected policymakers need to decide if the data can be collected anonymously.

A new technology called the blind signature, an extension of the digital signature, enables data to be collected anonymously. A standard digital signature provides authentication using public key encryption. In this type of encryption, two keys are created – one private and one public. Only the individual has access to the private key and the public key is made widely available. If a student, for example, encrypts a document with her private key, she basically “signs” that document. The institution can then decrypt the message using the public key (Cavoukian, 1996).

The advantage of a digital signature is that it provides authentication in an electronic form. The drawback of a standard digital signature, however, is that the identity of the person is revealed. The blind signature, on the other hand, extends the digital signature technology and ensures anonymity. The institution can authenticate the transmission (through its public key), but can not link the data to an individual.

Blind signature technology is currently employed for financial transactions, or “e-cash.” Banks sign and distribute digital notes without keeping a record of which notes an individual has been given. An individual who wishes to withdraw money from a bank must prepare a digital note with a secret serial number and submit it to the bank. The bank withdraws the money from the individual’s account and signs the note. When the individual gives the digital note to a vendor, the vendor takes the note to the bank and asks for it to be deposited. The bank can verify the signature on the note to determine its legitimacy, but as with most cash transactions, the bank can not determine which individual gave the note to the vendor (Hoffman and Carreiro, 1997).

The potential for anonymous technologies doesn’t stop at e-cash. Can information on personal family background, income, gender or ethnicity be collected without linking that to a particular individual? The institution still is guaranteed authenticity, but there is no risk of linking the data to a specific individual. This collection procedure is not appropriate for every situation, but when appropriate policymakers should investigate its possible usage.

Solution 3: Secondary Use

What makes the data interesting is often not a single item, but the correlations and compilations of data across collectors and databases. Technology, notably data-mining,

allows people to find interesting patterns and predict behavior. Who's likely to default on a loan? Buy life insurance? (Dyson, 1998)

The principle of secondary use means that data should be used only for the purpose for which it was collected (or a compatible purpose), unless the individual has given additional consent. Data mining and sorting information in new ways is now not only possible but may seem essential as institutions seek to better serve students (CAUSE, 1997). Even so, institutional policymakers need to consider that every time information is combined to create new information the question of consent and notification becomes an issue. Has the individual consented to the use and release of this new information?

Again, federal policymakers need to closely examine their own secondary use practices as related to student privacy. The passage of the Taxpayer Relief Act of 1997¹⁰ created the Hope Scholarship and Lifetime Learning Credits. The credits allow taxpayers to claim a nonrefundable credit against their federal income taxes for certain higher education expenses. The law requires postsecondary institutions to provide to the IRS each student's 1098-T form, which includes the student's name, social security number and amount spent on tuition. The Act's reporting requirements apply to *all* students who have paid tuition or related expenses to a postsecondary institution, even if that student did not apply to receive the tax credit. This information (including SSN) is reported to the IRS without the student's prior consent. In other words, even if Student A does *not* want to claim the credit, she still has to transmit personally identifiable data to the IRS without her explicit consent.

Solution 4: Privacy-enhancing Technologies

In addition to the blind signature technology described above, a number of developing technologies may provide solutions to improved privacy by creating secure and authentic transmission of data. There are typically three types of authentication mechanisms: something you know, something you have, or something you are.

- **Firewalls** are devices that restrict access between an internal network and a public network. A firewall may be used between the main Internet interface and a particular department. Consequently, only authorized users are allowed to interact with the internal computer.
- **Encryption** is important to protecting confidentiality and integrity of data when that data is being transmitted through unsecured public networks. There are two kinds of cryptographic systems: secret key and public key. In encryption, there is an element of the encryption process that can be known by all – the public key. There is also an element that is private and can not be shared – the user's secret key. If an individual wants to send a secure message, she encrypts the message (basically “scrambles” the data) and the recipient can decrypt or unscramble the data using the secret key.
- **Token and smart cards** were developed to overcome the problems associated with reusable passwords. With a smart card, authentication to a computer or network resource is based not only on something you know but also on something you have (the card itself). This technology could also be used anonymously.

The Train is Headed Down the Proverbial Track

Privacy. What it is, how it is defined, and what it means are all debatable. What is clear is that Americans are concerned about their own and that politicians are taking notice.

By early April 2000, fifty legislative proposals addressing privacy had been offered in both the U.S. House and Senate (Hatch, 2000). A recent Harris poll shows that concern is rising over privacy on the Internet, 92% expressed discomfort about web sites sharing personal information with other sites (BusinessWeek, 2000). In February 2000, two republicans (Sen. Richard Shelby [R-AL] and Rep. Joe

Barton [R-VA]) joined with two democrats (Sen. Richard Bryan [D-NV] and Rep. Ed Markey [D-MA]) to form the first-ever Congressional Privacy Caucus. Also formed was a Senate Democratic Privacy Task Force headed by Sen. Patrick Leahy of Vermont (Privacy Times, 2000). And when Phyllis Shchlaflay (Eagle Forum), Nadine Strossen (ACLU) and Ralph Nader join forces to lobby for privacy rights, you know you have a hot button issue (Ota, 2000).

There is no question that privacy concerns are rising because of the potential and real abuses that have occurred recently: identity theft, concerns about medical records, unsolicited email advertisements, credit card commerce and theft, breaches in email security, viruses and worms. The pressure is on. In an age when information is worth a significant amount of money and power, both government and private industry are struggling with just how to ensure privacy without stifling the growth of technology.

In many ways, educational institutions are ahead of the curve. They have had information and record-keeping regulations in place for the past 25 years. But, it is time to take a look at those regulations and policies and bring them up to date. FERPA is not keeping pace. The law has been amended six times, which created its 14 exceptions to the prior written consent rule. Exceptions have been created to deal with campus crime, binge drinking, and law enforcement. Ironically, the most specific provisions in the legislation *are* the exceptions to its requirements (Privacy Protection Study Commission, 1977). Not only has the law been excepted, but numerous federal laws have been enacted since FERPA's passage that are at cross-purposes with the FERPA regulations. The passage of the Taxpayer Relief Act of 1997 and the Solomon Amendment¹¹ may be politically legitimate, they may even be legitimate from a public policy standpoint; but the impact that the legislation would have on privacy was not an issue of debate. It is only after the laws are passed that the question of how to "comply" with FERPA are addressed¹².

As the privacy debate heats up, student privacy will inevitably come into play. Over the last 30 years, the U.S. has taken a sector approach to privacy protection. Now privacy advocates are calling for an omnibus approach¹³. Institutions should not sit by and wait for information policies to be passed that are then applied to higher education as an afterthought. That happened the first time around in FERPA. That is also what is happening with the recent passage of the Gramm-Leach-Bliley "Financial Services Modernization" Act. The law, passed in November 1999, enables financial institutions to share personally identifiable information among affiliates. Consequently, the Federal Trade Commission issued privacy regulations associated with the law. The FTC has maintained that, for the purposes of the G-L-B law, colleges are "financial institutions" because they administer student loans, and should be subject to the privacy regulations the agency has issued. The higher education community, however, is arguing that FERPA has provided enough privacy protection for student financial and other records (ACE, 2000).

It is clear that institutions do not want to see themselves in a position like that under the G-L-B Act. They do not want to struggle with privacy provisions that are overly broad or redundant. Instead, educational policymakers and legislators need to agree on privacy policies that are balanced and flexible. Policies that are based on a code of fair information practice that is applicable to today's environment.

It is time for policymakers to take a good look at privacy policies outside the FERPA box. It is no longer enough to just "comply" with FERPA. FERPA is ready for an overhaul. The exterior of the law is a complex web of regulations. But, exceptions, new legislation and an outdated understanding of personal privacy protection have gutted the Act.

New technology has not caused a crisis in privacy. New technology has caused consumers and policymakers to become increasingly aware of the delicate line we walk when we discuss privacy.

The train is headed down the track and it is picking up steam.

References

Agre, P. & Rotenberg, M. (Eds.). (1998). *Technology and Privacy: The New Landscape*. Cambridge, MA: The MIT Press.

Alderman, E & Kennedy, C. (1995). *The Right to Privacy*. New York: Alfred A. Knopf.

American Association of State Colleges and Universities. (2000, April). Educational Records and Privacy Rights: A New Battleground for the Information Revolution? *AACRAO Data Dispenser*. Washington, DC: AACRAO.

American Association of State Colleges and Universities. (2000). *Hope and Lifetime Learning Credit Reporting Requirements* [On-line]. Washington, DC: AACRAO. Available: <http://www.aacrao.org>

American Association of State Colleges and Universities. (2000). *Practical Online Guide to the Family Educational Rights & Privacy Act* [On-line]. Washington, DC: AACRAO. Available: <http://www.aacrao.org>

American Council on Education. (2000, March 31). Letter to FTC on Gramm-Leach-Bliley Act Privacy Rule. Available: <http://www.aacrao.org>

Banisar, D. (1994). Privacy of Education Records. *Electronic Privacy Information Center* [On-line]. Available: <http://www.epic.org>

Brin, D. (1998). *The Transparent Society*. Reading, MA: Addison-Wesley.

BuisnessWeek. (2000, March 20). It is Times for Rules in Wonderland. *BusinessWeek Online*. Available: http://www.businessweek.com/2000/00_12/b3673001.htm

CAUSE. (1997). *Privacy and the Handling of Student Information in the Electronic Networked Environments of Colleges and Universities*. Boulder, CO: CAUSE.

Cavoukian, A. (1996). Go Beyond Security – Build in Privacy: One Does not Equal the Other. *Cardtech/Securtech 1996 Conference* [On-line]. Available: http://www.eff.org/pub/Privacy/960514_cavoukian_priv-sec.speech

Dyson, E. (1998). Privacy Protection: Time to Think and Act Locally and Globally. *First Monday* [On-line]. Available: http://www.firstmonday.dk/issues/issues3_6/dyson/

Family Policy Compliance Office. (2000) *Legislative History and Major FERPA Provisions* [On-line]. Washington, DC: U.S. Department of Education. Available: <http://www.ed.gov/offices/OM/fpco/Legislativehistory.html>

Ferencz, S.K. & Goldsmith, C.W. (1998). Privacy Issues in a Virtual Learning Environment. *CAUSE/EFFECT*, 21 (1), 5-11.

George, B. (1978). The Buckley Amendment. [American Association of Collegiate Registrars and Admissions Officers Conference Paper]. 25-39.

Hatch, O. (2000, March 27). What is the Best Way to Ensure Online Privacy? *Roll Call* [On-line]. Available: <http://www.rollcall.com>

- Henderson, H. (1999). *Privacy in the Information Age*. New York: Facts on File.
- Hoffman, L.J. & Metivier Carreiro, K. (1997). Computer Technology to Balance Accountability and Anonymity in Self-regulatory Privacy Regimes. *Privacy and Self-Regulation in the Information Age*. Washington, DC: National Telecommunications and Information Administration. Available: http://www.ntia.doc.gov/reports/privacy/privacy_rpt.htm
- Kaplin, W.A. & Lee, B.A. (1995). *The Law of Higher Education*. San Francisco: Jossey-Bass Publishers.
- Lemmey, T. (1999). Architecture is Policy. *Electronic Frontier Foundation* [On-line]. Available: http://www.eff.org/pub/Privacy/19990406_Eff_MS_P3P_Paper/
- Masci, D. (1998, November 6). Internet Privacy. *The CQ Researcher*, 8 (41), 955-975.
- O'Brien, D. M. (1979). *Privacy, Law, and Public Policy*. New York: Praeger Publishers.
- Office of Information and Privacy. (1998). *Overview of The Privacy Act of 1974* [On-line]. Washington, DC: U.S. Department of Justice. Available: http://www.usdoj.gov/foia/04_7_1.html
- Ota, A. (2000, March 25). Internet Privacy Issue Beginning to Click. *CQ Weekly* [On-line]. Available: <http://www.cq.com>
- Privacy Protection Study Commission. (1977). *Personal Privacy in an Information Society: The Report of the Privacy Protection Study Commission*. Washington, DC: Government Printing Office.
- Privacy Times. (2000, February 18). Fearsome foursome Forms Congressional Privacy Caucus. *Privacy Times* [On-line]. Available: www.privacytimes.com
- Rainsberger, R. (1998). *Guidelines for Postsecondary Institutions for Implementation of the Family education Rights and Privacy Act of 1974 as Amended*. Washington, DC: AACRAO.
- Rhinehart, P.T. (1996, Spring). The Use of Electronic Data Interchange Under the Family Educational Rights and Privacy Act. *CAUSE/EFFECT*, 34-39.
- Rotenberg, M. (1998, March 26). *Testimony and Statement for the Record on Communications Privacy* [On-line]. Subcommittee on Courts and Intellectual Property House Judiciary Committee. Available: <http://www.epic.org/privacy/internet/rotenberg-testimony-398.html>
- Rotenberg, M. (1998, May 7). *Testimony and Statement for the Record on the European Union Data Directive and Privacy* [On-line]. Committee on International Relations, U.S. House of Representatives. Available: <http://www.epic.org/privacy/internet/rotenberg-testimony-598.html>
- Smith, H.J. (1994). *Managing Privacy: Information Technology and Corporate America*. Chapel Hill: the University of North Carolina Press.
- U.S. Congress. (1976, June 3). *Congressional Record, Senate* (122:81). Statement by Senator James L. Buckley on K. Cudlipp's "The Buckley Amendment Two Years Later". p. S8482.

U.S. Department of Health, Education, and Welfare. (1973). *Records, Computers, and the Rights of Citizens; Report of the Secretary's Advisory Committee on Automated Personal Data Systems*. Washington, DC: Government Printing Office.

Yudof, M., Kirp, D. & Levin, B. (1992). *Educational Policy and the Law*. West Publishing Co.

¹ In 1969, the Russell Sage Foundation drew up a comprehensive set of record-keeping guidelines and the National Education Association called for record-keeping reform. (George, 1978). Additionally, due to the Watergate scandal break-in and cover-up in 1972, Congress was concerned with curbing the illegal surveillance and investigation of individuals by federal agencies. Privacy advocates were concerned with the potential abuses of the government's increasing use of computers to record personally identifiable data, especially when that data could be connected to an individual's unique Social Security Number. (Office of Information and Privacy, 1998)

² Since FERPA was offered as an amendment on the Senate floor and was not the subject of committee consideration, traditional legislative history as first enacted is unavailable. The major source of legislative history for the amendment is contained in the explanation of the Buckley/Pell Amendment in the December 13, 1974 *Congressional Record*, pages 39862-39866.

³ The Code of Fair Information Practices was developed by the Department of Health, Education, and Welfare's Advisory Committee on Automated Data Systems. The Committee, established in 1972, was charged with analyzing how the government would collect and maintain data, especially medical records. Its Code of Fair Information Practices laid the foundation for almost every privacy bill that followed it. It is still viewed today as the model that government, institutions, and private industry should maintain when dealing with personally identifiable information. These principles were later adopted by the Organization for Economic Cooperation and Development in their formulation of *Guidelines for the Protection of Personal Data and Transborder Data Flows*.

The Code of Fair Information Practices is based on five principles:

1. There must be no personal data record-keeping systems whose very existence is secret.
2. There must be a way for a person to find out what information about the person is in a record and how it is used.
3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.
4. There must be a way for a person to correct or amend a record of identifiable information about the person.
5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data. (U.S. Department of Health, Education and Welfare, 1973)

⁴ Educational records are considered any record that contains information directly related to a student and are maintained by an educational agency or institution or by a party acting for the agency or institution. This term has a very broad scope. Any information that makes a student personally identifiable, such as an ID number or home address, is considered an educational record. (34 C.F.R. § 99.3) Records which fall outside of this definition include: sole possession records; records created and maintained by a law enforcement unit for a law enforcement purpose; employment records (unless contingent upon attendance); medical records made and maintained in connection with treatment; Records containing information about an individual which is created after he/she is no longer a student at that institution.

⁵ See U.S.C. § 1232g and 34 C.F.R. § 99.

⁶ See 34 C.F.R. § 99.3. Directory information can contain: name, address, email address, telephone listing, field of study, weight and height of athletes, most recent previous school attended, photographs, date and place of birth, participation in officially recognized activities and sports, dates of attendance, degrees, and awards. Directory information **cannot** include: Student identification numbers; Social security numbers; Ethnicity/race/nationality; or gender.

⁷ FERPA has been amended a total of six times since its passage, creating 14 exceptions to the prior written consent rule: December 1974 (Buckley/Pell Amendment); August 1979; November 1990 (Campus Security Act); July 1992; October 1995 (Improving America's Schools Act); and October 1998 (HEA of 1998).

As originally enacted, there were five exceptions to the prior written consent rule. Educational records may be released: (1) To school officials who have legitimate educational interests; (2) To other schools or school systems in which the student intends to enroll; (3) To authorized representatives of the Department of Education, Comptroller General, or State educational authorities; (4) In connection with a student's application for or receipt of financial aid; and (5) In compliance with a judicial order or pursuant to any lawfully issued subpoena. In December 1974 five additional exceptions were adopted almost immediately after the original enactment: (6) A grandfather clause was included for states that required certain data collection; (7) Educational records could be released to organizations conducting studies for the purpose of developing, validating or administering predictive tests, administering student aid programs and improving instruction as long as the studies conducted did not permit the personal identification of students and that the information would be destroyed when it was no longer needed; (8) Information could be released to accrediting organizations; (9) Information could be released to parents of dependent students; (10) Information could be released in connection with an emergency. In 1990, with the passage of the Campus Security Act, another exception (11) was provided which allowed postsecondary institutions to disclose to an alleged victim of any violent crime the final results of any disciplinary proceeding conducted against the alleged perpetrator. In 1995, IASA added a new exception (12) for law enforcement purposes that allowed release of data to the designee of a federal grand jury subpoena or other subpoena. In the 1998 HEA amendments the following exception was added: (13) postsecondary institutions may disclose the final results of any disciplinary proceedings for a crime of violence or nonforcible sex offense to anyone (including the public) if the institution determines that the student committed a violation of its rules or policies with respect to the crime. The 1998 HEA amendments also added a new exception (14) that allowed institutions to disclose to a parent or legal guardian information regarding a student's alcohol or substance abuse violation if the student is under 21.

The number of exceptions gives one pause. The exceptions have become more specific than the law itself. The Privacy Act of 1974 has not fared any better, however. That law has also been amended six times and has 12 exceptions.

⁸ Athletic Participation and Financial Support (EADA) data must be reported to the U.S. Department of Education.

⁹ Required by the 1998 HEA Reauthorization.

¹⁰ See P.L. 105-34 § 25A.

¹¹ With the enactment of the Solomon Amendment in 1996, institutions were required to provide directory-type information on students, upon request from representatives of the Department of Defense for military recruiting purposes. According to the law (regulations have been modified), the institution must provide the information even if the student has opted for nondisclosure. In addition, directory information that is provided to DOD regarding students, is not the same information as FERPA mandates as acceptable directory information.

¹² See Director of the Family Policy Compliance Office letter regarding FERPA and the Taxpayer Relief Act. Available: <http://www.ed.gov/offices/OM/hope.html>.

¹³ Privacy advocates like Marc Rotenberg, Director of the Electronic Privacy Information Center and an Adjunct Professor at Georgetown University Law Center, have advocated that the sectoral approach to privacy policy is not working. For example, we have federal privacy laws for video records but not for medical records. There are federal privacy laws for cable subscriber records but not for insurance records. Although advocates and lawmakers are focusing their concerns on private industry, the possibility of creating an omnibus Internet privacy bill is real. This bill could then be easily applied to higher education institutions.