Chapter 1

FERPA and the Regulatory Universe of Privacy

WHEN THE FEDERAL Family Educational Rights and Privacy Act (FERPA) was germinating in the legislative consciousness of Washington, the nation—and, indeed, the entire world—was immersed in an intense dialogue and heated debate about how to manage the explosion of information and data in every facet of government, business, and industry.

Who was keeping information about private individuals? How were they storing, maintaining, and releasing that information? What rights allowed them to do so? And what rights did private citizens have in this escalating inundation of unsupervised and unregulated data and information?

> *No one shall be subject to arbitrary interference with his privacy, family, home, or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to protection of the law against such interference or attacks.*
>
> —UNIVERSAL DECLARATION OF HUMAN RIGHTS, *United Nations, 1948*

From the global and national discourse on privacy, legislation emerged in the United States that, however different in format from its European counterparts, sought to establish and ensure universal tenets for information and records management that would impact every sector of our society.

For the higher education community, FERPA has had the dominant impact. But as American society and campus operations have become increasingly complex, other legislation has affected institutional policy and procedure so that a thorough understanding and appreciation of the privacy debate is necessary to ensure comprehensiveness and compliance in our daily practice and work responsibilities.

Toward the Codification of Privacy Rights

The Constitution of the United States recognizes the privacy of United States citizens as an inalienable right, both explicitly and implicitly. The Fourth Amendment codifies the right of individuals "to be secure in their persons,

Wheaton v. Peters

Wheaton v. Peters, in 1834, is considered the first ruling by the U.S. Supreme Court on copyright. The case involved two reporters of the courts in Pennsylvania—Henry Wheaton and his successor, Richard Peters. Wheaton had compiled court rulings, arguments, and summations in a set of 24 volumes for use by attorneys. When Peters took over, he continued to provide the same service but streamlined the content of Wheaton's earlier work. Reduced to just six volumes of materials, Peters' less expensive work quickly became more popular than Wheaton's.

After Wheaton sued Peters in the Pennsylvania courts and lost, he appealed his case to the Supreme Court. The Supreme Court, however, upheld the lower court's ruling and, in essence, created legislation regarding copyright that set written work apart from patents for inventions and other creations. The Court upheld the property of writers but also held that individuals could not hold copyrights on the decisions and rulings of the court system.

houses, papers, and effects, against unreasonable searches and seizures" and goes on to set limits and specifications for such searches and seizures. Privacy advocates have also used the First Amendment right to free assembly and provisions in both the Ninth and Fourteenth Amendments to further base legal challenges supporting the privacy of individuals.

In 1890, attorneys Samuel Warren and Louis Brandeis, founders of the distinguished Boston law firm Nutter, McClennan, & Fish, published an article in the *Harvard Law Review* entitled "The Right to Privacy." In addition to coining the expression "the right to privacy," the article is considered the first publication to argue for individual privacy and to advocate for legislation that would provide legal protections and remedies against the invasion of privacy. Warren and Brandeis incorporated the phrase "the right to be let alone" in their text, quoting the 1834 Supreme Court case of *Wheaton v. Peters* and *A Treatise on the Law of Torts,* a 1888 textbook by T. M. Cooley. In these initial platforms on privacy, the contention was generally viewed as one between the private individual and government.

In fact, the dialogue on privacy has frequently focused on the relationship between government and private citizens. Historians often summarize the immigration to the New World as an escape from a European system that was attempting to fetter the private citizen and deprive him of personal and public freedoms. Against the prospect of such tyranny and control, the American Revolution was waged and a new nation forged.

As American society evolved, the fledging nation would experience and be forced to deal with many of the same challenges that have faced governments since the dawn of civilization. With advances in industry,

technology, and business practice, the privacy debate would arise again in a new context.

In the years following World War II, distrust and suspicion swelled across America in response to widespread government initiatives to conduct national census activities. The compilation of a massive database about private citizens raised fear and anxiety about the potential misuse of such data. European immigrants, in the shadow of the Holocaust and the attempted extinction of the Jews, were wary of government interest in ethnicity and religious affiliation. In truth, memories were still all too recent regarding the branding, stamping, and tattooing practices inflicted upon prisoners in the Auschwitz concentration camp complex. The post-World War II population of the United States included many, citizen and refugee alike, who had witnessed or escaped the crimes of Nazi Germany.

The introduction and use of any type of national identification system in the United States was an understandable cause for concern. After all, even in the United States, ethnic identification efforts had already been used to locate Japanese immigrants for relocation and internment during the Pacific conflict.

In the wake of World War II, Europe had quickly organized efforts to protect the privacy of citizens against big government. In 1970, the German centralization of computer records regarding citizens spawned the first privacy laws. Sweden passed the first national data protection law in 1973 and initiated a process to issue national identity (ID) cards. A similar initiative was launched in Great Britain as England centralized the issuance of national drivers' licenses.

As country after country embarked upon its own privacy legislation, it became apparent to the Europeans that national initiatives would soon impact international economic trade. A British company that had applied to produce magnetic stripes for Sweden's ID cards was denied the contract because in Sweden's evaluation, British law did not provide sufficient protections for the privacy of information about Swedish citizens. To facilitate trade and commerce among the European nations, an initiative was launched to establish international agreements on privacy, trade, and communication.

On January 28, 1981, the Council on European Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data came together in Strasbourg, France, setting into motion the events that would lead to the first international law on data protection. The Data Protection Act was ratified and enacted on October 1, 1985, in France, Germany, Norway, Spain, and Sweden. Other Europeans countries would

Council of Europe

The Council of Europe was founded in 1949 with the objective of promoting and facilitating unity among the nations of Europe. The council's specific goal is developing throughout Europe "common and democratic principles based on the European Convention on Human Rights."

Headquartered in Strasbourg, France, the council comprises 47 member countries. The council also claims five observer countries: the Holy See, the United States, Canada, Japan, and Mexico.

The council's website is www.coe.int.

subsequently follow. Then, in 1995, the European Union's Data Protection Directive was adopted.

Despite the national and international legislative developments, however, it soon became apparent, through assessments and surveys conducted throughout Europe, that individual citizens remained unaware of their personal rights and protections. This was a tremendous concern for the Council of Europe, which had incorporated public education into its mission.

On January 28, 2007, the first Data Protection Day was held throughout Europe. Organized by the Council of Europe, the intent of the celebration was to commemorate the beginning of dialogue on privacy and individual protections and to educate citizens throughout the continent about their rights. Individual member nations were encouraged to determine, budget for, and sponsor educational and social events for their citizens. The council's website was used as an organizational base to compile a listing of events throughout Europe and to promote unity for the multinational initiative.

The Adoption of Fair Information Practices

With the exception of some European influences, the story of privacy in America took a somewhat different course.

It was a long time before the work of Warren and Brandeis would significantly impact legal thought in America. Despite foundations in the U.S. Constitution, privacy was essentially left to state and local courts, leading to inconsistencies across court jurisdictions. In many views, privacy was understood as a personal right, one that ends with the death of an individual and one that only generated legal action when an invasion of privacy was determined to have occurred. Because privacy was viewed as

Louis Dembitz Brandeis

Born in 1856 in Louisville, Kentucky, Louis Dembitz Brandeis was an attorney, Supreme Court Justice, and prominent advocate for free speech, privacy, women's rights, trade unions, and the minimum wage.

Attending schools in Louisville and Dresden, Germany, Brandeis graduated from Harvard University. He practiced law in Boston before being appointed to the U.S. Supreme Court by President Woodrow Wilson in 1916. He was the first Jewish Supreme Court Justice in U.S. history and was the leader of the American Zionist movement. In addition to influencing Wilson's New Freedom economic doctrine, Brandeis published two important works in 1914: *Other People's Money and How the Bankers Use It* and *Business–A Profession*.

Upon his death in 1941, Brandeis was cremated and his remains were transported to the Louis D. Brandeis Law School at the University of Louisville, where many of his personal files are archived. In 1948, Brandeis University was founded in Waltham, Massachusetts, and named in his honor.

a personal right, corporations and partnerships were judged to possess no particular right to privacy.

These premises would be challenged over the years through cases that would be heard by courts at every level. It was not until *Olmstead v. United States* that Brandeis would once again incorporate the phrase "the right to be left alone" in his legal arguments. From those 1928 proceedings, the first wiretapping case heard by the U.S. Supreme Court, concerns about privacy exploded, eventually expanding beyond mere protection against government inquiry.

In 1965, a Special Inquiry on Invasion of Privacy was convened by the U.S. House of Representatives. The House Committee on Government Operations examined a diverse variety of activities where the privacy of citizens could potentially be invaded and violated. The areas probed focused upon operations within the federal government, including the psychological testing of employees and applicants, the use of data from farm census questionnaires, and the confidentiality of federal investigations, employee files, and income tax returns. The committee's scrutiny extended to an examination of surveillance practices at government facilities, including electronic eavesdropping, mail deceptions, prying into private trash, and even to the existence of strategic peepholes.

Underlying those discussions in the mid-1960s was the emerging realization that, with the advent of computers and technology, the stage was being set for the formation of a national database on U.S. citizens. With personally identifiable information (PII) about individuals being systematically collected by a number of federal agencies, it would not be difficult

or inconceivable to compile, collate, and index data to create extensive and comprehensive profiles about private citizens.

> *The real danger is the gradual erosion of individual liberties through automation, integration, and interconnection of many small, separate record-keeping systems, each of which alone may seem innocuous, even benevolent, and wholly justifiable.*
>
> —US PRIVACY STUDY COMMISSION (1977)

Agencies were already using social security numbers (SSN) as an index. Establishing the SSN as a "standard universal identifier" (SUI) would facilitate the creation of a national database and its speedy population

Social Security Numbers

The social security number (SSN) was established in 1936, when the New Deal Social Security Program was enacted through the Social Security Act (42 USC §405(c)(2)). Initially established as a means to track individual accounts within the Social Security Program, the number has since become a national identification (ID) number, beginning with its usage by the U.S. Army and the Air Force in 1969.

Initially, individuals did not need an SSN until the age of 14 or when an individual could first participate in the work force and file federal income taxes. By 1986, the minimum age was lowered to 5, since dependent children could be claimed on federal income tax forms. By 1990, age 1, or as soon as possible after birth, became the norm for procuring an SSN.

The nine-digit structure of the SSN is delineated AAA-GG-SSSS. The AAA, or area number, refers to a geographical region, not necessarily a state. By 1973, area numbers were based upon zip codes. The group number (GG) is used to provide natural breaks in blocks of allocated numbers. The SSSS is the serial number assigned to specific individuals. There are some number structures that are not used in the SSN. These include all zeroes in any one of the numbers groupings, numbers beginning with 666, and certain number sequences that have been set aside for advertisement purposes.

Social security accounts were established to provide for the economic welfare of citizens. The first laws for public welfare date back to the English Poor Law of 1601, which the colonists brought with them to the New World. In his last pamphlet, *Agrarian Justice,* Thomas Paine, in 1795, argued for the establishment of a public system to provide economic security for citizens. But the first systematic program was not devised until 1862 when legislation established the Civil War Pension Program, designed to care for soldiers after the war and for the widows and children of disabled soldiers. Despite numerous amendments through the early 1900s, the program was never extended to the general public.

As far back as 1862, company pension programs sought to address economic security for workers. The Alfred Dolge Company, a producer of pianos and organs, was one of the first to establish such a program. As late as 1932, however, less than 15% of the work force was covered by any type of pension program.

The Social Security Program began making its first payments in 1937, initially in single, lump sums to the beneficiary. In 1939, an amendment to the Social Security Act established the monthly payment system, which has been in use since 1940.

with vital and confidential information. No one could be sure about how much data sharing was occurring between agencies of the federal government. And given the fact that the government was comprised of numerous agencies, who would challenge the appropriateness of such information sharing, especially since it was all supposed to be one government?

The availability of information, questions about the transmission and access of data, and the security of information were issues that cried out for answers and raised concerns for many citizens. But in the early and mid-1960s, an organized platform for dialogue and activism was essentially nonexistent in the United States. A model would soon emerge from Europe, however, where international commerce would drive the discussion and compel the first privacy laws regarding personal information.

Concerns about privacy, databases, and information access continued into the next decade. As already mentioned, privacy became a global concern that expressed itself in different ways and in a variety of arenas—in medical, financial, commercial, and communications.

In Europe, Sweden took the lead with strategies and dialogue that evolved into the adoption of what became known as the Fair Information Practices. Privacy Commissioners were soon designated in a number of European countries, as well as in Canada, Australia, New Zealand, Japan, and Hong Kong.

The Fair Information Practices would strongly influence the development of privacy legislation in the United States. Among the privacy discussions taking place in the early 1970s was one that focused on the privacy of medical records in the wake of mounting computerization. A task force was convened under the direction of the U.S. Department of Health, Education, and Welfare (HEW) and, in 1973, it issued a report entitled "Records, Computers, and the Rights of Citizens."

The HEW report is significant in the development of and its influence on privacy legislation in the United States. Its achievements included the following.

- *Code of Fair Information Practices.* The report established a Code of Fair Information Practices, based upon practices developed and established in Europe. This code set the standards and defined benchmarks for best practices in privacy legislation and records and information management.
- *Privacy Legislation***.** The report recommended that Congress pass legislation to adopt the code for all organizations maintaining automated personal data systems. The recommendations included not only requirements for the documented specification of protections

and safeguards but a mandate for annual disclosures of policy and practice to the public.

- *Restrictions on Using the Social Security Number*. Concerned with the potential of using the SSN to establish a standard universal identifier (SUI), the report recommended that the SSN should be used only where absolutely necessary or where existing legislation already required the use of the SSN. Further, the report stipulated that no citizen should be compelled to provide an SSN unless required by Congressional ruling.

All of these provisions directly influenced the passage of the Privacy Act of 1974, as well as the numerous privacy regulations that followed. Of prime importance was the codification of the Fair Information Practices, not only as a precursor to subsequent privacy legislation and records management initiatives but as a qualification of the United States' participation in the global economy.

The U.S. Code of Fair Information Practices

The 1973 HEW task force identified five key components in its Code of Fair Information Practices. A generation after their adoption, these practices may seem logical and self-evident. However, one must remember that the political, economic, and technological climate of the early 1970s was a very different landscape from that of our 21st century. The code not only influenced subsequent privacy legislation but provided a solid foundation for best practice and for determining policy and procedure in records and information management in nearly every U.S. industry.

A brief examination of the Code of Fair Information Practices will contribute to a deeper understanding of FERPA as well as provide some guidance for policy development strategies in all areas of college and university administration.

The first two Fair Information Practices are a prohibition against secrecy and a mandate to disclose the existence of a database and its contents to the population about whom the database is compiling information. Any entity that collects and maintains personally identifiable information about individuals must disclose to its clients and to the public the fact that information is being collected. Recordkeeping systems cannot remain secret or private. Individuals have a right to know that information is being kept about them—and, moreover, to know *what* information is being collected and how that information is being used.

The third tenet is designed to prevent secondary or "further disclosure" of collected information. Further disclosure refers to the release of information beyond the recordkeeper, beyond those authorized to access the

CODE OF FAIR INFORMATION PRACTICES

- *Database Existence*. A recordkeeping system that compiles and stores personally identifiable information about individuals must not be kept secret.
- *Primary Usage*. Individuals whose personally identifiable information is being collected and stored have a right to know what information is being kept and how it is being used.
- *Secondary Usage*. Individuals must be able to prevent recordkeepers from disclosing personally identifiable information about themselves without their consent.
- *Amendments*. Individuals must be able to correct or amend personally identifiable information that is being stored about them.
- *Security Protections*. Organizations that collect and store personally identifiable information about individuals must ensure that data will only be available for internal use and must take precautions to prevent the misuse of that data.

data, including the individual identified by the data. Entities that gather or receive data cannot use the information for anything other than for the purpose that was initially disclosed to the subjects of the data. In order to disclose information for any other purpose, the recordkeeper must first obtain the consent of the individual or individuals identified by the data.

Because nothing is perfect, and because inaccurate or incorrect data can easily make its way into any information system, individuals have a right to seek to amend the information that is being kept about them. This fourth practice implies that individuals must have some access to inspect the information that is being collected about them. Otherwise, how would individuals become aware of inaccuracies? More to the point, the code advocates distinct processes that allow individuals to request amendments to the content of records that are being maintained.

Lastly, recordkeepers have a responsibility to provide security protections for the data they keep. They must ensure that the information collected will only be used for the purposes disclosed. Further, they must take the necessary precautions to prevent the misuse, misappropriation, and unauthorized access of data. Initially, these security concerns focused on physical access. By the end of the 20th century, however, electronic access would create the need for technological and virtual protections as well.

All of these practices are represented in the Privacy Act of 1974 and are evident in subsequent U.S. privacy legislation, such as the Fair Credit Reporting Act and FERPA.

The Privacy Act of 1974

On the heels of the HEW report and the country's adoption of the Code of Fair Information Practices, both the U.S. House of Representatives and the U.S. Senate entertained separate and distinct legislative debates on privacy. Both were narrowly focused on the privacy of information that was being collected and maintained by agencies of the federal government. And both produced two somewhat different proposals for privacy in America.

HR 16373 was the proposal initiated in the House of Representatives, while S 3418 represented the Senate's effort. While the Senate bill was viewed as the more rigorous in its requirements, the House bill was criticized as harsher in its application of consequences or penalties. The House bill required that damages or penalties could only be assessed against the government if a violation was demonstrated as "willful, arbitrary, or capricious." But the House bill also proposed the creation of a Privacy Protection Commission to oversee the implementation and enforcement of its legislation.

> *The privacy and dignity of our citizens [are] being whittled away by sometimes imperceptible steps. Taken individually, each step may be of little consequence. But when viewed as a whole, there begins to emerge a society quite unlike any we have seen—a society in which government may intrude into the secret regions of a [person's] life.*
>
> —ASSOCIATE JUSTICE WILLIAM ORVILLE DOUGLAS

The bill that President Gerald Ford signed in December 1974, and which passed into law the following year, was a compromise between the proposals of the House and the Senate. The Senate passed the amended legislation, known as the Privacy Act of 1974, on December 17. It was ratified the next day by the House of Representatives.

The Privacy Protection Commission, originally proposed by the House bill, was reduced to a Privacy Protection Study Commission, with only advisory responsibilities. It had neither oversight nor enforcement authorities. In 1977, however, the commission published its "Personal Privacy in an Information Society" report, detailing its concerns regarding inadequacies of the Privacy Act of 1974. Among these was the definition of "system of records," which limited application of the act to systems in which data retrieval was accessed by name, SSN, or some other personal identifier. Further, public disclosure in the act was tied to publication in the government's *Federal Register,* which the commission judged too limited in its circulation and accessibility.

Features of the Privacy Act of 1974 included the following.

Application. The act applied only to certain agencies of the federal government and had no impact on state and local governments. Curiously enough, although the Office of the President was covered by the act, the act applied to neither the House nor the Senate.

Appeals for Amendment. Assuring individuals that they can seek to amend records, the act stipulated that if a request for amendment is refused, the recordkeeper must advise the individual of an appeal process and allow 30 days for an appeal to be submitted. Individuals may also provide a statement to the recordkeeper detailing their objections to any record and that statement must be retained and disclosed by the recordkeeper whenever the disputed record is disclosed.

Disclosures without Consent. The act detailed exceptions to its requirement of prior consent for further disclosure of information beyond the purpose for which the data was initially collected. Among the exceptions is one for "routine use" by government agencies, which critics claim has been abused over the years.

Retention Requirements. To ensure an audit trail, records of disclosures must be retained for a period of five years. With the exception of records detailing disclosures for law enforcement purposes, these records of disclosure must be made available for inspection whenever requested by the individual identified in the records.

Data Minimization. Agencies must maintain only those records that are "relevant and necessary" to accomplish their purposes. The intent was to prohibit the collection and maintenance of information for which the agency had no right or privilege to maintain.

Data Sharing Limitations. Agencies that share data must do so by written agreement, detailing purposes, legal authority, data matching practices, and other information relevant to the exchange of information. The agreement must be renewed every 18 months and must be made available to the public, the Committee on Government Affairs of the Senate, and the Committee on Government Operations in the House.

Right to Sue. Individuals can sue to have their records amended and can recover reasonable attorney fees and litigation costs from the United States government. Courts can also rule against agencies for any violation of other parts of the Privacy Act if the violation is determined to be "intentional or willful." In addition to reasonable attorney fees and costs, the act specified that individuals could recover no less than $1,000.

Section 1983: Right to Sue

Section 1983 of Title 42 of the U.S. Code has its beginnings in the Ku Klux Klan Act of 1871 and the Civil Rights Act of 1872. Requested of Congress by President Ulysses S. Grant, the legislation was enacted as an emergency measure against the growing racial violence and social unrest that struck the Southern states following the end of the Civil War.

More than a century later, Section 1983 continues to serve as the basis by which citizens enforce their Constitutional rights.

> Every person who, under color of any statute, ordinance, regulation, custom, or usage of any State or Territory or the District of Columbia, subjects, or causes to be subjected, any citizen of the United States or other person within the jurisdiction thereof to the deprivation of any rights, privileges, or immunities secured by the Constitution and laws, shall be liable to the party injured in an action at law, suit in equity, or other proper proceeding for redress.

Criminal Penalties. A number of criminal actions and penalties are defined. Government employees who knowingly and willfully disclose personally identifiable information may be found guilty of a misdemeanor and be fined up to a maximum of $5,000. Agencies may be fined up to the same maximum amount for failure to disclose the existence of their systems of records. In addition, the act provided that anyone who requests records under false pretenses may be found guilty of a misdemeanor and fined a maximum of $5,000.

Use of the SSN. No federal, state, or local agency can require anyone to provide a social security number, unless such disclosure is required by federal statute. Agencies that require individuals to provide an SSN must disclose by what legal authority the requirement is being made.

Oversight. The director of the Office of Management and Budget (OMB) was designated to have oversight authority for the implementation and enforcement of the Privacy Act of 1974.

U.S. Office of Management and Budget

The United States Office of Management and Budget (OMB) is the largest office within the Executive Office of the President of the United States (EOP) and is a cabinet-level office. It performs administrative responsibilities for the White House by overseeing the activities of the many federal agencies. The OMB gathers data for the President's annual budget as well as communicates with the agencies.

The OMB is run by six managers, all of whom are appointed by the President and approved by the Senate. Among the directors are the administrators of the Office of Information and Regulatory Affairs, the Office of Federal Procurement Policy, and the Office of Federal Financial Management.

The OMB's website is www.whitehouse.gov/omb.

Sector Approach to Privacy

Except for the adoption of the Code of Fair Information Practices, the United States embarked upon an approach to privacy that differed significantly from the European approach. Whereas European strategy consisted of comprehensive legislation and the national designation of privacy secretaries or ministers, the U.S. undertook what has been called a *sector approach* to privacy. That is, the development and enforcement of privacy standards in the United States is achieved through a mixture of federal, state, and local legislation as well as through self-regulation within the various sectors of business and industry.

Examples of Privacy Initiatives in the United States

Year	Legislation/Action	Focus
1968	Wiretap Act	Written, oral, and, later, electronic communications
1970	Fair Credit Reporting Act (FCRA)	Accuracy, fairness, and privacy of consumer credit information
1974	Privacy Act of 1974	Personally identifiable information collected and maintained by government agencies
1974	Family Educational Rights and Privacy Act (FERPA)	Privacy of student education records
1996	Health Insurance Portability and Accountability Act (HIPAA)	Portability of health insurance coverage and standards for communication of medical records
1996	Economic Espionage Act	Protection of trade secrets
1999	Gramm-Leach-Bliley Act, or Financial Modernization Act	Protection of consumer information held by financial institutions
2000	Safe Harbor Program	Framework of privacy standards for information exchange proposed to avoid interruptions in business between the U.S. and Europe
2001	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act	Increased government authority to investigate and deter terrorism
2002	Homeland Security Information Sharing Act	Sharing of Homeland Security information with state and local entities
2002	Sarbanes-Oxley Act	Corporate financial reporting and accounting fraud
2003	Fair and Accurate Credit Transactions (FACT) Act	Amendments and enhancements to Fair Credit Reporting Act
2004	Identity Theft Penalty Enhancement Act	Aggravated identity theft established as a federal crime

Each facet of American enterprise has developed its own legislation to address specific issues within its unique operations. Federal regulations were established where economic and informational transactions involved either government recordkeepers or national and international business endeavors. State and local governments developed geographically specific policies and rules that, while limited to a defined jurisdiction, have also contributed to broader debates and inspired adaptations in arenas beyond their original applicability.

California was the first state to establish an Office of Information Security and Privacy Protection, a state agency charged with promoting and protecting the privacy of individual consumers. In 2003, the California Senate passed Senate Bill 1386 (SB 1386), called the California Security Breach Information Act or California Information Practice Act. SB 1386 is directed at all individuals and businesses that conduct operations in the state of California and who collect and manage personally identifiable information about consumers. The bill requires these entities to notify affected individuals whenever there is a breach of their information systems that compromises the personally identifiable information they maintain. Since the enactment of SB 1386 in California, other states have passed similar legislation protecting their own residents.

Another aspect of this sector approach to privacy regulation has been the development of professional associations and organizations to establish standards within their theater of operations and to provide collegial guidance for the promulgation of best practices and ongoing professional development. The American Medical Association (AMA), the American Dental Association (ADA), and the American Bar Association (ABA) are prominent examples of such profession-specific organizations. In some

California Office of Information Security and Privacy Protection

California Senate Bill (SB) 90 created the Office of Information Security and Privacy Protection (www.oispp.ca.gov/) in 2000. The office opened for business in 2001, with two distinct offices, each with a specific purpose.

- The Office of Privacy Protection was created to focus on consumer protections and to monitor consumer privacy.
- The Office of Information Security, which existed as part of the State Department of Finance, focuses on the privacy of data gathered and maintained by state government agencies.

Both divisions encourage adherence to fair information practices.

American Association of Collegiate Registrars and Admissions Officers

The American Association of Collegiate Registrars and Admissions Officers (AACRAO) is an international, nonprofit organization representing professionals in higher education admissions and registration offices. Founded in 1910 as the American Association of Collegiate Registrars (AACR), the association has grown swiftly from its initial group of only 24 higher education professionals.

AACR changed its name to AACRAO in 1949. By 2008, the association boasted 10,000 members from some 2,500 institutions in 30 countries. Across the United States, state and regional associations focus efforts in specific geographical areas.

AACRAO serves its membership in a variety of ways, providing professional development programs, annual conferences, and other events. Business activities also include publications and newsletters, consulting, and legislative interpretation and guidance.

AACRAO has also become a respected source for information on foreign education and evaluations. What began as a cooperative agreement with the U.S. Agency for International Development in 1964 eventually evolved into the creation of an AACRAO-AID Office and finally the Office of International Education Services.

AACRAO is headquartered in Washington DC. The Association's website can be found at www.aacrao.org.

fields, strategy-specific groups have arisen such as the American Society for Training and Development (ASTD) and the Association of Records Management Administrators (ARMA), now ARMA International. The list goes on and on.

Higher education has benefited from the work and contributions of such organizations as the National Education Association (NEA), the American Association of Collegiate Registrars and Admissions Officers (AACRAO) and its regional chapters, the National Association of College and University Business Officers (NACUBO), and the Council on Law in Higher Education (CLHE).

Common threads throughout the development of privacy legislation in the United States have evidenced the widespread impact and influence of the HEW's adoption of the Code of Fair Information Practices and the implementation of standards established for government recordkeeping through the Privacy Act of 1974. In many cases, their influences are direct and immediately apparent, utilizing language and practice that merely translates the original guidance to industry-specific protocols.

It is legislation, records management strategies, and basics of student services administration that finally come together in a national approach for the education sector in the Family Educational Rights and Privacy Act (FERPA).

Council on Law in Higher Education

The Council on Law in Higher Education (CLHE) is a nonprofit organization that provides a variety of resources to higher education leaders in the areas of government legislation, interpretation, and guidance. Founded in 1998 by attorney Daren Bakst, CLHE has published newsletters such as *The Regulatory Advisor* and, in 2004, a collaborative compendium entitled *Privacy in the 21st Century.*

CLHE's website can be found at www.clhe.org. The website includes links to various government branches and legislative bodies as well as extensive search tools for both federal and state government agencies and legislation.

Regulations for Student Records Privacy

In 1974, within the regular proceedings of the U.S. Senate, Senator James Buckley of New York proposed an amendment to the General Education Provisions Act (GEPA). The new section, sometimes referred to as the Buckley Amendment, was formally entitled "Protection of the Rights and Privacy of Parents and Students" and focused on safeguarding the privacy of education records. On August 21, 1974, President Gerald Ford signed into law the federal Family Educational Rights and Privacy Act (FERPA) or the Education Amendments of 1974.

In the canon of U.S. Law, FERPA is codified at 20 USC §1232g and assigned to 34 CFR §99.

The "USC" in the first citation refers to the U.S. Code. FERPA is cataloged at Title 20, Chapter 31, Subchapter III, Part 4, §1232g of the U.S. Code. The U.S. Code establishes the policy from which the regulations flow in the CFR.

"CFR" refers to the Code of Federal Regulations, the catalog of legislative literature approved and passed into law by the federal government. §99, or Part 99, is the particular section of the 34th index or volume that

James Lane Buckley

A one-time hopeful for the Republican presidential nomination, James Lane Buckley hails from New York City, where he was born in 1923. A Yale graduate, Buckley served in the Navy and later worked as a corporate director and vice president. In 1971, as a candidate of the Conservative Party of New York, he was elected senator and served until 1977. Senator Jesse Helms led a group of Republicans who encouraged Buckley to run for president, but the nomination that year went to Gerald Ford.

In 1982, Buckley was named President of Radio Free Europe and held the post until 1985, when President Ronald Reagan appointed him to the U.S. Court of Appeals for the District of Columbia. Buckley served as a federal judge until 2000.

In 1975, Buckley published *If Men Were Angels: A View from the Senate.*

is specifically FERPA. Whenever text in the regulatory language refers to FERPA as a whole, it means 34 CFR §99 and may use the phrase "this part" when referring to itself in its legislative entirety.

References to paragraphs or regulatory citations in sections of the CFR are often prefaced with the legal icon for paragraph or section: §. Once context within a particular CFR is established, as with 34 CFR §99, specific citations to language within the regulations may be indicated as simply §99 and the specific paragraph or line. For example, §99.2 was the citation quoted in the Preface. Throughout this publication, direct quotes from the FERPA regulations are so listed.

Once it was signed by President Ford, FERPA was set to go into effect on November 19, 1974. The new act, however, contained so many ambiguities that numerous questions and concerns about its implications and enforcement were raised—not only by the education community but by the bill's sponsors as well. Taking into account issues raised by institutions, students, and parents, Senator Buckley and his colleague, Senator Claiborne Pell, collaborated on and presented a "Joint Statement in Explanation of the Buckley/Pell Amendment." Passed on December 13, 1974, the Joint Statement amended the original Buckley Amendment and was made retroactive to FERPA's effective date.

As a privacy regulation, FERPA was designed to apply to both K–12 and postsecondary education. The language of the regulations reflects this applicability. But discussion continued about the application of privacy to the K–12 environment, identifying a need for even greater protections since the subjects of K–12 schools were minors. In 1978, the Protection of Pupil Rights Amendment (PPRA), or the Hatch Amendment, was proposed and

Claiborne de Borda Pell

Senator Claiborne Pell is best known to the education community for his efforts in the creation of the Basic Educational Opportunity Grants, or Pell Grants, which he proposed in 1973. A native of New York, where he was born in 1918, he served as its Democratic senator between 1961 and 1997.

A graduate of Princeton and Columbia, Pell went on to serve in the U.S. Coast Guard and the Coast Guard Reserve. For a time, he worked in the U.S. Department of State, serving in Czechoslovakia, Italy, and Washington, D.C. Upon retiring from the Senate, he was appointed as a delegate to the United Nations.

Pell was a strong supporter of education and was the primary force behind the bills that created the National Endowment for the Arts and the National Endowment for the Humanities. He was also an advocate of mass transportation, recognized by the renaming of Newport Bridge to the Claiborne Pell Bridge.

The Pell Center of International Relations at Salve Regina University is named in Senator Pell's honor. He passed away on New Year's Day, 2009.

Protection of Pupil Rights Amendment

The Protection of Pupil Rights Amendment (PPRA) is the privacy legislation at 34 CFR §98 and applies to the K–12 segment of education that receives funding from the federal government. Passed in 1978 and amended in 2002, the statute is, like FERPA, administered by the Family Policy Compliance Office (FPCO).

PPRA guarantees parental rights to involvement in the decision and policy-making process where surveys and nonemergency physical examinations of students are concerned. Local educational agencies (LEA) are required to notify parents of their policies on an annual basis at the beginning of the school year, disclosing their policies in regard to surveys, educational materials, and physical examinations. Notification within a reasonable time period must also be made whenever there are any changes in policies.

Parents are guaranteed rights under PPRA, including the right to inspect and review educational materials and surveys as well as the right to opt out of or remove their children from participation in any survey. The No Child Left Behind (NCLB) legislation amended PPRA to require parental consent before the administration of surveys that include questions about the student or the student's family in eight specific areas:

- Political affiliations and beliefs
- Religious practices or beliefs
- Mental and psychological problems
- Sexual behavior and attitudes
- Behavior that is illegal, antisocial, self-incriminating, or demeaning
- Critical appraisals of individuals with whom there are close familial relationships
- Privileged relationships—ministers, physicians, lawyers, etc.
- Income

The PPRA is sometimes referred to as the Hatch Amendment.

passed to address the additional concerns in the primary and secondary school environment.

At the same time, the Family Policy Compliance Office (FPCO) was established in the U.S. Department of Education and given responsibility for the administration, interpretation, and enforcement of both FERPA and the PPRA.

Since its passage, FERPA has needed clarifications, amendments, and updates to stay current with the national education scene. For a number of years, little change was made to the FERPA regulations. But then in the 1990s, a series of ameliorations addressed issues of the decade and FERPA concerns in a changing business and social landscape. Some of these changes were focused on specific incidents that drew national attention and affected both FERPA and higher education—such as the dorm hall murder of co-ed

Jeanne Clery, the escalation of alcohol and drug usage on campus, 9/11, and increased incidents of violence in the schools. In addition, other changes arose as legislation in other sectors of American society imposed their own amendments on FERPA and on how institutions conduct the business of education.

Amendments to FERPA over the Years

1974	December 31	Buckley/Pell Amendment
1979	August 6	Education Amendments of 1978
1979	October 17	Department of Education established
1990	November 8	Campus Security Act
1992	July 23	Higher Education Amendments of 1992
1994	October 20	Improving America's Schools Act
1998	October 7	Higher Education Amendments of 1998
2000	October 28	Campus Sex Crimes Prevention Act
2001	October 26	USA PATRIOT Act of 2001
2008	December 9	Amendments of 2008

The most recent set of amendments was proposed in the March 24, 2008, edition of the *Federal Register*. The amendments were surprisingly from the perspective of the sheer volume of changes proposed. In many ways, however, these extensive amendments held little that was new. The majority of the amendments signified an incorporation of interpretation and guidance made by the Department of Education (ED) over the years. Some of the amendments incorporated much-needed updates; after all, records management practice in 2008 had evolved and experienced vast changes in application and policy since FERPA was first proposed in 1974. And still other changes were incorporations of the impact of recent federal legislation to amend FERPA.

In the December 9, 2008, edition of the *Federal Register*, the final FERPA regulations were issued. In essence, all of the proposed amendments were adopted, with relatively few changes made to the final text of the proposed changes. Throughout this book, references to the March 24 and December 9 editions of the *Federal Register* are quoted, with citations to the applicable page numbers in each of the publications.

FERPA continues to be amended as needed, as the changing cultural environment and operational needs of our educational institutions warrant.

Evolution of the U.S. Department of Education

Originally proposed by President Warren Harding in 1923, the Department of Health, Education, and Welfare (HEW) did not come into existence until 30 years later in 1953. President Dwight D. Eisenhower, using his reorganizational authority, created the department as a cabinet-level department, under a Secretary of Health, Education, and Welfare. HEW was the only such department to ever be created by presidential authority.

In 1979, the HEW was reorganized by the Department of Education Organization Act, signed by President Jimmy Carter. The act separated the department into two distinct entities—the Department of Education (ED) and the Department of Health and Human Services (HHS).

The ED opened its doors on May 4, 1980. It is the smallest of the cabinet departments, employing less than 5,000 people.

Enforcement of FERPA

When it was passed in 1974, the enforcement of FERPA was initially assigned to the Department of Health, Education, and Welfare (HEW). But in 1979, the HEW was reorganized. The Department of Education (ED) was born in 1980. Jurisdiction for the interpretation, adjudication, and enforcement of FERPA became the responsibility of the Family Policy Compliance Office (FPCO).

Part of the ED in Washington, D.C., the FPCO is responsible for administering both FERPA and the PPRA. LeRoy Rooker, the office's longest-serving director, managed the FPCO from 1988 until early 2009.

CONTACTING THE FAMILY POLICY COMPLIANCE OFFICE (FPCO)

The Family Policy Compliance Office (FPCO) may be contacted directly by school administrators, students, parents, and the general public by writing to:

Family Policy Compliance Office
U.S. Department of Education
400 Maryland Avenue SW
Washington DC 20202–5920
(202) 260–3887 or FAX (202) 260–9001

Education officials *only* may send electronic inquiries to *FERPA@ed.gov.*
www.ed.gov/policy/gen/guid/fpco/index.html

The FPCO regularly works with a myriad of constituencies—institutions, students, parents, state and local departments of education, government agencies, public and private organizations, and other citizens. Its scope of responsibility covers kindergarten, along with elementary, middle, junior, and high school (K–12), as well as higher education and other postsecondary institutions. Since FERPA applies to education agencies, the office also deals with providers of different services related to educational research and records management for the education community.

Inquiries to the FPCO are welcome; however, since the office services the entire nation and deals with legislative interpretation and guidance, questions are best submitted in writing. Parents, students, and other citizens should submit written correspondence by U.S. mail or fax. Education officials should check with the registrar of their individual institutions regarding local policy and practice prior to inquiring with the FPCO.

All communications, regardless of the delivery method, should include a few basic information items that affect the FPCO's response. These items include the following:

- Composer's name and contact information (address, telephone number)
- Full name of the school in question
- Location of the school in question—complete address, city and state, and school district (if applicable)

It is important to provide location information since state and local law may sometimes have critical or intervening implications in regard to how an institution administers the federal regulations.

The FPCO maintains extensive information on the Department of Education website and posts valuable and timely communications for parents, students, and institutional administrators. In addition to news and legislative updates, the website houses a library of reference information on FERPA and other legislation affecting education in general. A collection of "Dear Colleague" letters share official responses to inquiries and complaints that provide official interpretation, guidance, and instruction on issues arising from the administration of FERPA.

As the primary interpreter, adjudicator, and enforcer of FERPA, the FPCO has the responsibility and authority to respond to complaints about alleged violations of FERPA. This is, in fact, one of the four guarantees that the regulations make: the right to file a complaint when FERPA rights are violated or thought to have been violated by institutions or educational agencies. The FPCO investigates, thoroughly examining the issue of the complainant, reviewing the processes and practices of the institution, and mediating a response that ensures compliance with FERPA.

Further discussion regarding the submission of complaints is provided in Chapter Three.

Applicability of FERPA and Penalties for Noncompliance

FERPA is referred to as a spending clause or spending statute, a definition that focuses the applicability of the regulations and identifies the area of potential penalty. Indeed, both application and penalties are financial, or financially based.

> Except as otherwise noted, in Section 99.10, this part applies to an educational agency or instituti nds have been made available under any program administered by the Secretary. . .
>
> *§99.1(a)*

The first section of the regulations addresses the issue of their applicability, noting specifically that if an institution receives monies or funding from the federal government, that institution is required to comply with FERPA. Funding includes financial aid programs, and the regulations go on to mention specifically Pell Grants and the Guaranteed Student Loan Program. But funding can also include other government or agency grants, cooperative agreements, contracts, subgrants, and subcontracts with the federal government.

In its statement of applicability, the regulations go on, in §99.1(d), to clarify that not only is the institution as a whole required to comply with the regulations but that compliance is also expected from each and every component of the institution. In other words, the regulations do not merely govern operations in the records unit but apply to every department and office throughout the institution.

> If an educational agency or institution receives funds under one or more of the programs covered by this section, the regulations in this part apply to the recipient as a whole, including each of its components (such as a department within a university).
>
> *§99.1(d)*

a. The Office reviews a complaint, if any, information submitted by the educational agency or institution, and any other relevant information. The Office may permit the parties to submit further written or oral arguments or information.

b. Following the investigation, the Office provides to the complainant, if any, and the educational agency or institution a written notice of its findings and the basis for its findings.

§99.66

If the statement of applicability is to institutions that receive funding from the federal government, then the penalty for noncompliance is a loss of that federal funding. Noncompliance can be identified in *any* area of an institution, but the consequence—a loss of federal funding—would impact the *entire* institution. It is a daunting realization that an institution could lose its eligibility to participate in federal funding based upon a violation that could occur in any one segment of its operational areas!

According to §99.66, when an investigation is undertaken and a determination of a violation has been made, the FPCO issues a formal notice of its findings. It then allows the institution a reasonable amount of time to rectify the situation that created the violation. The "reasonable amount of time" is determined by the nature of the complaint and the seriousness of the violation.

During this period, the FPCO works with the institution to bring the institution back into compliance with FERPA.

If the Office finds that an educational agency or institution has not complied with a provision of the Act or this part, it may also find that the failure to comply was based on a policy or practice of the agency or institution. A notice of the findings issued under paragraph (b) of this section to an educational agency or institution that has not complied with a provision of the Act or this part—

1. Includes a statement of the specific steps that the agency or institution must take to comply; and

2. Provides a reasonable period of time, given all the circumstances of the case, during which the educational agency or institution may comply voluntarily.

§99.66(c)

The situation that initiated the complaint may have been a misguided policy or procedure or a departmental practice developed under erroneous information. It might also involve misunderstanding on the part of an employee with regard to an institutional policy or procedure. Whatever the cause, once identified, the institution must make the appropriate changes to bring itself into compliance with FERPA. If it does not, then the FPCO can utilize any number of actions—including the withholding of federal funding—to bring the institution into compliance.

> If an educational agency or institution does not comply during the period of time set under §99.66(c), the Secretary may take any legally available enforcement action, including, but not limited to, the following enforcement actions available in accordance with part E of the General Education Provisions Act—
>
> *§99.67(a)*

In the more than 35 years since its enactment, no institution has lost its federal funding. In investigating complaints of alleged violations of FERPA rights, the FPCO has always worked with institutions to bring their policy and practice into compliance. This is not to say, however, that the threat may not become justified by some future infraction.

One of the questions often voiced by staff in discussions about the penalties under FERPA focuses upon whether a student has the right to sue under these regulations—and especially whether an individual recordkeeper at an institution can be sued under FERPA. Although the Privacy Act of 1974 included a Section 1983 right to sue, that right was never carried over into the final language of the FERPA regulations. This does not mean that individuals and institutions cannot be sued under other privacy and ethics regulations and statutes. Depending upon the circumstances and upon the applicability of other state and local laws, legal suits may still be possible.

The issue of Section 1983 rights—the right to sue—has been raised numerous times over the years and evidenced quite dramatically in the case of *Gonzaga University v. Doe.* In this case, John Doe sued Gonzaga University not only on the basis of a violation of his privacy rights but also for defamation of character, a breach of his educational contract, and other complaints. In 1997, the Spokane County Superior Court ruled in the student's favor,

Gonzaga University v. Doe

In 1993, John Doe was an undergraduate student enrolled in the School of Education at Gonzaga University in Spokane, Washington. John planned to work in a Washington elementary school but would first have to graduate and obtain an affidavit of good moral character from his school. Roberta League was the teacher certification specialist at Gonzaga, working with Dr. Susan Kyle, director of Field Experience, Janet Burcalow, chair of the Education Department, and Dr. Corrine McGuigan, dean of the school.

In October 1993, League overheard a conversation between students accusing John of date rape and other aberrant sexual behavior. League took the news to Kyle, and the two began an investigation that included interviewing the alleged victim, Jane Doe. Despite conflicting reports and Jane's request to Burcalow not to pursue the matter, McGuigan concluded that there was sufficient evidence to preclude her issuing an affidavit of good moral character on John's behalf. John learned of this decision on March 4, 1994, after having submitted his final tuition payment.

John filed a suit against Gonzaga and League. Jane was initially included in the suit and she countersued. Later, however, John and Jane dropped their charges against each other, and Jane testified via videotape and deposition that John had not sexually assaulted her.

In 1997, the Spokane County Superior Court decided in John's favor, awarding damages that totaled $1.15 million. The damages included $100,000 for invasion of privacy, $500,000 for defamation, $55,000 for breach of educational contract, $50,000 for negligence, and $450,000 in punitive damages and for violation of FERPA rights.

The case went to the Washington Court of Appeals and then to the U.S. Supreme Court, which, in 2002, endorsed the award on John Doe's behalf except for the damages claimed under FERPA. In its decision, the Supreme Court concluded that FERPA's nondisclosure provisions did not confer a private or individual right to sue. The only penalties defined in the FERPA regulations are the withholding of federal funds from institutions, which is an action administered solely by the Department of Education.

awarding a sizeable monetary settlement. But the university appealed and the case was eventually heard by the U.S. Supreme Court. While most of the student's award was preserved, the Supreme Court ruled that FERPA did not provide a basis for an individual's right to sue. The Supreme Court reversed the portion of the previous court's award that had been based upon FERPA.

Although the Supreme Court ruling on *Gonzaga University v. Doe* explicitly determined that individuals have no right to sue under FERPA, the issue continues to be raised from time to time.

Moreover, the bases for the monetary awards in *Gonzaga University v. Doe* serve to illustrate the kinds of complaints that can be used as a basis for legal action against an institution. In other words, FERPA does not cover everything in regards to the wider implications of privacy and educational

rights. FERPA cannot be used as a basis for legal redress, but other legislation may very well provide those platforms.

Further, the case of *Gonzaga University v. Doe* illustrates quite clearly that education officials—not just their institutions—can be cited for complaints and violations that escalate privacy rights beyond FERPA. FERPA trainers would do well to include ethics and moral responsibility as additional topics in their FERPA training curriculum.