Federal Controls on State Information Disclosure:

FERPA, HIPAA and DPPA

By Harry Hammitt
Vice President, Virginia Coalition for Open Government

Volume 2, Number 2

Reinstituting the FOI Reports service on behalf of the NFOIC

Although many state public records laws post-date the federal Freedom of Information Act and take their basic design from the federal legislation, information policy at the state level has traditionally evolved separately from that of the federal government. But the ability of the federal government to mandate information policies in the states at variance with state practice became clear when Congress passed the Drivers Privacy Protection Act in 1994, a law designed to limit public access to records held by state motor vehicle departments. The DPPA is not the only federal statute that has significant impact on state information disclosure practices. The DPPA, the Family Educational Rights and Privacy Act (FERPA), and medical privacy regulations promulgated by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act (HIPAA), form a triad of federal privacy legislation that has had substantial impact on the ability to gain access to records at the state level.

These three statutes are characteristic of the patchwork approach to privacy adopted by the United States. The federal Privacy Act[1] provides broad protections for personal information collected and maintained by the federal government, but the breadth of its coverage is unusual in American privacy laws. European and commonwealth countries, on the other hand, have broad data protection laws under which personal information is presumed to be non-disclosable unless it falls within an exception to the rule of non-disclosure. But U.S. legislators have consistently rejected broad generic privacy protections and have opted instead for protection of certain types of records. Although those who support such an approach often defend such piecemeal protection as focusing on those records that most deserve privacy protections, the reasons for protecting certain types of information are often the result of political decisions rather than good policy. It is hard to argue that video rental records[2] are more deserving of privacy protection than medical or financial information.

What is particularly remarkable about the patchwork privacy laws that are the subject of this report – FERPA, HIPAA and DPPA – is the way in which they depart from the model set up in the Privacy Act. The Privacy Act allows the federal government to use personal information it collects for purposes compatible with the reason for which the information was collected. It creates a rule of non-disclosure without consent and provides 12 exceptions to that rule – such as need to know, required disclosure under FOIA, routine uses, court orders, statistical and research use, and disclosure for use in credit reporting. The statute's enforcement mechanism, however, is almost completely dependent on individuals who can request access to their own personal information, challenge its accuracy, and sue an agency for damages for any violation of the statute that results in an adverse effect on them. As such, the Privacy Act is self-enforcing and depends on individuals going to court to enforce individual rights. The results of such litigation establish legal interpretations that can be used to support future individual actions. From a policy perspective, the reason to make such a law self-enforcing is because it is individuals that have the greatest incentive to make sure that their own records are accurate and used appropriately. But such a self-enforcing policy does not exist in FERPA, HIPAA, or DPPA, although there is a limited right of personal action in the DPPA. Instead, FERPA, HIPAA and the DPPA prohibit or discourage covered institutions from disclosing certain kinds of information and leave enforcement up to the Department of Education in the case of FERPA, the Department of Health and Human Services in the case of HIPAA, and the U.S. Attorney General in the case of the DPPA. Federal courts nevertheless had been willing to infer a private right of action for FERPA

[1] 5 U.S.C. 552a
[2] 18 U.S.C. 2710

and similar statutes by allowing individuals to sue under 42 U.S.C. § 1983, a catch-all provision that grants federal courts jurisdiction over actions involving federal statutes. However, in *Gonzaga University v. Doe*[3], the Supreme Court ruled that a private right of action cannot be inferred under statutes like FERPA. Instead, a private right of action exists only when Congress specifically provides such a remedy. The practical effect of this decision is to prohibit individuals from bringing suit directly under FERPA, leaving as the only remedy an action brought against a school by the Department of Education for violating FERPA.

Considering their notoriety with journalists as commonly-used reasons for denying access to government records, there is not a great deal of litigation under FERPA, HIPAA or the DPPA compared to litigation under broader statutes like the Freedom of Information Act and the Privacy Act. This is probably because they are such specialized statutes and their restrictions so specific that the incentive for bringing suit is much less than with more generic access or privacy laws. However, it is certainly the case that FERPA often figures in litigation brought under a state's public records law as the ultimate reason for denying access, although the reason given by the public body is that disclosure is prohibited by a federal law or regulation. This report will survey current court interpretation and policy goals of these two statutes (FERPA and DPPA) and one regulation (HIPAA's medical privacy regulation).

Family Educational Rights and Privacy Act (FERPA)

The Family Educational Rights and Privacy Act was introduced by Sen. James Buckley (R-NY) as a floor amendment during reauthorization of the Elementary and Secondary Education Amendments of 1965.[4] At the time, Buckley indicated that he introduced the legislation to counteract "the growing evidence of the abuse of student records across the nation."[5] The amendment was based on recommendations from a study of records and record-keeping issued by the Department of Health, Education and Welfare.[6] According to its sponsors, Buckley and Sen. Claiborne Pell (D-RI), the purpose of the legislation was "to assure parents of students, and students themselves if they are over the age of 18 or attending an institution of postsecondary education, access to their education records and to protect such individuals' rights to privacy by limiting the transferability of their records without their consent."[7] Because of problems in drafting, the original Buckley amendment was substantially rewritten and the new version, enacted on December 31, 1974, was made retroactive to the law's effective date.[8]

To achieve the basic two goals of FERPA[9] – access to student records by individual students and their parents and a general rule of non-disclosure to other third parties – the amendment tied compliance to federal funding. Section (a)(1)(A) and (a)((1)(B), relating to student access to records, says that no funds shall be made available to institutions that do not have a policy for providing appropriate access. Section (b)(1) contains the privacy requirements.

---

[3] 536 U.S. 273 (2002)
[4] See Education Amendments of 1974, Pub. L. No. 93-380, 513, 88 Stat. 571. See also S. Rep. No. 93-1026 (1974).
[5] 121 Cong. Rec. 13,990 (1975) (statement of Sen. Buckley)
[6] Katherine Cudlipp, "The Family Educational Rights and Privacy Act Two Years Later," 11 U. Rich.L.R. 33, 33 (citing U.S. Dept. of Health, Education and Welfare, "Report of the Secretary's Advisory Committee on Automated Data Systems, Computers and the Rights of Citizens," 1973)
[7] 120 Cong. Rec. 39,863 (1974) (Joint Statement in Explanation of Buckley/Pell Amendment)
[8] Buckley/Pell Amendment, Pub. L. No. 93-568, 88 Stat. 1858.
[9] 20 U.S.C. 1232g

That section states that

> no funds shall be made available under any applicable program to any educational agency or institution which has a policy or practice of permitting the release of education records (or personally identifiable information contained therein other than directory information as defined in paragraph (5) of subsection (a) of this section) of students without the written consent of their parents to any individual, agency, or organization.[10]

This prohibition is followed by a number of exceptions. Student directory information may be disclosed under FERPA. The statute defines directory information in Section (a)(5)(A) as:

> the student's name, address, telephone listing, date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, and the most recent previous educational agency or institution attended by the student.[11]

However, an institution that discloses directory information must provide public notice of the categories of information designated as directory information and must allow a reasonable period of time after notice is given to allow a parent, or the student if 18 or older, to inform the institution that all or any such information designated should not be disclosed without the parent or student's prior consent.[12]

The statute only applies to students, defined as "any person with respect to whom an educational agency or institution maintains education records or personally identifiable information,"[13] and the definition specifically excludes "a person who has not been in attendance at such agency or institution."[14] However, while the rather broad definition of "student" could be stretched to include teachers, faculty, administrators, and others who similar connections to educational institutions, case law has established that the law's privacy protections apply only to students as that term is commonly understood.[15]

The statute makes clear that educational institutions should allow access to students and their parents and should prohibit access to most others. But the statute contains no direct prohibition on public access. Instead, the only penalties for disclosure are a potential cut-off of federal funds. To accomplish this goal, the Department of Education would have to determine that an educational institution has a "policy or practice" of permitting inappropriate third-party access to student records and would then have to recommend that federal funding be curtailed. This is certainly an onerous standard and there is no apparent evidence that any institution has ever lost its federal funding due to a breach of the privacy provisions in FERPA. However, the mere possibility of losing funding has been more than sufficient to encourage educational institutions to abide strictly by FERPA's edicts.

While FERPA's primary goal is to safeguard the privacy of student records by prohibiting third party access without consent, other policy and political pressures have resulted in a series of

---

[10] 20 U.S.C. 1232g(b)(1)
[11] 20 U.S.C. 1232g(a)(5)(A)
[12] 20 U.S.C. 1232g(a)(5)(B)
[13] 20 U.S.C. 1232g(a)(6)
[14] Id.
[15] *See, for example, Klein Independent School District v. Mattox*, 830 F.2d 576 (5th Cir. 1987).

amendments that have carved out exceptions for information dealing with campus security. In 1990, Congress passed the Campus Security Act, which amended FERPA by adding a new Section (b)(6).[16] This provision permits

> an institution of postsecondary education [to disclose], to an alleged victim of any crime of violence (as that term is defined in section 16 of title 18), or a nonforcible sex offense, the final results of any disciplinary proceeding conducted by such institution with respect to such crime or offense.[17]

Other parts of Section (b)(6) allow universities to disclose the final results of any disciplinary proceeding against a student alleged to have committed a crime of violence or nonforcible sex offense if the institution concludes that the student committed a violation of its rules or policies.[18] The final results shall include only the name of the student, the violation committed, and any sanction imposed, but may include the name of any other student, such as the victim or a witness, but only with the written consent of the other student.[19]

In 1992, FERPA was again amended to make law enforcement records more accessible.[20] The amendment revised Section (a)(4)(B)(ii) by excluding from the definition of educational records "records maintained by a law enforcement unit of the educational agency or institution that were created by that law enforcement unit for the purpose of law enforcement."[21] In 2000, Congress again amended FERPA to allow schools to disclose information about registered sex offenders.[22] Congress further amended FERPA as part of the Patriot Act, allowing the Attorney General and other law enforcement officials to gain access to educational records for the purposes of investigating terrorism.[23] Most of these changes were designed to make schools more accountable on matters of campus crime, but they have also created a tension within FERPA between its privacy goals and subsequent amendments requiring that more campus crime information be made available to the public.

Litigation under FERPA

Even though litigation under FERPA is not extensive in comparison with broader statutes like FOIA or the Privacy Act, many of the court decisions that do exist focus on disputes over whether the statute applies to certain categories of student information. Much of the litigation has focused on access to information about campus crime and disciplinary proceedings. The outcome of such litigation has varied since Congress has amended FERPA on several occasions to require more disclosure of campus crime information. Aside from litigation dealing with access to campus crime and disciplinary proceedings, most other FERPA cases have involved questions concerning the definition of student educational records.

a. campus crime and disciplinary proceedings

---

[16] Campus Security Act, Pub. L. No. 101-542, 104 Stat. 2385.
[17] 20 U.S.C. 1232g(b)(6)(A)
[18] 20 U.S.C. 1232g(b)(6)(B). Changes in (b)(6)(B) and (C) were the result of the Higher Education Amendments of 1998, Pub. L. No. 105-244, 112 Sta. 1835.
[19] 20 U.S.C. 1232g(b)(6)(C)(i) and (ii)
[20] Pub. L. No. 102-325, 106 Stat. 840.
[21] 20 U.S.C. 1232g(a)(4)(B)(ii)
[22] Campus Sex Crime Prevention Act, Pub. L. No. 106-386, 114 Stat. 1538 (codified as 20 U.S.C. 1232g(b)(7))
[23] U.S.A. Patriot Act, Pub. L. No. 107-56, 115 Stat. 367

Certainly the hottest battle in the early 1990s was litigation brought by student journalists to gain access to records concerning campus crime and other disciplinary proceedings. Reading the strictures of the statute broadly, universities had consistently claimed that FERPA prohibited the disclosure of most law enforcement records. But in a case brought by Southwest Missouri State University student journalist Traci Bauer, a federal district court found that "FERPA is not a law which prohibits disclosure of educational records. It is a provision which imposes a penalty for the disclosure of educational records." The court concluded that the records Bauer sought were available under Missouri's Sunshine Law.[24] The same year as the *Bauer* decision, the Student Press Law Center challenged an action taken by the Department of Education threatening to withhold funding from 14 universities releasing campus crime information. The court ruled that the Department's policy violated the First Amendment and pointed out that "defendants' suggestion that the universities may choose to comply with state law and forego federal funding is unrealistic and disingenuous." Saying that the government had to provide some rational justification for restricting the students' First Amendment right to access the information, the court observed that "in light of the universities' willingness (absent coercion to the contrary) to release campus crime reports in full, the Government must assert some interest that outweighs the public's First Amendment right to receive the information."[25]

The 1992 amendment to the law enforcement exception provided more access to campus crime information, but the fight then moved to whether FERPA covered quasi-judicial disciplinary proceedings. Student journalists at the University of Georgia won an important victory when the Georgia Supreme Court ruled that the Organization Court, a student-run court overseeing fraternal organizations on campus, was subject to the state's Open Meetings Act. The university argued that FERPA prohibited public access to the proceedings, a claim the court rejected, noting instead that "we have serious questions whether [FERPA] even applies to the exemptions argued by the defendants since [FERPA] does not prohibit disclosure of records. . .Assuming, without deciding, that the threat of withdrawal of federal funding is equivalent to a prohibition of disclosure, we do not believe the documents sought are 'education records' within the meaning of [FERPA]." Echoing the *Bauer* court, the state Supreme Court observed that "the records are not of the type that [FERPA] is intended to protect, i.e., those relating to individual student academic performance, financial aid, or scholastic probation." The court concluded that "the Organization Court, acting with the Office of Judicial Programs, is the *vehicle* by which the University carries out its responsibility. . .[H]aving delegated official responsibility and authority to the Organization Court, the defendants cannot hide behind meetings at which official action is taken on their behalf . . . by contending that a group of students, none of whom are members of the Board of Regents, is taking that action."[26] However, an appellate court in North Carolina reached the opposite conclusion, finding that records of an undergraduate disciplinary court were protected by FERPA.[27]

When the Ohio Supreme Court embraced the reasoning of the *Red & Black* decision by the Georgia Supreme Court and ruled in favor of the student newspaper at Miami University,[28] the argument over the extent to which student disciplinary records were protected by FERPA heated up. The Ohio Supreme Court ruled that the proceedings of the Miami University Disciplinary

[24] *Bauer v. Kincaid*, 759 F. Supp. 575 (W.D. Mo. 1991)
[25] *Student Press Law Center v. Alexander*, 778 F. Supp. 1227 (D.D.C. 1991)
[26] *Red & Black Publishing Company v. Board of Regents*, 427 S.E.2d 257 (Ga 1993)
[27] *DTH Publishing Corp. v. University of North Carolina at Chapel Hill*, 496 S.E.2d 8 (N.C. Ct. App. 1998)
[28] *State ex rel. Miami Student v. Miami University*, 680 N.E.2d 956 (Ohio 1997)

Board, which adjudicated cases involving criminal matters, "are nonacademic in nature. The UDB records, therefore, do not contain educationally related information, such as grades or other academic data, and are unrelated to academic performance, financial aid, or scholastic performance." As a result of the Ohio Supreme Court decision, both Miami and Ohio State University indicated they would begin disclosing disciplinary records under the Ohio Public Records Act, particularly in response to requests by the *Chronicle of Higher Education*. The Department of Education then filed suit in federal district court seeking a permanent injunction against the disclosure of student disciplinary records.

In *USA v. Miami University*,[29] the court sided with the government, noting that "interpreting the term 'education records' so as to not include student disciplinary records would permit public disclosure of such records and would lessen students' privacy rights under FERPA. This would undermine one of the stated purposes of FERPA, as it would allow universities to release students' disciplinary records without consent." The court found that the Education Department's interpretation of law enforcement records that could be disclosed under the law enforcement exception distinguished between "law enforcement records" and "disciplinary records" and was a reasonable reading of the statute that precluded a finding that disciplinary records fit within the law enforcement exception. The court also rejected the *Chronicle*'s argument that FERPA did not provide for court intervention by the Department. The court noted instead that, because the Department could "take any other action authorized by law with respect to the recipient," this included the "power to file civil actions in federal court." The court added that "without the ability to file lawsuits in federal court, the Department is left without a meaningful remedy by which to accomplish FERPA's purpose; the primary remaining enforcement mechanism would be withdrawal of funding to any educational institution that violates FERPA. Such a harsh remedy would serve as a significant blow to universities and other institutions, and potentially could cause a decrease in the level of education. In the long-run, the students attending these institutions and their parents – parties whom FERPA was intended to protect – would be the ones most penalized by such action."

The district court's decision was affirmed by the U.S. Court of Appeals for the Sixth Circuit in 2002.[30] The appellate court found that Congress, by amending FERPA to provide for disclosure of records pertaining to campus crime, had implicitly made a distinction between the disclosure of law enforcement records and the protection of disciplinary records that fell short of criminal action. Further, the court was persuaded by the Education Department's regulations and noted that "the agency draws a clear distinction between student disciplinary records and law enforcement unit records. The former are protected as 'education records' under the FERPA without regard to their content while the latter are excluded from the definition of 'education records' and receive no protection by the FERPA."

The Sixth Circuit's interpretation has reduced potential access to disciplinary records to the narrow slice of proceedings against a student for a crime of violence or nonforcible sex offense if the institution finds that the student committed a violation of the institution's rules or policies. Further, the Clery Act,[31] a separate provision that requires universities to report statistics on campus crimes and certain aspects of financial aid, mandates that both the accuser and the accused be informed of the outcome of any institutional disciplinary proceeding brought alleging a sex

[29] 91 F. Supp. 2d 1132 (S.D. Ohio 2000)
[30] *U.S. v. Miami University*, 294 F.3d 797 (6th Cir. 2002)
[31] Jeanne Clery Disclosure of Campus Security Policy and Campus Crimes Statistics Act, 20 U.S.C. 1092

offense.[32] Even so, although FERPA allows disclosure of the final results of such a proceeding to the victim, until recently most schools required victims to sign confidentiality agreements restricting their ability to further disclose such information. The Department of Education in July 2004 ordered Georgetown University to abandon its policy of requiring victims to sign confidentiality agreements prohibiting them from further disclosure of the results of the proceedings. At the time, the University said it was following its understanding of the requirements of FERPA and the Clery Act.[33]

The expanded availability of campus crime information had led to related litigation in several states over disclosure of law enforcement records of campus police at private universities. In two cases brought against private colleges for access to law enforcement records, the courts found that neither institution was covered by the state public records law and the fact that campus police had certain law enforcement authority did not make them representatives of the state.[34] However, the Georgia legislature passed an amendment to the public records law requiring access to crime records at private colleges and universities. Similar legislation proposed in Massachusetts did not pass.[35]

b. defining student educational records

Much of the other litigation under FERPA has focused on definitional issues. Since its non-disclosure provisions apply to student educational records, reporters and others trying to gain access to school records have tried to characterize the records sought as falling outside a narrow universe of student records pertaining to academic status, while schools have invariably argued for the broadest definition of educational records. Overall, the schools have probably won more than they have lost, but it is hard to divine any immutable principles from the cases.

In *University of Connecticut v. FOI Commission*,[36] the Connecticut Supreme Court reversed a ruling by the FOI Commission. The Commission had found that the identities of students working as interns for the local police did not qualify as student educational records but were instead employment records of the police that must be disclosed. Although the court did not rely directly on FERPA and found that the names were protected by an exemption in the state FOIA protecting the names and addresses of students enrolled in a public school from disclosure without consent, the court concluded that the records were about the students and not about the police.

The Maryland Court of Appeals found that parking tickets given to members of the basketball team at the University of Maryland were not education records. The court noted that "we hold that 'education records' within the meaning of [FERPA] do not include records of parking tickets or correspondence between the NCAA and the University regarding a student-athlete accepting a loan to pay parking tickets."[37] Finding that the general privacy exemption in the state's public records act did not protect the names of incoming freshmen at Southern

---

[32] 20 U.S.C. 1092(f)(8)(B)(iv)(II)
[33] Student Press Law Center, "Agency says D.C. university cannot bar victim from disclosing disciplinary outcome,"July 23, 2004.
[34] *Corporation of Mercer University v. Barrett & Farahany, LLP*, 610 S.E. 2d 138 (2005) and *Harvard Crimson v. President & Fellows of Harvard College*, 840 N.E. 2d 518 (2006)
[35] Whitney McFerron, "New Georgia law opens crime records at private colleges; Massachusetts legislation falls short," Student Press Law Center, Fall 2006.
[36] 585 A.2d 690 (Conn 1991)
[37] *Kirwan v. Diamondback*, 721 A.2d 196 (Md. 1998)

University Illinois who had not yet registered but had asked about campus housing, the Illinois Supreme Court granted access to Stan Lieber, a local landlord looking for information about potential student tenants. By ruling the way it did, the court implicitly decided that the disclosure of such information was also not prohibited by FERPA.[38] In Wisconsin, the Supreme Court ruled that the University of Wisconsin must disclose statistical information about gender, ethnicity and scholastic standing of students who attended state universities, as well as those who applied and decided not to attend. The court ruled that "the University inappropriately relied on FERPA in denying [the plaintiff's] open records request, because FERPA does not prohibit disclosure of records where personally identifiable information is not included."[39] The staff of the Virginia Freedom of Information Advisory Council advised a requester that George Mason University was probably not required to release a copy of student email addresses even though they fit within the definition of directory information. The staff pointed out, however, that under FERPA a school was allowed to disclose directory information, but was not required to do so.[40]

Some states, while recognizing FERPA as a basis for non-disclosure of student educational records, also have incorporated its prohibitions into exemptions in state public records laws. For instance, the *Chicago Tribune* was denied access to non-identifying information about students in the Chicago school system under the Illinois Student Records Act.[41] Rejecting the newspaper's argument that the records did not identify individual students, the court pointed out that "the clear and plain wording of the exemption does not contain any language with respect to identification of individuals in order to invoke the exemption."

The Supreme Court also ruled in another FERPA case prior to its ruling in *Gonzaga v. Doe*. While *Gonzaga*'s restriction on private causes of action under FERPA has widespread implications, the Court's ruling in *Owasso v. Falvo*,[42] dealt with the seemingly obscure issue of whether grades assigned to homework that had been passed out in class and graded by individual students could be considered student educational records for purposes of FERPA. Kristja Falvo had complained that the practice resulted in her children being ridiculed by their classmates and had sued when the school refused to abandon its practice of allowing students to grade homework. The Tenth Circuit ruled that the practice did violate FERPA and that the students were acting as agents of the school.[43] The Supreme Court reversed, finding that the records were not subject to FERPA.

Health Insurance Portability and Accountability Act (HIPAA)

After the failure of the healthcare task force initiative during the Clinton administration's first term, Congress began to look at smaller healthcare issues that might attract a legislative consensus. Because at the time a major issue for healthcare consumers was the ability to carry over health insurance provided by one employer to a subsequent employer, a bill sponsored by Sen. Nancy Kassenbaum (R-KS) and Sen. Ted Kennedy (D-MA) made health insurance portability its central focus. The Health Insurance Portability and Accountability Act of 1996 accomplished that goal and also included provisions for increased use of electronic records so that medical records and information could be moved quickly from one location to another to help

[38] *Lieber v. Board of Trustees of Southern Illinois University*, 680 N.E. 2d 374 (Ill. 1997)
[39] *Osborn v. Board of Regents of the University of Wisconsin System*, 647 N.W. 2d 158 (Wis. 2002)
[40] Opinion AO-33-01, Virginia Freedom of Information Council, June 14, 2001.
[41] *Chicago Tribune v. Board of Education of City of Chicago*, 773 N.E.2d 674 (Ill 2002)
[42] 534 U.S. 426 (2002)
[43] *Falvo v. Owasso Independent School District*, 233 F.3d 1203 (10th Cir. 2000)

improve healthcare. In order to achieve this goal, Congress recognized that sensitive medical records would require some level of privacy protection to help ensure their appropriate use and confidential treatment. Unfortunately, Congress was unable to agree on a legislative resolution to privacy concerns so it instructed the Department of Health and Human Services to promulgate a medical privacy rule if Congress failed to act within three years. When the three-year deadline came and went, HHS drafted a medical privacy regulation. The final rule became effective in April 2003.[44]

The Privacy Rule applies only to *covered entities* which are defined as: a health plan, a health care clearinghouse, and a health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.[45] Only protected health information (PHI) – defined as information relating to an individual's physical or mental health, provision of health care, or payment of health care – is covered under the regulation. Such information is covered if it identifies, or could be used to identify, the person who is the subject of the information. The record must be created or received by a covered entity. The rule incorporates features from fair information practices, requiring entities to use or disclose the minimum amount of protected health information necessary to accomplish the intended purpose, although there are a number of exceptions. Patients have a right to see and copy their own health information, including an accounting of who has access to the information. Patients can also request a correction or amendment to records. Health plans and health care providers are required to provide written notice of their privacy practices, including the patient's right of access and correction, and anticipated uses and disclosures of information that can be made without patient consent. Consent is not required when health information is used for treatment, payment, or health care operations related to treatment and payment. The Privacy Rule calls for an individual to authorize all other types of disclosures, although, again, there are many exceptions.

Health information can be disclosed to others without consent, but there are restrictions. Information can be disclosed for research purposes if the research protocol has been reviewed by an Institutional Review Board or privacy board. There are a number of exceptions to the requirement that an individual authorize disclosure or use. For instance, information can be disclosed for law enforcement purposes, including pursuant to a simple, undefined administrative request for information; pursuant to a grand jury subpoena; for national security concerns; and as required by law.

The regulations also contain civil penalties, capped at $25,000 a year for each provision that is violated, and criminal penalties, which increase depending on the severity of the charge; 10 years in prison is the maximum sentence allowed. Finally, the regulations provide a baseline for privacy coverage nationwide. States that have, or wish to pass, health information laws that provide greater protections for individuals, may do so.

The Office of Civil Rights at the Department of Health and Human Services is charged with enforcing the Privacy Rule. After three years and 19,420 complaints so far, the Office has closed more than 73 percent – more than 14,000 – after finding no violation, or allowing health care providers to promise to fix the problem, thus avoiding any penalty.[46] The first prosecution brought under the Rule was against Richard Gibson, a phlebotomist in Washington State, in 2003.

---

[44] HIPAA, Pub. L. 104-191

[45] *Standards for Privacy of Individually Identifiable Health Information* ("Privacy Rule"), 45 C.F.R. 160, 162, and 164; at § 160.103

[46] Rob Stein, "Medical Privacy Law Nets No Fines," Washington Post, June 5, 2006, p. A1.

Gibson stole identifiable health information from a cancer patient, used the information to obtain credit cards in the patient's name and ran up more than $9,000 in charges. Although Gibson could have been charged with fraud or identity theft, the U.S. Attorney prosecuted him under HIPAA. Gibson pled guilty and was sentenced to 16 months in prison and $15,000 in restitution.[47] Since Gibson's prosecution, charges have been brought in a case in Texas and another in Florida.

Because HIPAA applies to "covered entities," there has been a legal dispute as to whether an individual, as opposed to an institution or office, can actually be held liable for violating the Privacy Rule. A memo issued by the Department of Justice's Office of Legal Counsel in June 2005[48] added fuel to the fire by indicating that only covered entities named in HIPAA are subject to criminal liability. The memo noted that "depending on the facts of a given case, certain directors, officers, and employees of these entities may be liable directly under section 1320d-6, in accordance with general principles of corporate criminal liability, as these principles are developed in the course of particular prosecutions. Other persons may not be liable directly under this provision."[49]

The rule allows covered entities to disclose limited basic care information such as the general condition of a patient, although a patient can object to such disclosures. But its primary intent is to protect personal medical information from disclosure without the actual consent of the patient. Nevertheless, its coverage is limited to covered entities and does not generally include police or fire departments except to the extent that they function as a healthcare provider. For example, an ambulance service would likely be considered a healthcare provider and would be a covered entity under the Privacy Rule, assuming that it also bills for its services electronically. To the extent that a local fire department provides similar services and bills for them electronically, such services could well be covered by the Rule. But unless police normally take individuals to the hospital and bill electronically for such services, the fact that police may convey an accident victim to the hospital in an emergency is not sufficient to qualify the police as a healthcare provider. Generally speaking, ambulance or emergency medical services personnel at the scene of an accident probably could not disclose personal medical information, while the police at the same accident site probably could.

The Privacy Rule has often been applied broadly and both providers and non-providers have at times claimed that they could not disclose information whose disclosure was not actually prohibited by the Privacy Rule. It should be noted, however, that there are state laws that may restrict or prohibit the disclosure of medical information as well and such laws may form the legal basis for prohibiting disclosures by the police. So far there has been little litigation concerning the role the Privacy Rule plays in restricting information, but the Attorney General in Texas and the Attorney General in Kentucky have both issued binding rulings on its effect.[50] The Texas AG opinion pointed out that the HIPAA regulations require disclosure where required by law and indicated that "the Public Information Act is a mandate in Texas that compels Texas governmental bodies to disclose information to the public. . .We, therefore, believe that the disclosures under the PIA come within [the required by law provision of the HIPAA regulations]. Consequently, when a covered entity that is a governmental body subject to the PIA is presented with a written request

[47] Gene Johnson, "Seattle Technician Sentenced in Identity Theft," The Columbian, Nov. 6, 2004, p. c2.
[48] "Scope of Criminal Enforcement under 42 U.S.C. § 1320s-6," June 1. 2005. Available online at www.usdoj.gov/Olc/hipaa_final.htm
[49] Access Reports, "DOJ Memo Limits HIPAA Privacy Liability," v. 31, n. 11, June 1, 2005, p. 3.
[50] Open Records Decision No. 681, Office of the Attorney General of Texas, Feb. 13, 2004 and Order 04-ORD-143, Office of the Attorney General of Kentucky, Aug. 24, 2004.

under the PIA for protected health information, it must evaluate each disclosure under the PIA as it does now under current procedures." While the AG found that the Privacy Rule does not prohibit disclosure, he went on to indicate that most medical information was likely protected by Texas law already. The opinion issued by the Kentucky Attorney General dealt with access to personal information contained on accident reports filed by the Covington police. The AG observed that "records generated by police officers do not contain protected health information, even if those records reflect the officer's observations of an individual's medical condition, and such records are not governed by the Privacy Rule. The incidental delivery of emergency aid by a police officer does not transform the police officer into a health care provider since his primary function is the protection of public safety." However, the AG concluded that the identifying information could be withheld under the state's general privacy exemption.

In the first state appellate ruling on the relationship between the Privacy Rule and a state public records law, the Ohio Supreme Court ordered the Cincinnati Health Department to disclose lead citations and lead-assessment reports indicating that blood tests showed that a child living at a residential address had elevated lead levels.[51] The Health Department argued that disclosure was prohibited by the Privacy Rule. The court first found that the information, which was collected to warn property owners that their property might constitute a lead hazard, was not health information. Turning to the Privacy Rule itself, the court noted that the Department of Health and Human Services indicated that "federal FOIA requests 'come within [a section] of the privacy regulation that *permits uses or disclosures required by law if the uses or disclosures meet the relevant requirements of the law.*' By analogy, an entity like the Cincinnati Health Department, faced with an Ohio Public Records Act request need only determine whether the requested disclosure is required by Ohio law to avoid violating HIPAA's privacy rule." A Texas appeals court, relying heavily on the Ohio Supreme Court's ruling, also found that the Privacy Rule allowed disclosure where permitted by the Texas Public Information Act.[52] The court noted that an exception to the rule of non-disclosure of personal medical information in the regulations allowed disclosure where required by another law. The court added that the commentary accompanying the Privacy Rule "makes it clear that when determining whether to release protected health information in response to a Freedom of Information Act request, an agency must look to the limits and exemptions in the Act, not to the Privacy Rule." Applying this rationale to the Public Information Act, the court observed that "if the request is made under the authority of a statute that requires disclosure. . .the agency must disclose the information as long as the disclosure complies with all relevant requirements of the statute compelling disclosure."

Drivers Privacy Protection Act (DPPA)

As is the case with many pieces of legislation, the Drivers Privacy Protection Act had its genesis in several isolated incidents that rose to the attention of politicians and formed the basis for legislation with a much greater impact than necessary to address the problem. The primary story-line for the DPPA was the death of television actress Rebecca Schaeffer, killed by an obsessed fan in 1989 who found her home address by hiring a private investigator to obtain her personal information from California Department of Motor Vehicles records. Because celebrity stalking was a real problem in California, the state legislature responded by passing a law allowing individuals to use a post office box or business address instead of a home address on their driver's

[51] *State ex. rel Cincinnati Enquirer v. Daniels*, 811 N.E.2d 1181 (Ohio 2006)
[52] *Abbott v. Texas Dept of Mental Health and Mental Retardation*, Tex. App-Austin, 2006 WL 2504417

records. [53] The issue of easy access to driver's records surfaced in Congress in the fall of 1993, this time tied to incidents in which pro-life groups were reportedly harassing doctors and patients at abortion clinics by using DMV records to track them down. These incidents, coupled with the Schaeffer murder, prompted Sen. Barbara Boxer (D-CA) and Rep. Jim Moran (D-VA) to introduce separate but similar pieces of legislation designed to restrict public availability of state DMV records. Boxer's bill passed quickly through the Senate with no hearings or debate, but Moran's bill was the subject of a two-day hearing in February 1994 held by the House Subcommittee on Civil and Constitutional Rights.[54]

The battle lines were drawn early in the debate and opposition to the bill included the press, direct marketers, and private investigators. Arguing that the press used DMV records for public interest purposes, Richard Oppel told the subcommittee that "the bill, with all of its exemptions, creates a false sense of security for the public. It will not stop stalkers. But it will keep information out of the hands of those (the press) who have used it for public good." Steve Metalitz, testifying on behalf of the Information Industry Association, said the Moran bill took a "presumed secret" approach to DMV records. He urged the subcommittee that a "presumed public approach would be more consistent with our legal framework concerning public records." He added that Congress should focus "on specific uses which are vulnerable to abuse – in the case of DMV records, license plate look-ups of names and residential addresses. While most of these are legitimate, Congress could, if necessary define which look-ups should be prohibited. This would leave a broad spectrum of other uses free of unneeded federal restrictions." On the privacy side, Janlori Goldman of the ACLU told the subcommittee that "DMV records [should] be treated as Privacy Act-like records, generally unavailable to the public or other government agencies without the record subject's consent."[55] State governments were also unhappy about the bill since the sale of DMV records, primarily to direct marketing companies, provided a significant revenue stream. In Florida alone, the DMV made $18 million annually selling DMV records.[56] However, some states, even before congressional consideration of the DPPA, did not consider DMV records to be public.

Congress passed the DPPA in 1994.[57] The law restricted access to driver's records without consent, although there were a number of exceptions for use by law enforcement, companies verifying personal information submitted to employers, criminal and civil litigation, insurers, private investigators for a permitted use, tow truck operators, toll transportation facilities, bulk marketing, and to requesters who had obtained the permission of the subject. The press was offered an exception of its own, but declined because it believed such an exception would allow government to determine who was a member of the press and because it did not want to appear to be receiving special privileges beyond those granted to the general public. Individuals were allowed to "opt-out" of most disclosures, particularly those made for commercial purposes. This position, which was preferred by the direct marketers, meant that individuals were required to ask their state DMV not to disclose their records; otherwise their records would be presumed disclosable for bulk marketing purposes and for "other purposes," a loophole originally designed to provide for press access. However, in 1999, Sen. Richard Shelby (R-AL), upset by some of the reported abuses of public records by data brokers, pushed through an amendment to the bulk marketing exception, changing the standard of consent to the much more stringent "opt-in,"

[53] Cal. Veh. Code 1808.21
[54] Access Reports, "DMV Records Hearing Shows Lack of Consensus on Solution," v. 20, n. 4, Feb. 16, 1994, p. 1.
[55] Ibid. at p. 2-3.
[56] Access Reports, "Privacy Concerns of Public Records Debated," v. 19, n. 23, Nov. 24, 1993, p. 1, at 2.
[57] Pub. L. 103-322; 18 U.S.C. 2721 et. seq.

meaning that individual DMV records could not be disclosed for marketing purposes unless an individual specifically consented to such disclosure. The Shelby amendment also did away with the "other purposes" exception.

Aside from preventing disclosure of personal information contained in a motor vehicle record unless covered by an exception, the DPPA also restricts the resale and redisclosure of such records. Generally, an individual or entity eligible to have access to motor vehicle records can resell or redisclose those records only for purposes permitted by the statute. For instance, while the press has long argued that stalking incidents similar to the Rebecca Schaeffer murder could continue because private investigators still have access to motor vehicle records, the law actually prohibits private investigators from using the information for a purpose other than those specifically spelled out in the statute.[58] However, the lines can easily get blurred in the case of data brokers, who can, for instance, legally resell motor vehicle records to companies verifying personal employment information, or for use in litigation. To avoid potential liability for resale of motor vehicle records to non-qualifying clients, data brokers have established policies to ensure that such records are accessible only by clients legally entitled to have access. The DPPA specifically warns against resale or redisclosure to third parties not entitled to have access to DMV records by making the procurement of motor vehicle records for unlawful purposes a violation of the statute.[59] The statute is also violated if personal information from a motor vehicle record is obtained by making a false representation.[60] The statute provides for criminal fines to any person who knowingly violates its provisions. However, the primary enforcement tool is a civil penalty levied against a non-complying state DMV by the Attorney General. Such fines can amount to $5,000 a day for each day for which the agency is in substantial non-compliance.[61] Individuals may also bring a civil action against "a person who knowingly obtains, discloses or uses personal information, from a motor vehicle record, for a purpose not permitted under this chapter." An individual whose information has been improperly disclosed can be awarded $2,500 in liquidated damages plus reasonable attorney's fees and costs.[62]

Litigation under the DPPA

To critics of the Drivers Privacy Protection Act, there appeared to be no more than superficial constitutional authority allowing Congress to require the states to prohibit access to public records. While Congress claimed its authority flowed from the Commerce Clause, which allows Congress to legislate on matters affecting interstate commerce, several states viewed the law as a violation of the Tenth Amendment, which prohibits Congress from legislating on matters reserved to the states. This constitutional argument seemed particularly potent at the time because the Supreme Court had struck down several federal laws,[63] particularly provisions of the Brady gun control legislation, after finding they violated the Tenth Amendment. Many state attorneys general believed the DPPA also ran afoul of the Tenth Amendment. The constitutional argument was litigated in several federal appellate courts with mixed results.[64] The conflict established by these contrary decisions brought the case to the Supreme Court, which heard *Condon v. Reno* from

[58] 18 U.S.C. 2721(c)
[59] 18 U.S.C. 2722(a)
[60] 18 U.S.C. 2722(b)
[61] 18 U.S.C. 2723(a) and (b)
[62] 18 U.S.C. 2724(a) and (b)
[63] *See, for example, Printz v. United States,*521 U.S. 898 (1997)
[64] *Pryor v. Reno*, 171 F.3d 1281 (11th Cir. 1999); *Travis v. Reno*, 163 F.3d 1000 (7th Cir. 1998); *Oklahoma ex rel. Oklahoma Dept of Public Safety v. United States*, 161 F.3d 1266 (10th Cir. 1999); and *Condon v. Reno*, 155 F.3d 453 (4th Cir. 1998)

the Fourth Circuit, which had found the law unconstitutional. In a unanimous decision, the Supreme Court upheld the law's constitutionality, finding the Commerce Clause provided ample support for congressional authority and rejecting the states' Tenth Amendment claim.[65]

Since its constitutionality was affirmed, there has been occasional litigation under the DPPA, although only a handful of cases have dealt with potential third-party access, focusing more often on claims that an individual or institution improperly disclosed or used personal information in motor vehicle records. From an access perspective, the two most important decisions are *Davis v. FOI Commission*[66] and *Atlas Transit, Inc. v. Korte*.[67] In *Davis*, the requester asked for motor vehicle grand lists from the Bridgeport tax assessor. The tax assessor declined, indicating that the DPPA prevented her from disclosing the information. The complaint was heard by the Connecticut FOI Commission, which ruled that the restrictions in the DPPA did not apply to records in the possession of the tax assessor and that a state law required that tax assessors' records were publicly available. The tax assessor appealed to the superior court, arguing that she had been given custody of the motor vehicle records by the commissioner of motor vehicles and, thus, had the same obligation to protect them as did the commissioner of motor vehicles. But the court observed that "the tax assessor is not the legal custodian of the department of motor vehicle records, but rather is given such records annually to compile a motor vehicle grand list each year. . ." The court also rejected the assessor's claim that the DPPA qualified as a federal prohibition against disclosure of such records, noting instead that the DPPA did not "expressly prohibit disclosure by the tax assessor." The court added that "to conclude otherwise would require finding an implicit repeal of [state law] and Connecticut's historical system of making grand lists, including personal property grand lists, available to the public for correction and disputation. . . [I]f the legislature had intended to restrict access to the name, address and ownership information provided to tax assessors by the department of motor vehicles . . ., it would have done so explicitly and specifically."

In *Atlas Transit*, the Wisconsin Court of Appeals rejected a claim made by several bus companies who furnished drivers for the Milwaukee public schools that names and drivers' license numbers of drivers were exempt under both the privacy exemption in Wisconsin's public records law and the federal DPPA. In response to a request by a local television reporter, the school system decided to provide identifying information about bus drivers. The companies were required to furnish such information as part of their contract with the school system. The school system gave the drivers 14 days to challenge its decision in court and the bus companies filed for a restraining order and permanent injunction. After finding the public interest in disclosure outweighed the personal privacy interest in withholding the information, the appeals court turned to the application of the DPPA. The court first noted that "the DPPA does not prohibit the release of this information by [the school system]. Therefore, there is no exclusion under [the public records act]." The court added that even "assuming the DPPA's reach included [the school system], the act contains several exceptions that appear to exempt the sought-after information. . . In sum, the DPPA does not prohibit [the school system] from releasing information on drivers collected by a private employer, and even if it did, several exceptions appear to permit this type of use of the information."

---

[65] *Reno v. Condon*, 528 U.S. 141 (2000)
[66] 760 A.2d 1188 (Conn. 2001); *affirmed* 787 A.2d 530 (Conn. 2002)
[67] 638 N.W.2d 625 (Wis. 2001)

The District of Columbia Court of Appeals found that the DPPA prohibited the disclosure of information concerning the identity and addresses of motorists who had received a ticket as the result of being photographed by a traffic light surveillance camera at a specific intersection. In *Wemhoff v. District of Columbia*,[68] attorney Daniel Wemhoff argued that he qualified for access to the information under the exception in the DPPA allowing access in connection with litigation. But the court indicated that "based on our own reading of [the pertinent exception], acquiring personal information from the motor vehicle records for the purpose of finding and soliciting clients for a lawsuit is not a 'permissible use' within the meaning of [the DPPA]." The court pointed out that "if a District employee discloses personal information in the motor vehicle records for the purpose of allowing solicitation of clients by a private attorney, that employee arguably would be vulnerable to a lawsuit, as would be the private attorney if he used the personal information to find clients for a class action lawsuit."

In another case, brought under Pennsylvania's Right to Know Act, the court found that records pertaining to snowmobile registrations were protected by the DPPA. Henry Hartman, who published the newsletter for the Pennsylvania State Snowmobile Association, argued that he was entitled to the records under the exception for use in vehicle safety because the newsletter published articles on safe use of snowmobiles. The court rejected that claim and also found that the Department of Conservation and Natural Resources, which was the custodian of the records, was subject to the DPPA as part of the Transportation Equity Act for the 21st Century.[69]

Due largely to the fact that Florida failed to revise its implementing legislation for the DPPA after the law was amended in 1999, changing the opt-out standard for bulk marketing sales to the stricter opt-in standard, there have been several class action suits brought against users of DMV records. One such suit was brought against the News-Press.[70] The plaintiffs alleged that the company had purchased bulk DMV records from the Florida Department of Highway Safety and Motor Vehicles, and was using the information without the consent of the individuals identified in the records. The plaintiffs asked for liquidated damages of $2,500 for each member of the class. In light of the Supreme Court's recent decision in a Privacy Act case, *Doe v. Chao*,[71] in which the Court ruled that a plaintiff had to first show actual damages to be eligible for the statute's $1,000 minimum recovery, the court here concluded that Congress must have intended the same analysis in an action brought under the DPPA. The court found that the newspaper could be sued for improper use of the DMV records, but because the plaintiffs had made no showing of actual damages the court concluded that it was unlikely that the plaintiffs could prevail.

Another district court judge in Florida reached a similar conclusion in *Kehoe v. Fidelity Federal Bank & Trust*.[72] However, the court's conclusion concerning the effect of *Doe v. Chao* on the award of damages under the DPPA was reversed by the U.S. Court of Appeals for the Eleventh Circuit.[73] The Eleventh Circuit ruled that plaintiffs were not required to prove actual damages to be eligible for liquidated damages of $2,500. The Supreme Court refused to hear Fidelity's appeal[74] and Fidelity settled the case by agreeing to pay $50 million.[75]

---

[68] 887 A.2d 1004 (D.C. 2005)
[69] *Hartman v. Dept of Conservation and Natural Resources*, 892 A.2d 897 (Penn 2006)
[70] *Schmidt v. Multimedia Holdings Corp.*, 361 F. Supp. 2d 1346 (M.D. Fla, 2004)
[71] 540 U.S. 614 (2004)
[72] 2004 U.S. Dist. LEXIS 11464, S.D. Fla, June 14, 2004.
[73] *Kehoe v. Fidelity Federal Bank & Trust*, 421 F.3d 1209 (11th Cir. 2005)
[74] *Fidelity Federal Bank & Trust v. Kehoe*, 126 S. Ct. 1612 (2006)
[75] *Kehoe v. Fidelity Federal Bank and Trust*, EPIC news archive, www.epic.org/privacy/drivers/kehoe.html

The success of the Fidelity suit was based largely on Florida's failure to implement the opt-in amendment to the DPPA. Plaintiffs trying to sue data brokers and similar organizations in other jurisdictions have been much less successful. In *Russell v. ChoicePoint, Services, Inc.*,[76] the court rejected a claim against ChoicePoint, Lexis-Nexis, and other data brokers for impermissible use of personal information from motor vehicle records. Russell argued that the companies violated the DPPA by reselling the records to third parties. But the court disagreed, finding instead that § 2721(c), which allows for resale of DMV records to authorized recipients for uses permitted under the act, provided the legal basis allowing the Louisiana Department of Motor Vehicles to sell the records to the data brokers. Under similar circumstances, the U.S. Court of Appeals for the Tenth Circuit ruled that Image Data, a company that was developing an electronic identification system to be used at retail stores that relied primarily on personal information obtained from drivers' license records, was eligible to receive the information under the DPPA's exception for use in preventing financial fraud and similar crimes.[77]

Several other cases have dealt with whether a company or individual was eligible to receive DMV records under an exception in the DPPA. Rejecting the claim of a company that reformatted DMV information to computer disks and sold it to law enforcement agencies, the Iowa Supreme Court ruled that, even though its clients were eligible to receive the information, the company's use of the information did not fit within a permissible use of the records.[78] The U.S. Court of Appeals for the Seventh Circuit dismissed Kenneth McCready's attempt to require the State of Illinois to disclose DMV records to him so that he could use them to better identify lien holders of security interests in used automobiles that McCready bought and sold. Rather than determine whether or not McCready fit within an exception to non-disclosure, the court ruled that he did not have a private right of action to force disclosure of DMV records. The court pointed out that "what is missing is not jurisdiction but a right of action. The statute authorizes private suits, but only by persons whose information has been disclosed improperly."[79]

Conclusion

FERPA, HIPAA and the DPPA are all somewhat different legislative responses to specific problems, but together they form a constellation of privacy protections that have created significant restrictions on access to the kinds of records to which they pertain. The original passage of FERPA seems to be driven by the personal interest of Sen. Buckley and it wasn't until the law was implemented and narrowly interpreted by schools that its bite was truly felt. HIPAA represented a long overdue recognition that medical information deserved greater privacy protections and, while the Privacy Rule, and particularly its interpretation by healthcare providers, has probably gone a bit further than necessary in some respects, providing privacy protections to medical records is certainly a worthy goal. The DPPA was a response to anecdotal reports and, as such, produced what critics saw as a legislative overreaction whose protections were largely vitiated by broad exceptions allowing various kinds of commercial uses of the records. Congress only partially resolved the legitimate use of such information by the press and its allies in the non-profit world, and even that imperfect solution in the law was taken away by the Shelby amendment. Congress did little to respond to the concerns of states that used this information as a source of revenue. Although the revenue value of DMV records is not an adequate reason for

[76] 302 F. Supp. 2d 654 (E.D. La, 2003)
[77] *Miller v. Image Data LLC*, 91 Fed. Appx 122 (10th Cir. 2004)
[78] *Locate.Plus.com, Inc. Iowa Department of Transportation*, 650 N.W. 2d 609 (Iowa 2002)
[79] *McCready v. White*, 417 F. 3d 700 (7th Cir. 2005)

failing to protect privacy, there was no real discussion of how states might be able to make up the expected loss in revenue. The press probably should have negotiated an exception for itself and, at least in my opinion, that was a strategic mistake. It is probably too late to go back and provide such an exception, but the law would certainly be more palatable if there were some vehicle for access for public interest purposes. That statement holds true for all three statutes and none of them contains a remedy that might result in disclosure on public interest grounds.

Aside from the limited rights in the DPPA, all three statutes provide no right of private action, a serious flaw in that individuals whose information has been improperly maintained, used, or disclosed certainly have the greatest incentive to pursue such an action. Requiring that the Education Department, the Department of Health and Human Services, or the Attorney General bring any action to ameliorate problems is not a particularly satisfactory policy to ensure compliance. Nevertheless, what all three statutes also have in common is that they have generated such a pervasive fear of the results of non-compliance that impacted institutions would much rather risk a suit under the relevant public records statute than to disclose information covered by either of the three statutes. Perhaps more cynically, the statutes allow the impacted institutions to justify a natural resistance to disclosing information in the first place.

Whatever the shortcomings of these three statutes and the impact they have had on access to information, it now seems clear that a social and political demand to cut back on access to personal information was inevitable. The rapid strides made by technology have made it much easier to manipulate personal information in ways that are both good and bad. And, unfortunately for access advocates, the advent of identity theft has provided a realistic concern strong enough to move politicians and policymakers towards solutions that protect against the misuse of personal information in public records. Access advocates have always urged that laws should be designed to punish the misuse of information rather than to restrict or prohibit its public availability. But the easy availability of such information is likely too tempting a target for identity thieves and that issue in and of itself would almost certainly have driven the public access/privacy protection debate in the direction of greater privacy protections. In the end, with or without FERPA, HIPAA and the DPPA, the imperative towards protecting personal information seems inevitable.