SHIFTING STANDARDS IN CAMPUS PRIVACY

This primer for boards lays down the law on privacy issues—from student records, to computer files, to crime, to new security concerns.

LEGAL ISSUES RELATING TO PRIVACY at colleges and universities arise in a variety of contexts. "Privacy law" comprises a disparate array of statutes and legal doctrines that affect activities as varied as health care, telecommunications, banking, and human resources, to name only a few.

Many of the laws addressing privacy on campus seem to embrace either of two conceptions of the university's role. According to one conception, universities should protect their students from the peering eyes of government and the public. This principle is reflected, for example, in the policies of some campus police departments that traditionally have opted to address minor (and sometimes more serious) crime through the campus judicial system rather than turn students over to local law enforcement. Laws such as the Family Educational Rights and Privacy Act (FERPA), which charges colleges with protecting student privacy, seem broadly consistent with this view.

Another set of laws, though, casts the college more as a monitor of student (and faculty) compliance with government rules. This type of law primarily charges the institution not with protecting privacy but with turning over to the government information about students or faculty. Examples of this latter view seem to abound in legal reforms enacted after the 9/11 terrorist attacks.

For higher education officials, government regulation in the privacy arena seems to pose an array of new challenges. In part this is because colleges and universities do so much in addition to providing education, but it is also because the law imposes special privacy regulations on colleges and universities.

Traditionally, legal safeguards on privacy emanated principally from the U.S. Constitution and state common law. Since the 1970s, however, the federal government and the states have added a panoply of statutes and regulations designed to protect privacy in various contexts. Although many of these reforms have benefited students and others, the growing web of privacy laws also presents challenges.

When privacy-related issues arise in an institution's day-to-day functioning, practical

• BY ALEXANDER E. DREIER •

Illustration by Jeffrey Smith


John Q. Student
Geoffrey Smith 05

Ambiguities exist over the confidentiality and disclosure requirements of different laws. The courts have yet to resolve competing interpretations.

necessity often dictates that common sense substitute for fine-grained legal analysis, and when legal analysis is required, most colleges and universities turn to the general counsel. But boards of trustees should become conversant with major areas of the law both to help their presidents avoid costly litigation and to help produce sound policies in all institutional pursuits. What follows is a primer that illustrates for trustees some of the areas on which privacy law may affect institutional policy.

Student Records. No privacy legislation in recent years has vexed college and university officials more than FERPA. Also known as the Buckley Amendment, it generally prohibits higher education institutions from disclosing student records without the student's consent. The law's applicability to various campus activities and its catalogue of disclosure rules and exceptions mean that it must be taken into account in an array of institutional decisions. For example, it may affect policies on parental access to student academic transcripts, public release of information on student-athletes, and decisions on which institutional officials have rights to student databases.

The 1996 Health Insurance Portability and Accountability Act (HIPAA) generally protects the confidentiality of patient health information. HIPAA's privacy rule does not cover student records that are subject to FERPA, but it nonetheless may affect various university activities—from restrictions on use of patient information in clinical trials to the operations of academic medical centers. Because FERPA and HIPAA have different requirements, colleges and universities need sensitive institutional policies for managing student health information.

It is not always obvious which privacy laws apply to higher education. For example, the Gramm-Leach-Bliley Act, which Congress aimed at confidential information handled by financial institutions, can have implications for colleges and universities in their role as lenders. The Fair Credit Reporting Act includes rules on background checks that may come into play in the hiring process.

Colleges and universities also must take account of more time-tested sources of privacy rights. Most state courts recognize tort claims for invasion of privacy or publicizing private facts, though the parameters of these doctrines vary from state to state. False statements that damage reputations can give rise to state-law defamation claims.

At public institutions, the Fourth Amendment bars unreasonable searches and seizures and can form the basis for claims for damages and attorneys' fees. Public *colleges* do not enjoy the leeway the U.S. Supreme Court has given public *schools* to drug-test students. The court's 2002 decision in *Board of Education v. Earls,* which permitted public school drug-testing of students who participate in extracurricular activities, serves as a reminder of the different legal standards for public schools and higher education institutions.

Student Disciplinary Records. In cases of alleged student misbehavior, colleges and universities must balance thoughtfully the rights of victim and accused. As many university lawyers know, this balancing is required to satisfy the interplay between FERPA and what is called the Clery Act. Whereas FERPA generally protects the confidentiality of student records, the Clery Act specifically addresses when crime victims or the public may learn the results of student disciplinary hearings. It requires an institution to disclose disciplinary information to the victim of a sex offense (when the accused is found responsible) and permits disclosure to the public in other circumstances (in connection with a crime of violence).

Unfortunately, Congress did not clearly delineate how these Clery Act requirements

may be squared with FERPA, and the Education Department has not acted decisively to resolve these ambiguities. For example, from the mid-1990s until as late as March 2003, the Education Department's Family Policy Compliance Office (FPCO) seemed to endorse the institutional practice of requiring victims to keep disciplinary hearing results confidential. According to FPCO, "When an institution discloses the final results" of a disciplinary hearing to a sex-crime victim, "it must also inform the student that FERPA does not permit any redisclosure of this information." But a few months later, another office of the department seemed to reverse that interpretation, ruling that a university may not deny hearing results to sexual assault victims who refuse to sign a nondisclosure agreement. These interpretations have not been definitively tested in court.

Parental Access. At times, student privacy law conflicts with parents' expectations. When a troubled student reveals a mental health problem, for example, under what circumstances should college officials notify the student's parents? Under FERPA, parents of college students generally do not have a right to student records, and indeed FERPA may *forbid* disclosure to them. One broad exemption allows disclosure to parents if a student is a "dependent," as defined by the Internal Revenue Code.

Disclosure also may be permitted in a health or safety emergency or (if the student is under 21) if the student violates school drug or alcohol policy. (Medical treatment records are not covered by FERPA but may be subject to disclosure limitations under HIPAA.) However, none of these FERPA exceptions *requires* that institutions disclose student records to parents.

Thus, in some circumstances, college officials may have discretion regarding when to share with parents private information about students. Exercise of that discretion requires judgment and may entail liability risk for the institution. For example, if a student commits suicide or harms a classmate, questions may be asked about what counselors or faculty knew about the student's mental state and whether parents should have been informed.

On the other hand, counselors, faculty, or other college personnel may believe they have an obligation to preserve student confidences. State laws vary regarding legal privileges that attach to various counseling and treatment relationships (doctor-patient, counselor-counselee, pastor-parishioner, to name a few), as well as on the scope of the "duty to warn" a potential victim of foreseeable violence. Balancing liability risks is not always easy, and tough ethical questions often arise.

Sexual Harassment and Assault. Confidential revelations of sexual harassment or assault present some of the most difficult challenges for student privacy policy. How much confidentiality can a counselor guarantee to a student who confides that she was the victim of harassment or assault? Suppose the student does not wish to pursue the matter and fears having her accusation disclosed to the accused? The counselor may want to respect this wish but also protect potential future victims.

The institution's lawyer will point out that under Title IX of the 1972 Education Amendments (the same federal statute that mandates gender equity in athletics) courts have held liable institutions that failed to act to prevent known harassment of a student by a peer or a teacher. Thoughtful attention should be given to communicating clearly to students the limits on confidentiality of their communications with faculty and counselors in this sensitive area.

References and Recommendations. Employment or graduate-school recommendations that college or university employees provide for students or faculty can give rise to privacy-related claims against the institution. Some state courts have held that a false recommendation that conceals negative information can be the basis for a fraud or negligence claim. State

Confidential revelations of sexual harassment or assault present some of the most difficult challenges for student privacy policy.

employment-reference shield laws, designed to protect good-faith referees, are subject to judicial interpretation and may not in all cases fully immunize employers against claims arising out of negative recommendations.

A recent case involving Gonzaga University is instructive. In 1993, Gonzaga administrators became aware of allegations that a male student had sexually assaulted his girlfriend, another Gonzaga undergraduate. When Gonzaga was called upon to provide a character reference for the male student, later identified in court papers as John Doe, for his state teaching license application, university administrators balked, and later disclosed Doe's identity to state officials.

After the state denied the license, Doe sued Gonzaga for violation of FERPA, as well as defamation, negligence, breach of contract, and invasion of privacy. A jury in Washington State returned a $1.1 million verdict for Doe, finding Gonzaga liable for violating FERPA, though the U.S. Supreme Court later reversed the decision, ruling that individuals cannot sue under federal civil-rights law for violations of FERPA. Because courts already had held that FERPA also does not provide a direct private right of action, institutions should not face future suits for damages for violation of FERPA. (Full disclosure: The author and his law firm represented Gonzaga in its Supreme Court appeal.)

However, institutions still may be liable under state law for violation of student privacy. In *Gonzaga*, for example, the student was permitted to recover on his state-law claims. In addition, the U.S. Department of Education remains active in investigating complaints of FERPA violations.

Post-9/11 Security. One common effect of the USA Patriot Act and related laws aimed at addressing such issues as bioterrorism and immigration has been to facilitate the flow of information from universities to the federal government. For example, the Patriot Act amended FERPA to allow institutions to give student information to law-enforcement officials in terrorism-related federal investigations without informing the student. And the new Student and Exchange Visitor Information System (SEVIS) requires institutions to track international students more rigorously.

Similarly, post-9/11 rules on university research require more university reporting of information on faculty and students. Under regulations mandated by the 2002 Public Health Security and Bioterrorism Preparedness and Response Act, researchers who possess certain biological substances known as "select agents" (smallpox and a host of other exotic germs) must undergo an FBI background check. Nationals of certain countries and persons with a history of drug addiction, crime, or dishonorable discharge from the military may be disqualified.

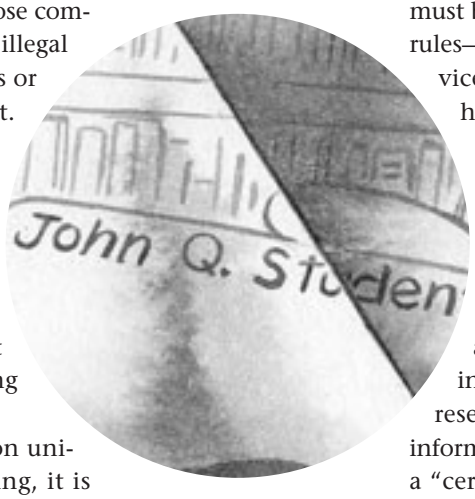
Because the select-agent rules charge universities with transmitting required information about researchers to federal agencies, they can place an institution in awkward positions. For example, a university that wishes to confirm that a prospective faculty member or graduate student will qualify to work with select agents may have to ask uncomfortable questions about the applicant's personal habits or his or her past.

If such an applicant reveals a history of drug use, how should this affect the employment decision? Is the applicant protected from discrimination on that basis under the Americans with Disabilities Act or other laws? In lieu of asking specific questions, some institutions may choose simply to offer a list of the regulatory disqualifying criteria and ask applicants who wish to work with select agents to confirm that they qualify.

Digital File-Swapping. Questions about privacy and reporting also come into play when

universities address student computer file-swapping of copyrighted music, movies, and video games. Clearly, students who engage in this practice may face personal legal repercussions. The 1997 No Electronic Theft Act makes unauthorized file-swapping a federal offense, and file-swappers also may be liable for violation of the Digital Millennium Copyright Act (DMCA). In 2003, students on several campuses who enabled file-sharing agreed to settle suits brought by the Recording Industry Association of America.

Some argue that these developments also create liability for the universities whose computer servers are used by students for illegal swapping, under theories of vicarious or contributory copyright infringement. The DMCA prescribes steps, which serve as a safe harbor, that a university or Internet service provider (ISP) may take to respond to infringement claims. Some universities have responded to such claims by disciplining file-swappers or, in at least one case, banning use of file-swapping software.



But while pressure has mounted on universities to thwart illegal file-swapping, it is unclear how far the law requires them to go. Even as many universities are weighing whether to configure software that tracks student downloading of pirated files, some have argued that the DMCA does not require a university or an ISP to monitor the private hard drives of individual users.

To take the argument a step further, intrusive monitoring of networks might conceivably create liability for a university. With detailed monitoring, could the university come to know more than it would like to know about a student's personal life? The contributory infringement doctrine, for example, generally does not apply unless the defendant has knowledge of the infringement. Aggressively invasive monitoring of student downloads may prompt student claims under a variety of legal theories. Student privacy concerns under FERPA and state law also may warrant, at a minimum, notification of the student before an institution responds to a subpoena requesting file-sharing information.

Research Data. Another area of potential risk for colleges and universities is litigation over breach of confidentiality in their capacity as sponsors of research. Specifically, privacy issues may be presented when research is conducted that collects human tissue, DNA, or confidential data regarding research subjects. HIPAA must be taken into account, but another set of rules—Department of Health and Human Services (HHS) regulations on protection of human subjects—also applies.

The HHS rules require that an institutional review board approve federally sponsored research that involves human subjects. Researchers must safeguard confidentiality in their research and disclose to subjects the risks associated with the study, including the risk of inadvertent breach of confidentiality. For research involving particularly sensitive information, an institution may seek from HHS a "certificate of confidentiality" designed to protect research results from compelled disclosure. In addition to these protections, many states have enacted statutes that require special confidentiality safeguards for genetic testing.

Compliance with privacy laws and regulations is mandatory. But in some areas the appropriate degree of protection for student and faculty privacy may be unclear, particularly where privacy concerns conflict with other legal obligations. With no abatement in privacy regulation in sight, colleges and universities will be well served by administrators and trustees who keep privacy concerns on their radar screens. ◆

Alexander E. Dreier (aedreier@hhlaw.com) is a partner in the higher education practice at the law firm of Hogan and Hartson in Washington, D.C.