Privacy in the University Setting

Beth E. Cate, Esq.
Associate University Counsel
Indiana University[1]

I. Everyone's talking about privacy

America is in the grip of a national debate about privacy—what it means, why we value it, how much we value it, and how much we should protect it when doing so may conflict with other cherished values. The media is dominated with stories involving privacy issues:

- In December 2005, the New York Times broke the story that the National Security Agency is conducting warrantless electronic surveillance of international communications involving US citizens. Since then, members of Congress, the Executive Branch, the media, and interest groups have been debating vigorously whether the NSA program strikes a lawful and appropriate balance between protecting privacy and preserving national security.

- An equally energetic debate on privacy was catalyzed by the recent Supreme Court confirmations of John Roberts and Samuel Alito. Members of the Senate, the Executive Branch, the media, and interest groups have been debating vigorously whether the Supreme Court, with these newest members, will continue to recognize a federal Constitutional right to privacy that encompasses the lawful choice to have an abortion, subject to the government's power to regulate abortion after fetal viability in the interests of the mother's or fetus's life and health.

 The views expressed in this essay and the accompanying presentation are those of the author and should not be attributed to, or blamed on, any office or official of Indiana University. My thanks to Elizabeth Armstrong, Laura Hamilton, Dick McKaig, and Damon Sims of Indiana University for their many valuable insights.

- Hardly a week goes by without the news media reporting a security breach that has exposed personal data in an electronic database and created the risk of identity theft. The Privacy Rights Clearinghouse reports that since February 2005, when the Georgia-based information company ChoicePoint disclosed that it had mistakenly sold personal information of 163,000 persons to a crime ring involved in identity theft, there have been 113 reported incidents of data security breaches involving the exposure of personal information. Roughly half of those – 54 – involved colleges or universities.[2] Lawmakers and enforcement agencies are scrambling at the state and federal levels to require entities that maintain personal information to better protect it against unauthorized disclosure and use.

These examples illustrate two points. First, as a legal and policy matter, the catch-all word "privacy" encompasses all sorts of disparate notions – the examples above include freedom from government eavesdropping, autonomy in making certain personal or family decisions, and control over disclosure and use of personal data. As I discuss further below, the law offers no single definition of privacy and no single "the right to privacy." Instead it recognizes, under the headings of privacy and liberty, a variety of interests that are given protection against intrusion or interference by the government or private parties, because those interests reflect values that are felt to be central to our individual well being, our collective self-image as a free nation, and our democratic self-governance.

Second, the debate about protecting privacy inevitably involves balancing privacy interests against other important interests and values: in the case of the NSA wiretap program, preserving national security; in the case of the Supreme Court's treatment of *Roe*, government interests in preserving the life and health of pregnant women and the unborn; in the case of electronic data privacy and security, the interest in preserving enough third-party access to personal data to allow for sound economic and policy decision making, news reporting, and other valuable activities. With the exception of the

[2] "A Chronology of Data Breaches Reported Since the ChoicePoint Incident," available at http://www.privacyrights.org/ar/ChronDataBreaches.htm (current as of February 3, 2006).

sort of privacy we enjoy as part of our absolute right under the First Amendment to think and believe in our own minds whatever we want, privacy rights are not absolute in the law. Nor should they be. While as individuals we may need a measure of undisturbed personal space and solitude in order to reflect, introspect, self-protect, and so on, as members of families, friendships and communities, we need to share personal information in order to build relationships and fulfill our common obligations and objectives.

College campuses are no strangers to privacy concerns, particularly involving students. But these days, many factors are contributing to a reassessment on campus of how to properly balance protection of student privacy with other important values and interests, including but not limited to:

- Protecting students from a variety of risks that may arise from student use of information technologies to share personal information about themselves—how and how much should schools intervene?
- Intervening institutionally and involving parents or others as needed to address students' emotional and developmental needs, to improve their chances of academic success, promote their physical and emotional well being, and prevent them from inflicting harm on themselves or others—when is the right time and what is the right way to intervene?
- Fully investigating student allegations of discrimination, harassment, and other wrongdoing by faculty and others—how do schools deal with student fear or reluctance to participate?
- Preventing and redressing unlawful use of university facilities by students—how much should schools monitor network use for unlawful file sharing?

The law can contribute meaningfully to debate over these issues, but it cannot, on its own, fully elucidate or resolve them. Insight and input from other disciplines are needed: sociology, psychology, public health, and informatics, to name a few. As a lawyer, I will

start where I am most familiar, and offer a summary of privacy law that can provide a backdrop to a broader discussion of how to construct and articulate a shared set of privacy norms that make sense on campus. Then I will move on to that broader discussion.

II. An overview of US privacy law

Privacy law in the US may be thought of as encompassing several different strands that overlap to some extent in the underlying values they attempt to serve under the heading of privacy or liberty:

- Protection against the unauthorized disclosure or use of personal information, by the government or private parties;
- Redress of harm caused by highly offensive invasions of one's privacy by government officials or private parties;
- Protection against unwarranted government intrusion on one's thoughts, beliefs, communications, and transactions; and
- Protection against unwarranted government regulation of certain personal decisions.

A. Common law privacy rights

Louis Brandeis and Samuel Warren are widely considered to have inaugurated the notion of privacy law in 1890 when they published "The Right to Privacy" in the Harvard Law Review.[3] A century before the wretched excesses of today's paparazzi, they argued that the law should allow individuals to sue for invasion of privacy when the press, using their newfangled photographic and mechanical equipment, intruded inexcusably on the lives of citizens.[4] The authors rejected the notion that you can only claim a right to privacy if you

[3] Brandeis, Louis D. and Warren, Samuel D., "The Right to Privacy," *Harvard Law Review*, Vol. IV No. 5 (Dec. 1980).
[4] *Id.* ("Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.' For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons…").

have some underlying and separately recognized property right in the facts or expression you wish to withhold from the public. Instead, they argued, legal protection of privacy is and should be grounded in the "more general right of the individual to be let alone."[5]

The "right to be let alone," as Warren and Brandeis described it, amounted to letting you decide for yourself whether, when, and to what extent you will publish your personal information, and letting you sue others for the harms, including injury to your feelings, that result when others invade your privacy. They focused on protecting one's "private" life (for example one's family life), acknowledging that the law should protect the broad disclosure of data concerning someone's fitness for public office, discharge of public duties, or other matter of public policy interest.

By 1960 many states had recognized one of more forms of the common law privacy tort that Warren and Brandeis had proposed, including "intrusion upon seclusion," "public disclosure of private facts," and "false light publicity." These torts are generally defined as follows:

- Intrusion upon seclusion: a physical or other intrusion upon the seclusion or solitude of another, that would be highly offensive to a reasonable person
- Public disclosure of private facts: public disclosure of private information that would be highly offensive to a reasonable person and that does not involve a matter of legitimate public concern
- False light publicity: publishing information about someone that is false and that would be highly offensive to a reasonable person, where the publisher knew the information was false or was reckless about its truth or falsity

By requiring in each instance that the privacy invasion be "highly offensive to a reasonable person," though, these torts narrowed the scope of "the right to be let alone"

[5] *Id.*

to the right to be free from intrusions on solitude and misuses of personal information that cause grave emotional or reputational harm. These limitations generally reflect a balancing of privacy interests against strong societal interests in widespread access to information on which to base personal and public policy decisions.

B. Statutory and Contractual Information Privacy Rights

Colleges and universities are familiar with statutory protection of data privacy; for the past thirty years, the Family Educational Rights and Privacy Act (FERPA) has shaped schools' privacy practices with respect to student education records, a broadly defined term. Generally FERPA places control over the disclosure and use of student education records in the hands of the student, and enhances that control by requiring schools to give students annual notice of their rights and how schools will treat their data (what data will be treated as directory information, what officials will be deemed to have a legitimate educational interest in accessing records), and by allowing students to view and petition to correct their records and to learn of disclosures of their records.

The statute carves out a number of exceptions to the general principle of student control over disclosure and use of their data. These exceptions permit schools to share records without student consent in the interest of serving important competing values and policies. For example, the statute allows a school to:

- Share records in an emergency as needed to protect the health and safety of the student or others
- Share records with state education officials, educational testing organizations, and accrediting bodies, to better inform education policy
- Share records with a subsequent school to which a student applies for admission, to guard against misrepresentation by that student of his or her record
- Share with the victim of a violent crime or nonforcible sex offense the final disciplinary action taken against the student offender, in recognition

of the victim's deep personal interest in the outcome and in being part of the process

- Report drug and alcohol violations to parents of minor students

FERPA thus demonstrates a conscious balance of privacy interests and other educational, community, and public welfare interests. More recent data privacy and security statutes that schools must navigate, like HIPAA and Gramm Leach Bliley, follow suit by establishing a general framework of individual control of personal data tempered with exceptions for nonconsensual disclosures that serve important competing values. Other state and federal statutes grant protection for specific types of records that are deemed to be especially deserving of privacy, such as library patron records and Social Security Numbers. For example, many state open records laws exempt such records from disclosure; other state laws require encryption of such information and shredding it when it is no longer needed. Finally, a number of states have passed laws requiring institutions to notify individuals promptly when a systems breach occurs that exposes personal data to unauthorized access, and similar federal legislation has been proposed.

A major debate concerning privacy legislation is how much the law should value and therefore protect an individual's control over disclosure and use of his data, and how much the law should instead focus on preventing and remedying harmful uses of that data. Notably, statutes like FERPA and HIPAA do not require a showing of actual harm for an unauthorized disclosure to be a violation. Arguably these statutes presume that harmful consequences are likely to flow from unauthorized access, such as identity theft, decreased trust in data systems, decreased willingness to transact with such systems, and so on. But they may also reflect a sense that unauthorized access to personal information may be harmful *per se*, by depriving someone of control over the release of information about themselves. According to privacy law scholar Fred Cate, this emphasis on the value of control is the dominant trend in modern data privacy law, with legislators responding to "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communication to

others" – regardless of whether a particular use or disclosure of data is causing or likely to cause harm.[6]

The Federal Trade Commission's "core principles of privacy protection," which it advocates as a basis for any further data privacy regulation as well as voluntary organizational privacy practices, sound this theme. The core principles consist of:

- Giving notice to individuals of the personal data that an institution collects, before that information is collected, so that the individuals can make an informed choice as to whether they want to surrender their information in exchange for any benefits they may receive;
- Giving individuals options as to how their personal data may be used, and allowing them to opt out of uses they do not agree to (with the understanding that they may have to forego certain benefits or transactions unless their data may be used as proposed);
- Allowing individuals through simple and inexpensive means to review the data an institution collects about them and to contest the data's accuracy and completeness; and
- Taking reasonable steps to ensure that data collected is accurate (by using only reputable sources, destroying old and inaccurate data, and so on) and secured against unauthorized use or disclosure.[7]

The FTC's principles reflect a classic free market approach to determining the value of something, in this case privacy. They allow the individual to choose, based on full information, whether to transact with the organization that wishes to collect and use his data, and whether relinquishing certain levels of privacy (e.g., allowing the collector to share his data with affiliates) is worth whatever benefits or services the collector is offering in return. The law does not attempt to value individual privacy or protect it

[6] Fred H. Cate, "The Failure of Fair Information Practice Principles," forthcoming in *Consumer Protection in the Age of the 'Information Economy'* (quoting Alan F. Westin, *Privacy and Freedom* 7 (1967)).
[7] Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace—A Report to Congress* 11 (2000).

beyond the level set by these market forces. The law will enforce whatever bargain is struck, but as a matter of protecting contractual rights, not privacy *per se*. If an organization that collects personal data fails to adhere to the terms of its own privacy policies, an individual may sue for breach of contract, although the policies may impose significant barriers to a lawsuit, like requiring any disputes or litigation to be brought in a particular state or severely limiting recovery of damages.[8]

Some argue that the law should not emphasize individual control over the disclosure and use of personal data, for two reasons. First, such control is often illusory. Most people do not read the detailed, legalistic, and thoroughly boring privacy notices that the law requires – many do not even open them, according to a US Postal Service study[9] – so the assumption that people are making informed choices as to whether to transact with the organizations sending them is incorrect. The same goes for all those online privacy notices that few read or understand. Cate reports that in 2002, an average of .3 percent of Yahoo's users read its privacy policy.[10] Many privacy policies expressly state that the organizations posting them reserve the right to change them unilaterally, and it is up to the individual to keep checking to see what the current terms are, which very few are likely to do. If they do read the terms and disagree with them, they cannot negotiate changes – the only real choice they have is to forego the activity for which data collection is a prerequisite. So far, available data suggests that when confronted with such a choice, many people do not value their informational privacy as much as, for example, a Starbucks latte: in May 2005, VeriSign, an internet security company, approached 272 people and found that two thirds of them willingly gave up their company computer password in exchange for a $3.00 Starbucks coupon.[11]

[8] If the organization is a commercial entity subject to the jurisdiction of the FTC, the FTC may bring an enforcement action claiming an unfair or deceptive trade practice. See, e.g. See *In the Matter of* Guess?, Inc. and Guess.com, Inc., at http://www.ftc.gov/os/2003/06/; *In the Matter of* Microsoft Corporation, at http://www.ftc.gov/os/2002/08/; *In the Matter of* MTS, Inc. d/b/a Tower Records/Books/Video, at http://www.ftc.gov/os/caselist/0323209/0323209.htm; and *In the Matter of* Eli Lilly and Company, at http://www.ftc.gov/os/2002/05/.
[9] See Cate, supra.
[10] *Id.*
[11] "Many Would Trade Password for A Grande Mocha," TechWebNews, May 6, 2005.

Second, giving individuals control over their information imposes substantial costs—not only the financial costs of sending privacy notices and complying with opt-out requirements, but the costs of burdening free speech. Eugene Volokh of UCLA Law School argues forcefully that laws prohibiting third parties from sharing information about someone are classic speech restrictions that are strongly disfavored under the First Amendment. Rejecting the Warren-Brandeis distinction between protecting "private" facts and sharing "public" ones, Volokh argues that private facts – what people buy, their credit history, whether they've been convicted of a crime – can be as valuable to the recipients of that data in making decisions as classic "public interest" information. For example, an employer will want to know about a job applicant's criminal record or credit history, and may well not want to rely on the applicant's own word for it.[12]

C. Constitutional Privacy Protections

1. First and Fourth Amendment rights

Thirty years after the publication of the Harvard Law Review piece, then-Justice Brandeis developed the theme of a "right to be let alone" in his famous dissent in *Olmstead v. United States.*[13] In *Olmstead* the Supreme Court held that wiretapping telephone wires on a street outside Olmstead's home did not constitute a "search or seizure" under the Fourth Amendment, since the police had not physically invaded Olmstead's property or taken his tangible belongings. Rejecting this view, Justice Brandeis wrote that

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect

[12] Eugene Volokh, "Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You," in 52 Stanford L. Rev. 1049 (2000); Eugene Volokh, "Personalization and Privacy," in *Communications of the Association for Computing Machinery*, Vol. 43 No. 8 (Aug. 2000).
[13] 277 U.S. 438 (1928).

> Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the government, the right to be let alone-the most comprehensive of rights and the right most valued by civilized men. To protect, that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.

The Supreme Court ultimately adopted Justice Brandeis' view. Forty years later, in ***Katz v. United States***,[14] the Court held that federal law enforcement officials violated the Fourth Amendment by bugging the public phone booth in which Mr. Katz was transmitting illicit wagering information to other states. The Court concluded that the Constitution protects the privacy of communications that an individual subjectively considers private and that society is prepared to treat as private. "[T]the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection….But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[15]

Two years after ***Katz***, the Court again cited Justice Brandeis' dissent, this time to help flesh out privacy rights that are accorded by the First Amendment rather than the Fourth. The Court held that the First Amendment protects the right of an individual to read or watch, in the privacy of his own home, any material he likes, even obscene material that otherwise is not protected by law. In ***Stanley v. Georgia***,[16] the Court struck down a Georgia statute prohibiting the mere possession of obscene materials, reasoning that

> The right to receive information and ideas, regardless of their social worth, … is fundamental to our free society….[A]lso fundamental is the right to be free, except in very limited circumstances, from unwanted governmental intrusions into one's privacy….If the First Amendment means anything, it means that a State has

[14] 389 U.S. 347 (1967).
[15] *Id*. at 352.
[16] 394 U.S. 557 (1969).

> no business telling a man, sitting alone in his house, what books he may read or what films he may watch.[17]

The First Amendment also protects one's privacy to develop thoughts and beliefs and to convey them without government compulsion, censure, or repression. For example, the First Amendment protects the right to be free from government compulsion to speak on a topic or convey a particular message[18]; the right to speak anonymously[19]; and the right to keep our organizational memberships and affiliations confidential.[20]

These privacy protections serve both individuals and society. The individual benefits are well known to sociologists:

> A person needs time and privacy in which to assess the flood of information received, to consider alternatives and possible consequences so that he may then act as consistently and appropriately as possible…privacy operates as a kind of buffer between social pressures upon the individual and his response to them, a

---

[17] *Id*. at 564-65.

[18] In 1977, the Court held that a New Hampshire couple could not be compelled to display on their license plates the state motto, "Live Free or Die," which they said contravened tenets of their Jehovah's Witness faith. *Wooley v. Maynard*, 430 U.S. 705 (1977). In *Wooley*, the Court emphasized that

> [T]he right of freedom of thought protected by the First Amendment against state action includes both the right to speak freely and the right to refrain from speaking at all….The right to speak and the right to refrain from speaking are complementary components of the broader concept of "individual freedom of mind….Here … we are faced with a state measure which forces an individual, as part of his daily life - indeed constantly while his automobile is in public view - to be an instrument for fostering public adherence to an ideological point of view he finds unacceptable. In doing so, the State "invades the sphere of intellect and spirit which it is the purpose of the First Amendment to our Constitution to reserve from all official control."

Id. at 715 (quoting *West Virginia State Bd. of Ed. v. Barnette*, 319 U.S. 624 (1943), in which the Court held that requiring schoolchildren of the Jehovah's Witness faith to salute the American flag, under threat of expulsion, violated the First Amendment's guarantees of freedom of thought, speech and belief).

[19] See *John Doe No. 1 v. Cahill*, 884 A.2d 451 (Del. 2005) (to uncover the identity of an anonymous blogger who had criticized a city councilman and was being accused of defamation, the councilman would have to show that his defamation claim was strong enough factually to get to trial; this high standard was needed to "protect against the chilling effect on anonymous First Amendment internet speech that can arise when plaintiffs bring trivial defamation lawsuits primarily to harass or to unmask their critics.").

[20] *N.A.A.C.P. v. Alabama*, 357 U.S. 449 (1958) (state could not compel NAACP to disclose its membership lists). "Effective advocacy of both public and private points of view, particularly controversial ones, is undeniably enhanced by group association, as this Court has more than once recognized by remarking upon the close nexus between the freedoms of speech and assembly. …. This Court has recognized the vital relationship between freedom to associate and privacy in one's associations…. Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs." *Id*. at 460-62.

> buffer needed by the person and usually recognized by his fellows. But privacy does more than provide a kind of slippage between social pressure and individual response. It also protects the self; protects it from disclosure of mistakes made, motives, feelings, and actions which would be humiliating or damaging to have known….Privacy also has an ameliorative function….After bruising contact with the world, privacy may be required within which self-esteem can be restored….'It is perhaps an absolute necessity to withdraw to repair one's energies, to ruminate over the significance of past events, and to plan.'[21]

The societal benefits reflect the fact that protecting freedom of thought, anonymity of speech, and so on will encourage people to participate in the marketplace of ideas, which will strengthen democratic self-governance.

Privacy rights under the First and Fourth Amendments are not absolute. The veil of anonymity may be lifted and your communications read or overheard if the government can show that your speech is either unlawful or relates to unlawful activity. Similarly, courts will allow the government to collect and maintain personal data when it can demonstrate a legitimate interest and adequate data security measures.[22]

---

[21] Bates, Alan P., "Privacy—A Useful Concept?" in *Social Forces*, Vol. 42, No. 4 (May 1964), at 432-33 (quoting Alfred R. Lindesmith and Anselm L. Strauss, Social Psychology (New York: The Dryden Press, 1956), at 213-17); *see also* Jourard, Sidney M., "Some Psychological Aspects of Privacy" in *Law and Contemporary Problems*, Vol. 31, No. 2 (Spring 1966).

[22] See *Whalen v. Roe*, 429 US 589 (1977). In *Whalen* the Court found that the legitimate interests of the state of New York in curbing the overprescription of scheduled drugs and allowing needed disclosures for health care services and insurance coverage, outweighed patients' privacy concerns that maintaining a database would lead to misuse and mistaken disclosures, particularly when the state had taken substantial measures to secure the data. The Court did however sound a note of caution about the cumulation of vast computerized databases and suggest the constitutional balance might be struck differently with less legitimate need for the data or fewer security measures:

> We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. The collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces, and the enforcement of the criminal laws all require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed. The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures. Recognizing that in some circumstances that duty arguably has its roots in the Constitution, nevertheless New York's statutory scheme, and its implementing administrative procedures, evidence a proper concern with, and protection of, the individual's interest in privacy. We therefore need not, and do not, decide any question which might be presented by the unwarranted disclosure of accumulated private data - whether intentional or unintentional - or by a system that did not contain comparable security provisions.

Id. at 605.

Following the attacks of September 11, privacy interests have been subordinated increasingly to the real and perceived information-gathering needs of counterterrorism and law enforcement. This can affects schools directly, especially because our large foreign student (and faculty) population makes us a focus of counterterrorism efforts. The USA PATRIOT Act added an exception to the Family Educational Rights and Privacy Act that allows schools to disclose education records without student consent (and without notifying the student or maintaining any record of the disclosure) in response to an *ex parte* order obtained by the Attorney General or his designee in connection with an investigation of crimes of terrorism. Schools already were able under FERPA to disclose records without notification or recordation under exemptions for responding to grand jury and law enforcement subpoenas; to the extent that the Attorney General faces a lower standard in obtaining an *ex parte* order, however, privacy protections under FERPA may be said to have weakened.

Other provisions of the USA PATRIOT Act apply more generally but may be directed to colleges and universities. Section 215 of the USA PATRIOT Act amended federal law to permit the Federal Bureau of Investigation to obtain an order demanding any records or other tangible things – including records of what books university students and employees have checked out of the campus library and what websites they have browsed through university terminals – as long as the FBI specifies that the items are related to an authorized investigation to obtain foreign intelligence information or to protect against international terrorism.[23] Similarly, Section 505 of the Act broadened the FBI's authority to issue "National Security Letters," a form of administrative subpoena that is not reviewed or approved by a judge and that prohibits the recipient from disclosing its existence. NSLs are being used (according to some media reports, aggressively) to gather a variety of phone and internet use information as well as credit and financial data that the FBI believes may be relevant to a terrorism investigation. The data are then

[23] This provision has been at the center of the controversy surrounding the reauthorization of the Act. Section 215 is currently set to expire on March 10, along with several other provisions of the Act, unless House and Senate negotiators agree to a reauthorization.

shared within the federal government and mined for useful clues to potential terrorist activities.[24]

North Carolina State University received an NSL in Summer 2005, which sought information about a former student suspected of involvement in the July 7, 2005 London subway bombing. According to senior counsel at NC State, the NSL sought significantly more data than the FBI was entitled to under the law. The school refused to produce the records, and the FBI returned with a subpoena with which the school complied.[25]

Finally, while the lawfulness of the NSA wiretap program is currently being debated, it seems plausible that communications by foreign students may be caught up in NSA's surveillance activities as disclosed so far.

These post-September 11 law enforcement powers pose critical questions for the future conception of First and Fourth Amendment privacy rights and how those rights should be weighed alongside the legitimate data gathering needs of counterterrorism operations. First, these powers directly implicate the privacy interests and values associated with the First Amendment rights to free speech and association. When you know the government may be listening in on your conversations or reading your email, you may be less likely to speak or associate with others in the sort of open, unfettered way that we value highly because it promotes individual growth and fulfillment and contributes to the free flow of information that informs our personal decisions and public policies, although some have disputed the chilling effect of surveillance that takes the form of data mining vast caches of communications, the bulk of which may never be read by a human being. Recent lawsuits filed by the ACLU and the Center for Constitutional Rights argue that the NSA wiretap program chills investigative journalism, issues advocacy, and legal representation that involve significant communications with Muslims and others in the Middle East and elsewhere outside the United States.[26]

---

[24] See, e.g., Barton Gellmann, "The FBI's Secret Scrutiny," Washington Post, Nov. 6, 2005; Dan Eggen and Robert O'Harrow Jr., "US Steps Up Secret Surveillance," Washington Post, March 24, 2003.
[25] Gellmann, supra.
[26] See Complaint for Declaratory and Injunctive Relief in *American Civil Liberties Union et. al v. National Security Agency/Central Security Service et. al*, Case No. ____ (E.D. Mich.) (filed Jan. 17, 2006); Complaint for Injunctive

Second, no one disputes that the Fourth Amendment continues to require that the new data gathering operations be "reasonable," but reasonable people disagree on what is reasonable and who should and can make that call – an FBI agent? the Attorney General? a judge? Usually the law requires someone outside the Executive Branch to review the sufficiency of the evidence of likely wrongdoing before approving wiretaps and other orders that intrude upon the privacy of communications, as a guard against executive abuse of power. With the USA PATRIOT Act, Congress has shifted some of that authority from judges to the executive branch. In defending the NSA wiretap program, the President argues that Congress likewise has granted the executive branch broad surveillance authority, and that any gap in such authority is supplied by his Executive powers under Article II of the Constitution. The legitimacy of these arguments will continue to be debated as Congress convenes hearings on the program and courts consider the private lawsuits that have been filed challenging the program.

2. Rights to privacy and liberty in personal decisionmaking

"Privacy" is arguably a misnomer in characterizing the interest fueling most of the debate over recent changes to the Supreme Court bench. That interest is really about autonomy – the desire to make certain deeply personal decisions with little or no interference from the government. The modern legal origin of this interest is the Supreme Court's 1965 decision in *Griswold v. Connecticut*,[27] in which the Court reversed the convictions of two Planned Parenthood directors who had advised married couples on contraception. Connecticut statutes prohibited using contraception or assisting others to do so. The Court struck down the state laws as unconstitutional.

While the word "privacy" does not appear in the Bill of Rights or anywhere in the Constitution, the Court held that "specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance," that the marital relationship fell within a "zone of privacy created by several fundamental constitutional guarantees," and that decisions about conception made within

Relief in *Center for Constitutional Rights et. al v. George W. Bush et. al*, No. 06-CV-00313 (S.D.N.Y.) (filed Jan. 17, 2006).

[27] 381 U.S. 479 (1965).

that zone enjoyed constitutional protection. The Court cited privacy guarantees in the Third Amendment (right not to have soldiers quartered in one's home in peacetime); the Fourth Amendment (freedom from unreasonable searches and seizures); the Fifth Amendment (right against self-incrimination); and the Ninth Amendment (people may retain other rights not specified in Bill of Rights), to flesh out the constitutional basis for a marital privacy right that the Court called "older than the Bill of Rights."[28]

In the years following *Griswold*, the Supreme Court extended constitutional protection to other activities with deeply private and personal dimensions: the decision by unmarried couples to use contraception;[29] marriage between persons of different races;[30] the choice to have an abortion;[31] and homosexual intimacy between consenting adults.[32] The public, and to some extent the Court, continue to use the word "privacy" in discussing these cases, but the constitutional underpinning of this line of cases has shifted from the "penumbral" rights discussed in *Griswold* to the Due Process Clause of the Fifth and Fourteenth Amendments, which say that the government may not deprive you of liberty without due process of law.[33] "Due process" in this sense does not just mean that you are entitled to a hearing or some procedure before the government limits your liberty. It means that when the liberty in question is one that society has recognized as fundamental to our very notion of individual freedom and dignity – a liberty that we must have in order to think of ourselves as a truly free people – the government may only invade that liberty if it has a very good reason for doing so and does so in a limited way.

> "Although a literal reading of the [Due Process] Clause might suggest that it governs only the procedures by which a State may deprive persons of liberty, for at least 105 years … the Clause has been understood to contain a substantive component as well, one 'barring certain government actions regardless of the

[28] *Id.* at 483, 485.
[29] *Eisenstadt v. Baird*, 405 U.S. 438 (1972).
[30] *Loving v. Virginia*, 388 U.S. 1 (1967).
[31] *Roe v. Wade*, 410 U.S. 113 (1973).
[32] *Lawrence v. Texas*, 539 U.S. 558 (2003).
[33] See *Planned Parenthood of Southeastern Pa. v. Casey*, 505 U.S. 833, 847 (1992); *Lawrence*, supra at 578 ("The case does involve two adults who, with full and mutual consent from each other, engaged in sexual practices common to a homosexual lifestyle. The petitioners are entitled to respect for their private lives. The State cannot demean their existence or control their destiny by making their private sexual conduct a crime. Their right to liberty under the Due Process Clause gives them the full right to engage in their conduct without intervention of the government.").

> fairness of the procedures used to implement them.' …. It is a promise of the Constitution that there is a realm of personal liberty which the government may not enter...."[34]

As with other privacy rights, the right to make certain decisions free from government intrusion is not absolute and may be balanced against other important rights. Current abortion law permits the government to regulate abortion before fetal viability in the interest of the woman's health and the potential life of the fetus, as long as it does not unduly burden the woman's choice to have an abortion. After fetal viability, the government may regulate and even ban abortion as long as it creates an exception for protecting the life and health of the woman.

Some balance occurs at the outset, in determining whether a liberty interest is fundamental enough to warrant constitutional protection against state and federal regulation. Allowing judges to decide which interests are fundamental enough for protection under the Due Process liberty clause is highly controversial, with some arguing that this process effectively substitutes the policy preferences of unelected judges for those of elected representatives. An examination of litigation involving assisted suicide, the use of medical marijuana, and homosexual relations and marriage reveals substantial controversy over how strongly to weigh the privacy and liberty interests at issue and how much constitutional protection they should receive as a result.

III. Student privacy in the university

As in the law generally, privacy on campus does not have a single definition, and schools are confronted with the need to balance privacy interests against other important, usually conflicting, interests. This is particularly so in the context of student privacy.

Partly this reflects the evolving nature of the relationship between students and universities. In the heyday of *in loco parentis*, students essentially had no recognized

[34] *Casey*, supra at 846-47.

privacy rights. Schools regulated virtually all aspects of student lives, "from libido to laundry."[35] Privacy in the sense of liberty or autonomy in personal decisionmaking simply did not exist, in public or private institutions.

That changed in the 1960s, when student involvement in the civil rights movement and the Vietnam War, among other things, delegitimized the notion of universities as parental organizations wielding near-total control over student life. For the next few decades, the institutional relationship became more arms-length, with courts viewing students more like adults and holding them more responsible for their own behavior.[36]

More recently, a variety of forces – legal, pedagogical, technological, public relations, and cultural – may be shifting the institutional relationship with students again, not back to *in loco parentis* but toward a decrease in students' decisional autonomy and informational privacy. This poses substantial challenges for schools that wish to maintain an environment in which students are protected from harm (including harm resulting from their own immaturity) and yet given enough space to explore themselves, assume responsibility for their actions, to earn the trust of the school and trust it in turn to be acting with the students' best interests at heart.

A. Legal forces

Legally, since the 1990s courts have been more willing to find a "special relationship" between schools and students that requires schools to protect student safety and to prevent harms that are "reasonably foreseeable." Inevitably, when schools are faced with increased liability for protecting students from harm, they will want to assert the necessary control to minimize that liability, and that may well mean intruding upon a student's decisional or informational privacy.

[35] Glenn C. Altschuler and Isaac Kramnick, "A Better Idea Has Replaced 'In Loco Parentis,' The Chronicle of Higher Education (Nov. 1999).
[36] See Wendy S. White, "Students, Parents, Colleges: Drawing the Lines," The Chronicle of Higher Education (Dec. 16, 2005).

The recent proceedings in *Shin v. Massachusetts Institute of Technology*,[37] offer a case in point. The court allowed the parents of a student who committed suicide to proceed with their claims against certain administrators and staff members for failing to prevent her death (although it dismissed the claims against MIT itself). The administrators and staff had been involved for over a year in trying to address the student's mental and emotional problems, and had met the morning of her death to formulate a treatment plan. The court concluded, however, that the parents had demonstrated enough evidence that the MIT personnel did not respond promptly or effectively enough to the student's escalating threats of suicide. The *Shin* court cited another recent case, *Schieszler v. Ferrum College*,[38] in which a district court refused to dismiss a wrongful death claim against the college, the dean of student affairs, and the dormitory resident assistant following a student suicide in the dorm. The student had written three notes suggesting or stating that he intended suicide, which had been shared with the defendants. The court found that defendants knew of the "imminent probability" that the student would try to hurt himself, and therefore had a duty to protect him.

College administrators, risk management personnel, and health care professionals are struggling with how to respond to cases like *Shin* and *Schieszler*. Should they err on the side of caution and intervene more quickly and aggressively when students show signs of emotional disturbance, withdrawal, depression, and other behavior that might escalate into harm? Certainly, that would result in a decrease in student privacy, both in the sense of autonomy (requiring frequent counseling sessions or other health care procedures) and informational privacy (keeping close tabs on troubled students, seeking information about the student's health from, and sharing it with, the student's friends, family, classmates, professors, and so on, and perhaps stretching FERPA's "health and safety" and "legitimate educational interest" exceptions to do so). If a tragedy is prevented, the loss of privacy may not trouble anyone much. Most schools are more comfortable defending a breach of privacy in such circumstances than confronting grieving parents and defending against a wrongful death action.

[37] 2005 WL 1869101 (Mass. Super. June 27, 2005).
[38] 236 F.Supp.2d. 602 (W.D.Va. 2002).

At the same time, it is possible that intervening too quickly or assertively may produce harm, for example if it alienates the student or heightens feelings of depression, rejection, and abnormality. Although no one would deny that parents have compelling claims to know when their children are at risk, a policy of contacting parents right away may dissuade students from speaking openly with counselors. And if the fear of failing to prevent a tragedy (or a lawsuit) encourages schools to remove students on the margin, this may create or exacerbate the student's problems and eliminate his or her best chance for help. Assuming that schools do not get out of the student counseling business altogether, navigating these difficult shoals will require substantial input from talented and dedicated health care professionals.

B. Policy, pedagogy and public relations

Policy, pedagogy, and public relations forces are also likely to affect how schools approach the balance between student privacy and other interests. Here are some examples:

- Drug and alcohol use. FERPA now permits (but does not require) schools to notify parents or guardians, without student consent, when students under 21 years of age violate the law and school policy on drug or alcohol use or possession. This FERPA exemption reflects growing concerns over excessive drinking and drug use among college students, which has turned deadly several times in recent years. The exemption also reflects the view that schools and parents may be able to work together to combat substance abuse problems. But probably more so than with parent notification of depression or other health issues, students are likely to consider such notices an undue invasion of their privacy, in part because alcohol and drug use are often considered by students to be a normal and expected "rite of passage" in college. Deciding whether and when to notify parents is one of the most difficult privacy/prevention of harm balancing acts schools face. While schools may adopt general policies on this

issue, it is likely (and probably wise) that they will approach the use of this exemption in a case-by-case manner.

- Notification of victims of violent crimes and sex offenses: FERPA also permits schools to disclose, to victims and more generally, the final disciplinary action taken against a student who has been found responsible for committing a violent crime (defined to include forcible sex offenses and assault, which would cover for example date or acquaintance rape) or nonforcible sex offense. Notifying victims and allowing them to participate in the campus judicial process serve the critical values of acknowledging the harm done to the victim, demonstrating the institution's concern, responsiveness, and fairness, and providing closure. At the same time, notifying and involving the victim poses privacy issues with respect to the student found responsible, particularly since victims often will want to redisclose that information to others or have the institution disclose the outcome more generally on campus, and may see any attempt by the school to maintain the privacy of the student found responsible as a cover-up or an insufficient acknowledgment of the seriousness of the offense and the harm done to the victim. At that point, schools will need to balance the desire to alert others on campus to the fact that the student found responsible may be dangerous, against the desire to give that student a chance to learn from his or her errors and start over. The "privacy balance" in this type of case is particularly sensitive given the nature of the information at issue and the strong feelings that are likely to be present on all sides, not to mention the concern about possible legal risk if school officials do not notify the campus and the offense is repeated.

- Background checks and sex registries. Increasingly, students are encountering various forms of background checks or inquiries before they are admitted to study, to residence on campus, and to certain research and employment opportunities. Some background checks are required by law, such as the checks that occur as part of the visa process for foreign students and the federal background check for any student performing research with certain highly

dangerous chemical or biological agents. Others are voluntary but common, such as checking against the sex offender registries the names of student employees who work with children in campus daycare facilities or elsewhere. Now, in response to concerns about protecting the campus environment and avoiding liability and public relations damage, some schools are asking applicants for admission or residence to indicate whether they have been convicted of a crime (some limit the question to felonies), and if so, to describe the circumstances. Once schools have this information, they have to decide its significance to the admissions or residence decision. Will someone who was convicted of breaking into a home 8 years ago and stealing $50 be denied admission? On-campus housing? How about someone who was convicted 12 years ago of sexual assault? To make well-informed decisions, schools may need to get further details from or about the applicant, and they may want to share that information with other school personnel. For example, should the resident assistant of the dorm to which a student is assigned, be informed that the student was convicted 3 years ago of theft? Internet fraud? Felony drug use? Should the school monitor such students more closely to try to avoid recurrence of their crimes? These are difficult questions that

Another word about sex registries. FERPA lets schools disclose information they receive about a student being on the sex offender registry. Such information is of course publicly available, and schools will have certain clear and legitimate interests in sharing that information with relevant persons, such as when a student on the registry seeks to work with children. Taking affirmative steps to disclose the registry listing more broadly on campus raises similar questions about balancing privacy and the desire to give someone a second chance, against the concerns about putting members of the school community on their guard against possible repeat offenses and, to echo Volokh, allowing them to make up their own minds how much they want to interact with the student.

- Faculty-Student Relationships. Most schools have a policy prohibiting or restricting romantic or sexual relations between faculty members and students for whom the faculty have academic supervision or other official responsibilities. These policies serve many values – they protect the integrity of the academic process, they protect students against what may be subtly coercive interactions, they avoid the internal and external conflicts that such a relationship may spark, and they avoid the misconduct claims and litigation that well may follow when the relationship goes sour. But there is no denying that these policies intrude upon student privacy and autonomy.

- Investigating sexual harassment. Schools often confront situations in which students want to complain "informally" about faculty or staff behavior that they believe is sexual and inappropriate, but do not want to file formal complaints or have their names revealed. This poses a tension between wanting to protect the privacy of those who come forth to alert the school to a potential problem – and thereby encourage more people to feel comfortable reporting wrongdoing – and needing to investigate allegations fully and fairly. Pledges of protection against retaliation often do not remove the student's concerns about going forward visibly. Yet schools need to investigate, to make sure that any problems that exist are addressed and to avoid liability for not doing so, especially if the problem is repeated.[39] And they need to do so in a way that allows the accused to respond fully to the charge, which usually means revealing the source of that charge. A full investigation also may involve talking with other students, which the originator of the charge may see as a further violation of his or her privacy.

C. Technological forces

Technology is driving a number of privacy debates on campus. More and more institution transactions and recordkeeping is being done electronically, and as discussed

[39] Schools and individual faculty and staff may be held liable if they know of and do not respond to allegations of serious teacher-on-student or peer-on-peer sexual harassment. *Davis v. Monroe Cty. Bd. of Ed.*, 526 U.S. 629 (1999); *Gebser v. Lago Vista Indep. School Dist.*, 524 U.S. 274 (1998).

above, a growing body of federal and state statutes require that schools afford a certain level of privacy and security to that data. Additionally, schools provide students with considerable information technology resources and encourage them to use these resources fully in the service of their intellectual growth. To promote the greatest degree of freedom of thought, belief, and speech, schools (both public and private) generally try not to interfere with what students are doing on email or the campus network. At the same time, because systems may break down, become overloaded by spam or more legitimate uses, get hacked or attacked by viruses, or be misused by students themselves, schools are continually monitoring, diagnosing, and adjusting network operations and reserve the right to investigate, monitor or halt particular student IT activities that are problematic. Our computer privacy policies specify this in order to set expectations of privacy appropriately.[40]

Most schools try to limit intrusions on student use to cases of suspected crimes or policy violations involving IT resources—such as when the recording industry comes calling with a court order demanding the identity of the student who has unlawfully uploaded 5000 music tracks via his campus network connection—so that students will enjoy enough privacy online to reap the benefits outlined above. But the proliferation of technology in campus life is raising all sorts of new issues on the privacy frontier. For example, the increased use of "smart cards" on campus creates a data trail that must be identified and managed. The use of security cameras, and roving "campus cams" that schools may put on their home pages to entice applicants, place students' everyday activities on increasing display. And students' continued use of campus networks to engage in unlawful file sharing is prompting the recording and movie industries to call for more invasive technologies to detect and prevent this activity.

A further example: students now come to campus with a cell phone more or less permanently fixed to their palm, and many of these have camera functions, which allow

[40] Computer privacy policies echo some of the legal privacy themes discussed in Section II; on the one hand, they reflect a contractual model ("in exchange for access to campus IT resources you agree that the school may access your files without your consent in the following circumstances…."), and for publics, the policy terms in turn set privacy expectations in such a way that what schools need to do to investigate misuse or conduct data flow monitoring is not a "search" and does not raise constitutional concerns.

students to surreptitiously photograph their friends and others, including in the locker rooms and showers. Posting those photos to a website is the work of a moment for most students. So, for that matter, is posting photos taken with a regular camera, as the recent case at the University of Pennsylvania demonstrated. There, a student on the street witnessed two other students having sex in a window in plain view of others. He photographed them and posted the photos to the web. One of the students in the photos complained and the school charged the photographer with sexual harassment and computer misuse. A substantial controversy developed over whether the student photographer had done anything wrong and whether the students who had sex in the window had failed to protect their own privacy and thereby exposed themselves (no pun intended) to whatever resulted from their actions. Penn ultimately dropped the charges against the photographer, but the case has prompted much thoughtful discussion on campus conceptions of privacy and the norms surrounding the use and distribution of information. Do students having sex in a window intend for the whole online world to see them, or just the lucky few who happen down their street? Should their expectations matter? Do students who have grown up with the internet are used to getting and distributing information without many technological barriers, accept or impose themselves any ethical rules about what should or should not be shared?

D. Cultural forces

1. Some familiar factors

This leads us directly into some broader cultural considerations when considering what students want and expect to keep private on campus. Some cultural considerations are longstanding and perennial. Students, particularly undergraduates, are young and often painfully insecure and self-conscious. Acceptance by others, especially by their peers, is generally critical to their self esteem and overall well being. To be accepted, they must relinquish some and perhaps much information about themselves. At the same time, they may try to construct a particular persona that they feel is most acceptable to those with

whom they want to join, and keep private those views or traits that conflict with their public persona.

Elizabeth Armstrong and Laura Hamilton, two researchers at Indiana University who lived for a year in a freshman women's dorm as part of a longitudinal study of student risk-taking behavior,[41] told me one of their main observations was how important it was to students to control their image and how others view them. Moreover, students will relinquish privacy when it suits the construction or maintenance of their desired image – for example, by carrying on conversations with their friends or boyfriends loudly in the presence of others, and even having sexual encounters in the presence of others, to reinforce their image as popular, desirable, and fun-loving (a variation of this may be the willingness of college students to appear in shows like Girls Gone Wild). In the words of comedian Margaret Cho, "privacy and security are those things you give up when you show the world what makes you extraordinary."[42]

By the same token, privacy is what students invoke – and expect others to respect – when they want to keep certain things from certain people to avoid undermining their image. As our dean of students at Indiana puts it, students define privacy as "what I don't want you to know when I don't want you to know it." This approach is not limited to students, of course. But given the intense pressure on students to attract and be accepted by others, it can lead to serious problems. For example, Armstrong and Hamilton told me that among the freshmen women they studied, there is a culture that eating disorders are personal problems and weaknesses and should be handled quietly on one's own. This attitude poses clear challenges for schools wishing to raise awareness of and effectively address this all-too-common student health issue.

The value of privacy to students in this model, then, iOur dean of students at Indiana told me that students define privacy as "what I don't want you to know when I don't want you to know it."

[41] Publications discussing the results of the first phase of their study are forthcoming.
[42] See http://www.brainyquote.com/quotes/quotes/m/margaretch186795.html.

2. Some new factors

Other cultural forces are more recent, such as the changing nature of parent involvement in college life. Parents are demanding more involvement in their children's college experience. These so-called "helicopter parents" are figuratively (and sometimes physically) hovering over campus, keeping in close contact with their kids, helping to plan the kids' class schedules, communicating with faculty and administrators about the kids' needs, and inserting themselves as advocates into academic disputes and disciplinary processes. Partly because rising college costs promote a "consumer" mentality toward education among parents and students, and partly because the parents of today's college students are mainly baby boomers, a generation characterized if not caricatured as demanding and controlling, parents want to know what is going on with their children and to participate in an effort to secure the services and outcomes they desire. As a result, schools are encountering more and more students who are not maturing and learning to make decisions and take responsibility for their own actions, and who are relinquishing some of their privacy and autonomy in the process. Helen Johnson of Cornell notes that she "received hundreds of phone calls each year from parents 'taking on' problems that should have been handled by their sons and daughters."[43]

3. And a few more new factors

Still other cultural forces are both recent and technology-driven, or at least technology-enabled. Cell phones let people receive calls at any time and virtually anywhere, and they do—it is common to hear people in restaurants, hallways, Starbucks, all manner of public places, carrying on conversations about quite personal topics. Although students going back to the Warren-Brandeis days (and well before) may have encountered some form of tabloid press, students today have grown up surrounded by exhibitionism.

[43] Helen E. Johnson, "Educating Parents About College Life," The Chronicle of Higher Education (Jan. 9, 2004). See also Wendy S. White, "Students, Parents and Colleges: Drawing the Lines, The Chronicle of Higher Education (Dec. 16, 2005).

Reality TV shows – beginning with MTV's Real World, focused precisely on their age group – seem to dominate the medium, and students can watch people doing all sorts of ordinarily private things for public consumption. The internet is full of chat rooms, bulletin boards, and blogs containing the daily stream-of-consciousness outpourings of students and others (anyone with a keyboard, apparently). Cell phones and instant messaging let friends chronicle the events of their day to one another on a minute-by-minute basis.

What does this mean for privacy? A few things, perhaps. The concept of privacy as time to reflect and mull over ideas seems lost to these phenomena. Once a thought is had, it is expressed. Once an act is begun, it is beamed to the world.

At the same time, some measure of privacy may be achieved through anonymity, at least in the online and "public cell phone conversation" setting. Those who talk on the cell phone in the midst of a group of strangers may assume that no one knows them or cares what they are discussing and will tune them out. Students chatting online may use invented names and give out few personal identifiers; while this anonymity is certainly not total (webmasters at a minimum will know the personal information they used to establish their accounts), it may suffice by masking them from the other chat room dwellers they most care about. This harks back to the notion of controlling one's image, discussed above. It also echoes the First Amendment's view that anonymity helps to promote vigorous participation in public discourse.

And then there is Facebook. Founded in 2004 by Harvard undergraduates, Facebook is a virtual social network that lets college students throughout the country connect online. Almost five million college students use it, and it is the ninth most visited Internet site according to Nielsen/Net Ratings.[44] "Nearly three-quarters of Facebook users sign on at least once every 24 hours, and the average users sign on six times a day," according to a spokesman for the site.[45] Students register using their .edu email address and then post

[44] Nancy Hass, "In Your Facebook.com," *The New York Times*, Jan. 8, 2006.
[45] *Id.*

personal information about themselves, such as addresses, birth dates, contact information, political views, sexual preferences, favorite movies, hobbies, lists of friends (often with links to the friends' Facebook profiles), photos and diaries. Users can also form groups in which they can pursue similar interests. What students post is often rowdy and risqué, describing drunkenness, drug use, and sexual encounters, and is frequently illustrated with pictures of all of the above.

Facebook offers obvious benefits in terms of building community and friendships among students. At the same time, Facebook is at the center of a growing debate about student privacy and safety. Posting personal information together with contact information may expose students to the risk of physical or cyber stalking, phishing, and identity theft. And because anyone with a .edu email address may register with Facebook – including campus administrators, campus police, parents who have alumni .edu addresses, and employers who are either alumni or who otherwise have access to a .edu address – may read the information that students post about themselves, students may be unwittingly exposing themselves to other risks, such as lost job opportunities, student disciplinary proceedings, and arrests. Consider the following examples:

- In October 2005, campus police officers at Penn State logged onto Facebook and identified 50 students who had taken part in a riot after the Penn State-Ohio State football game. Their source? A Facebook group titled "I Rushed the Field After the OSU Game (And Lived!)". They correlated information from the group and elsewhere on the site, including photos, and rounded up the students for referral to the campus judicial system.[46]
- Campus police at the University of Kentucky and Northern Kentucky University have disciplined students who posted pictures of themselves drinking in the campus dorms.[47]

[46] *Id.*
[47] *Id.*

- An "outraged government employer" who had hired a number of interns from Indiana University read "distasteful information and pictures" on an intern's Facebook profile (after gaining access through another intern), and demanded that the intern remove the employer's name and the student's internship status from the site.
- A student's allusion to marijuana use in her Facebook profile "got to her parents and became the buzz [presumably no pun intended] at her grandmother's retirement home."[48]

Students have reacted in a variety of ways to the increased reports of non-student use of the Facebook. Some shrug off the viewership of non-students and make the assumption that they do not have any real privacy on the internet anyway. Others are outraged at what they consider a breach of trust and invasion of their privacy. This suggests a definition of privacy that relies less on how many people see one's information (potentially millions of other students can see it) and more on who those people are and whether they will treat the information in the same spirit in which one posts it: that is, that talk of drunkenness and topless photos from Spring Break are all part of the normal, expected harmless rough and tumble of college life, and not a predictor of the poster's maturity and responsibility in other contexts.

So far, Facebook has not indicated that it intends to try to limit non-student access, and that might be unenforceable anyway. A better approach would be to educate students to think hard about the risks of putting personal information out there on the internet, where it may be viewed relatively freely and proliferated widely, in one form or another. Some schools are beginning to do this, including Virginia Commonwealth University and Georgia College & State University.[49] Such education is critical, although it may be a hard sell if students feel that censoring their postings (or using the security safeguards that Facebook already provides, like being able to bar certain people from viewing one's profile) will undermine the very value of Facebook participation.

[48] Hass, supra.
[49] Read, supra.

IV. Concluding thoughts

The law has a few things to say about student privacy – it sets standards for securing student data, limits institutional sharing of that data, and offers certain protections against misuses of data and intrusions upon constitutional and contractual privacy rights. The values of privacy that are underscored in the law – freedom of thought and speech, decisional autonomy – can help guide broader debates on student privacy on campus. But these debates will need to occur largely among students, campus administrators, and health care professionals in a community-based effort to develop shared norms and expectations about the scope of privacy protection and the balance between privacy and other significant interests. Approaching these issues as a matter of shared concern will help build the trust necessary to navigate the difficult passageways when values conflict.