POINT/COUNTERPOINT:
SECURITY VS. PRIVACY—ARE WE STRIKING AN APPROPRIATE BALANCE?

PART I
THE PRIVACY PART OF THE EQUATION:
PROTECTING (AND NOT PROTECTING) DIGITAL PRIVACY ON CAMPUS

Lawrence White
Chief Counsel
Pennsylvania Department of Education
Harrisburg, Pennsylvania

This is a revised and updated version of a paper that was originally presented in February, 2000, at Stetson University College of Law’s 21st Annual National Conference on Law and Higher Education. The author wishes to thank Stetson University College of Law and Stetson Professor Robert D. Bickel for permission to adapt that paper for this EDUCAUSE conference.

The author also wishes to thank Margaret O’Donnell, Assistant General Counsel at The Catholic University of America, for her help and encouragement in the preparation of this outline.

The views expressed in this outline and during the accompanying presentation are those of the author. They do not necessarily reflect and should not be attributed to the Pennsylvania Department of Education or any PDE officer or official.

“You already have zero privacy. Get over it.”
—Scott McNealy, Chief Executive Officer of Sun Microsystems, 1999

I. INTRODUCTION

A. Americans are slowly waking to the realization that computers pose a threat to their privacy. Computers convert the most intimate of communications and activities—writing letters, speaking on the telephone, filling prescriptions, taking photographs—into electronic records that are easy to store and easy to access. Computerized surveillance technologies make it simple to track people’s movements and listen in on their private conversations. By networking computers and using them to exchange files at high speed,
a company can aggregate electronic information about the private habits of computer users. We are uneasy about the motives of the companies gathering that information and the uses to which the information is being put. We fear for our privacy in cyberspace.

This presentation explores some of the privacy problems that have surfaced on college and university campuses at the dawn of the digital millennium. It begins on a technological note by describing various ways in which advances in computer technology jeopardize the privacy rights of computer users and those whose movements are tracked by computers. Next, it defines privacy as a legal concept by examining the great Supreme Court landmarks on the constitutionally protected right of privacy. Third, the presentation examines the various ways—constitutional, common law, and regulatory—in which privacy advocates seek to protect people’s privacy in the age of computer technology. Last, it turns to the nation’s college and university campuses. It describes efforts underway to address computer-related privacy concerns, and it touches upon some other, non-computer-related issues involving privacy rights on campus.

Two important policy questions shape the presentation:

- Have colleges and universities been sufficiently sensitive to the privacy rights of campus community members?

- As colleges and universities strive, for perfectly understandable and unassailably correct reasons, to make their campuses more secure, are they in the process diminishing—wittingly or unwittingly—the privacy rights of campus community members? And if the answer is yes—if there is an unavoidable tradeoff between privacy and security—what principles should guide the higher education community in striking the balance reasonably?

B. Some introductory food for thought: “[H]ow cyberspace is not how cyberspace has to be. There is no single way that the Net has to be; no single architecture defines the nature of the Net.” Lawrence Lessig, CODE AND OTHER LAWS OF CYBERSPACE 25 (1999) (emphasis in the original). Here, abridged, is the continuation of that thought:

... [N]ot all universities [have] adopted the Net in the same way. ...

At the University of Chicago, if you wanted access to the Internet, you simply connected your machine to jacks located throughout the university. Any machine with an Ethernet connection could be plugged into these jacks. Once connected, your machine had full access to the Internet—access, that is, that was complete, anonymous, and free.
The reason for this freedom was a decision by an administrator—the provost, Geoffrey Stone, a former dean of the law school and a prominent free speech scholar. When the university was designing its net, its technicians asked Stone whether anonymous communication should be permitted. Stone, citing the principle that the rules regulating speech at the university should be as protective of free speech as the First Amendment, said yes. From that policy decision flowed the architecture of the University of Chicago’s net.

At Harvard the rules are different. If you plug your machine into an Ethernet jack at the Harvard Law School, you will not gain access to the Net. You cannot connect your machine to the net at Harvard unless the machine is registered—licensed, approved, and verified. Only members of the university community can register their machines. Once registered, all interactions with the network are monitored and identified to a particular machine; the user agreement carries a warning about this practice. Anonymous speech on this net is not permitted—it is against the rules. Access can be controlled based on who you are, and interactions can be traced based on what you did.

... Controlling access was the ideal at Harvard; facilitating access was the ideal at Chicago. Harvard chose technologies that make control possible, while Chicago chose technologies that facilitate access. ...

The networks thus differ in the extent to which they make behavior within each network regulable. This difference is simply a matter of code—a difference in the software. Regulability is not determined by the essential nature of these networks. It is determined instead by their architecture. [Lessig, supra, pp. 26-27 (emphasis in the original; footnotes omitted).]

Here’s the question for you, as university policymakers, to ponder as you listen to the views expressed by Rick Johnson and me during this presentation: what Internet architecture—in other words, what set of protocols and rules—best and most appropriately strikes the balance between (on the one hand) minimally regulated access to the Web and (on the other) the protection of the privacy rights of Web users?

II. A CRASH COURSE (NO PUN INTENDED) ON DIGITAL THREATS TO PRIVACY

A. Digitization.... The last decade has witnessed an explosion in the amount of information available in digital form. As letter writing is replaced by word processing, phonograph

---

2 A postscript: It has been five years since Professor Lessig published his book, an eternity in cyber-time. Just a few months ago, the University of Chicago implemented a new computer-use policy that represents a complete, 180-degree reversal of the laissez-faire policy described admiringly by Professor Lessig in 1999. See Policy on Regulated Computers: Security and Management Requirements for Computers Housing Sensitive Data on the University Network, http://security.uchicago.edu/regulated-computers/policy.shtml.
records by MP3 files, analog television signals by digitized cable transmissions, telephones by computerized telephony, conventional film by camera diskettes and DVD, digitization has revolutionized the way we create and store words, pictures and sounds.

“Exponential increases in computing power and dramatic decreases in the physical size and price of computers have created a frenzied cycle in which both individuals and organizations increasingly use computers, spawning phenomenal growth in and dependence on computer-based services, and resulting in greater demand for and use of computers.” Fred H. Cate, PRIVACY IN THE INFORMATION AGE (Brookings Institution 1997), page 1. (This book is cited below as “Cate 1997.”)

B. … Plus Interconnectivity…. At just the moment when the amount of digitized information is exploding, so is the number of users (individual and corporate) who can access that information. Today, about 60 percent of American adults have computers connected to the Internet, up from 49 percent in 2000 and less than 15 percent in 1995. In 1998, U. S. companies did an estimated $92 billion worth of business-to-business Internet commerce; five years later, in 2003, the comparable figure was $2.8 trillion, an astonishing thirty-fold increase in five years. (The figures in this paragraph are taken from two sources: a report by the Pew Internet and American Life Project titled The Ever-Shifting Internet Population: A New Look at Internet Access and the Digital Divide, April 16, 2003, www.pewinternet.org, and a study (undated) by the Boston Consulting Group reported in E-Commerce Times, www.ecommercetimes.com/perl/story/-2191.html.)

C. … Plus Speed…. The exponential growth in computer use is fueled by advances in the speed of computers, increased storage capacity, and improvements in interconnectivity technology. Twenty years ago, a computer with sufficient memory to store the contents of a small telephone book cost $10,000 and occupied a dedicated room. Today, a personal digital assistant a thousand times more powerful costs less than $500 and fits into a shirt pocket. As one observer has noted:

The practical ability to create, manipulate, store, transmit, and link digital information is the single most influential innovation of the twentieth century. Computers and the networks that connect them have rapidly become a dominant force in business, government, education, recreation, and virtually all other aspects of society in the United States and throughout the world. ... No form of communication other than face-to-face conversation and handwritten, hand-delivered messages escapes the reach of electronic information technologies. ... [N]o communication that bridges geographic space or is accessible to more than a few people exists today without some electronic component. And the dominance of electronic communication is growing at an astonishing pace. [Cate 1997, pages 5-6.]

---

3 To the Brookings Institution’s credit, the entire text of Professor Cate’s 1997 book is available online at http://brookings.nap.edu/books/0815713169/html.
D. *... Equals a tangible threat to traditional notions of privacy.* The proliferation of computers, our growing dependence on them to perform employment- and household-related tasks, and the ease and low cost with which data about our computer utilization can be collected and shared with third parties have prompted growing concern about the privacy rights of computer users. As noted privacy advocate Marc Rotenberg observed almost eight years ago, “privacy will be to the information economy of the next century what consumer protection and environmental concerns have been to the industrial society of the 20th century.” Quoted in James Gleick, *Behind Closed Doors: Big Brother Is Us*, NEW YORK TIMES MAGAZINE, September 29, 1996, page 130. See also Fred H. Cate, *The Privacy Problem: A Broader View of Information Privacy and the Costs and Consequences of Protecting It*, 4 FIRST REPORTS (a publication of The Freedom Forum’s First Amendment Center), March 2003, reprinted at www.law.indiana.edu/directory/-publications/fcate/privacyproblem.pdf (and referred to hereinafter as “Cate 2003”).

E. Privacy advocates identify three distinct kinds of threats associated with computer technology: concerns about the sheer volume of digitized information, loss of control over personally identifiable data, and loss of personal privacy through intrusive surveillance technologies.

1. *Concerns about the volume of information compiled about individuals without their knowledge.* As more data are collected in digital format, and as digital information becomes easier and cheaper to store, others know more about us than ever before. The amount of information routinely collected about people and stored in computers is startling and disturbing:

   • Every time a person uses an automated teller machine at a bank, the bank records details about the time, date, and nature of the transaction. At many ATMs, video cameras take pictures of customers. The pictures are digitized and stored along with the transaction record.

   • Supermarkets that offer magnetically-coded discount cards use those cards to track and store records of their customers’ purchases. Those records are used to customize advertising and discount coupons to match the purchasing preferences of individual customers. Like almost all such records, they are also sold to other companies for mailing-list and marketing purposes. “[A] woman in San Francisco reported that nine months after buying a home pregnancy test from Safeway she began receiving the company’s coupons for diapers and baby food, mailed to her home.” Christian Parenti, *The Soft Cage: Surveillance in America* 100 (2003).

   • Every time a customer makes a telephone call or uses a credit card, an electronic record is created and stored. Those records are sold to companies that use them to tailor mailing lists for advertising purposes. They are also sold to private
investigators and given to law enforcement agencies, which use them to track individuals’ private telephone calls and consumer purchases.

- Internet service providers assign a unique identifying stamp known as an Internet Protocol address (or “IP address”) to each subscriber’s account. When a customer accesses the World Wide Web through his or her Internet service provider, the customer leaves digital footprints that enable the ISP—or retailers who buy the information from the ISP—to trace the customer’s various destinations in cyberspace. Even if the customer seeks to conceal his or her identity, for example by using a pseudonymous e-mail address, it is relatively easy for the ISP to crack the alias using the customer’s IP address.

- Almost all e-commerce sites on the World Wide Web utilize “cookie” technology to learn basic information about people who visit their site, including Zip code, ISP, what parts of the Web site are visited, and how long the visit lasts. Visitors who purchases goods or services from the site are required to divulge other personal information, such as name, e-mail address, and credit card number. All this information is stored and used for marketing purposes. According to a survey conducted for the Federal Trade Commission by the Georgetown Internet Privacy Policy Survey Project, 93 percent of commercial Websites collect at least one type of personally identifying information (for example, name or e-mail address) from each person visiting the site, and 57 percent collect at least one form of demographic information (such as the visitor’s age, gender, Zip code, or purchasing preferences). The survey results are reported on the Online Privacy Alliance home page at www.privacyalliance.com/resources/gipps_execsummary.shtml.

- In many parts of the country, drivers pay tolls electronically by purchasing magnetic cards (“E-ZPass” cards in the eastern part of the United States) and placing them on the windshields of their automobiles. “Each E-ZPass tollbooth is equipped with a computer, connected by fiber-optic cable to a ‘data center’ in Secaucus, New Jersey, run by Chase Manhattan Bank. Each tag produces a precisely itemized monthly E-ZPass statement that reveals a billing address, a credit-card number, how often a driver is on the road and his or her whereabouts at a certain time. Without much discussion, a system of soft, unstaffed electronic checkpoints has been erected along thousands of miles of highway and at dozens of major urban bridges and tunnels controlling access to some of the nation’s most populous cities. If originally pitched to the public as such, would we have hesitated?” Christian Parenti, THE SOFT CAGE: SURVEILLANCE IN AMERICA 124-25 (2003) (footnote and internal quotation marks omitted).

- Just a few months ago, the nation’s largest and most profitable Internet search engine company (you may have heard of it—Google) introduced a new no-cost e-mail service with the cutesy name “Gmail.” Without public announcement or
disclaimer, Google incorporated into its server software a feature that literally reads each e-mail message, looks for nouns and verbs, and matches words to paid advertisements that appear on the margin of the screen. (Example: were you to type an e-mail note using the word “vacation,” your screen would show advertisements for airlines and cruise ships.) Google’s decision to snoop on customers’ e-mail drew predictable howls from privacy advocates and newspaper editorial writers. See Editorial, Big Google is Watching, CHICAGO TRIBUNE, April 28, 2004, p. 22.4

• “Spyware” and its close cousins “adware” and “annoyware” are proliferating and tainting the home computer experience for millions of Americans. From Katie Hafner with Michael Falcone, Heart of Darkness, On a Desktop, NEW YORK TIMES, September 4, 2003, Section G, page 1:

  ... [T]he number of home PC’s that are infested with alien software that comes in over the Internet and installs itself without the knowledge or consent of the PC user is increasing at an alarming rate.

  Richard M. Smith, a computer security expert in Brookline, Mass., estimates that one in every two Windows computers has unsolicited software lurking within. ...

  The programs hide in the recesses of the machine and seldom announce their presence. They can enter the machine by way of a virus that has attached itself to an incoming file. Or they can be downloaded unawares by simply clicking on, say, a pop-up ad. Mr. Smith said such assaults were called “drive-by downloads.” ...

  Until symptoms appear, the user knows nothing of the unwanted software’s presence. Spyware, which may piggyback on another downloaded program, often operates in the background, sending information back to a remote site and displaying pop-up ads tailored to the user’s online habits, or harvesting e-mail addresses to sell to spammers.

4 From that editorial:

The problem with Gmail is the apparent attempt to slip it by without anyone noticing the fine print. … Google buries the invasive advertising connection in its service agreement. Its jargon-filled explanation about how the service will “effectively target dynamically changing content” fails to spell out sufficiently the privacy trade-off at issue.

Beyond that, how can Gmail users be certain that those sending them emails won't get spammed? Will Google also track the search-engine usage of its Gmail customers, selling that information to the wider world, too?
Adware is similar but more benign, or at least better encased in euphemism; its defenders say that it is something that consumers consciously agree to download. More insidious programs, perhaps better described as annoyware, redirect the computer’s browser to pornographic Web sites, often to pump up those sites’ traffic figures, or commandeer the machine’s modem to dial 900 numbers at the computer owner’s expense. ...

“As the government collects and stores more and more personal information about citizens …, there is, first of all, the danger of the ‘Googleization’ of identity—a phenomenon that could allow government agents to single out any individual from the crowd and reconstruct his or her movements, purchases, reading habits, and even private conversations for any period of time.” Jeffrey Rosen, THE NAKED CROWD: RECLAIMING SECURITY AND FREEDOM IN AN ANXIOUS AGE 19 (2004). A study conducted by Jupiter Research, a media marketing firm, found that 70 percent of American consumers are worried about both the volume of information collected on their on-line habits and what happens to that information once it is stored in computer databases. The Jupiter study estimates that online merchants lose about $20 billion in sales annually from consumers who are unwilling to surrender personal information about themselves. Jupiter Research, Online Privacy: Managing Complexity to Realize Marketing Benefits, June 3, 2002, www.jupiterresearch.com/xp/jmm/press/2002-/pr_060302.html.

(2) Concerns about unauthorized access to records in computerized databases. Individual computer users are increasingly unable to control personally identifiable information about themselves once such information is stored in computerized databases. It may be information a person knowingly discloses but does not expect to be used for other purposes without permission (for example, information about a customer’s purchases at a Website that may be used by the operator of the site to market other products to that same customer). Or it may be information a computer user unwittingly reveals simply as a byproduct of using a particular technology (for example, the kind of information a company that maintains a Website can collect through cookies or other forms of electronic tracers, information such as a potential customer’s e-mail address or the URLs of other Web pages the customer may have visited). Interactive computing inevitably requires users to reveal personally identifiable information about themselves. Users are willing to provide this information as long as they understand the purpose for which it is sought and the limitations on the uses that will be made of it when it is in someone else’s custody. It is the unauthorized use of personal information—the surrender of ultimate control over personal data—that galls consumers and gives rise to privacy concerns.

(3) Surveillance concerns.

(a) Computers are increasingly used to track people’s movements, both in cyberspace and in real space. Intrusive surveillance technologies compromise privacy rights
in the more traditional geographic or spatial sense. “The paraphernalia of snooping,” to use THE ECONOMIST’s term, enable third parties to monitor people’s movements and intercept their communications on a micro-scale that would have been unimaginable a decade ago. Privacy concerns arise from the unauthorized use of technologies to spy on people’s activities in the workplace, at home, and in cyberspace. The End of Privacy: The Surveillance Society, THE ECONOMIST, May 1, 1999, page 22.

(b) Surveillance is not limited to the use people make of their computers in cyberspace. It has a real-space dimension too. A person who lives and works in a metropolitan area in the United States is photographed by surveillance cameras an average of twenty times per day. Cameras are everywhere—at highway interchanges, in the lobbies of apartment and office buildings, at entrances to parking lots, in stores, in banks, in elevators, in the hotel conference room in which you’re reading this outline, and increasingly in the workplace. In a 1997 survey, nearly two-thirds of 900 large companies surveyed admitted to engaging in some form of electronic surveillance of their workers. Companies place surveillance cameras in restrooms, lounges, locker rooms, and other areas that raise substantial privacy concerns. See generally American Civil Liberties Union, Feature: Public Video Surveillance, www.aclu.org/Privacy/Privacy.cfm?id=12705&c=39. In the last few years convenience stores and discount stores have installed sophisticated software to deter employee theft by tracking cash-register transactions. “At a Beall’s Outlet store [in Florida], for example, one manager had been identified by monitoring software as the source of an unusually high number of returns and refunds. Beall’s security personnel then pored over earlier transactions the manager had rung up and used surveillance cameras in the store to watch her. Before another week was out, they had enough evidence to confront her.” Jennifer Lee, Tracking Sales and the Cashiers; Retail Software Monitors Inventory But Also Watches For Employee Theft, NEW YORK TIMES, July 11, 2001, page C1.

(c) To the consternation of privacy advocates, advances in surveillance technology are finding their way into the marketplace. According to THE ECONOMIST, “video cameras the size of a large wasp may some day be able to fly into a room, attach themselves to a wall or ceiling and record everything that goes on there.” Satellite images, once the exclusive province of the armed forces, are now manufactured commercially and sold to companies desiring to spy on their competitors. Even more surreal are applications of the new science of “biometrics,” which uses technology to identify people from their voices, eyeballs, and genetic coding. While software manufacturers extol biometric applications as foolproof, cost-

---

5 Comparatively, that’s nothing. According to the American Civil Liberties Union, a closed-circuit television system installed by law enforcement officials in London utilizes 150,000 surveillance cameras and captures digitized images of each London pedestrian an average of 300 times per day. DC Video Cameras vs. Live Community Police in Our Neighborhood, www.aclu.org/Privacy/Privacy.cfm?id=12705&c=39.
effective ways of allowing employees or credit-card users to identify themselves, privacy experts express anxiety over the “ever widening trail of electronic data” that will be kept on individuals and stored in computer memories in the future. THE ECONOMIST, supra, at 22.

Surveillance images lend themselves to disturbing commercial exploitation and other forms of abuse. As one bizarre example of the unintended uses to which video images are being put, digital images of crimes recorded by surveillance cameras in stores and on street corners are purchased by commercial film producers, edited, and marketed in video stores. Cable News Network, Public Cameras Draw Ire of Privacy Experts, March 29, 1996 (www-cgi.cnn.com/-US/9603/public_places). In Washington, D.C. and Detroit, law enforcement officials reportedly used police surveillance tapes to blackmail customers at gay night clubs, to stalk women, and to get dirt on estranged spouses. Avis Thomas-Lester and Toni Locy, Chief’s Friend Accused of Extortion, WASHINGTON POST, November 26, 1997, page A1; M. L. Elrick, Cops Tap Database to Harass, Intimidate—Misuse Among Police Frequent, Say Some, But Punishments Rare, DETROIT FREE PRESS, July 31, 2001, page 1A.

III. FROM THE 21st CENTURY TO THE 19th: THE CONSTITUTIONAL RIGHT TO PRIVACY

A. Constitutional antecedents.

(1) As strange as it may sound, the Constitution of the United States does not use the word “privacy.” Although the Bill of Rights contains protections against government usurpation of other fundamental civil liberties, the right to privacy is not mentioned there or elsewhere in the Constitution. It was not until 1890 that legal scholars first attempted to articulate a fundamental civil liberty, the right of each individual “to determin[e], ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others,” a right scholars of the period referred to as “the right to privacy.” Samuel D. Warren and Louis D. Brandeis, The Right to Privacy, 4 HARV. L. REV.193, 198 (1890).6

6 This article, often described as the most famous law review article ever written, appeared after members of the Warren family, one of Boston’s most prominent, were the subjects of scandalous stories in Boston newspapers of the era. For colorful background on the Warren-Brandeis article, see William L. Prosser, Privacy, 48 CALIF. L. REV.383, 383-84 (1960); Bruce W. Sanford, LIBEL AND PRIVACY 523 (2d ed. 1999).

The “Brandeis” who contributed to the Warren-Brandeis article was Harvard Law School Professor Louis Brandeis. Much later in his life, Brandeis—by then Justice Brandeis of the United States Supreme Court—authored the dissenting opinion in Olmstead v.United States, 277 U.S. 438 (1928), that is widely identified today as the first judicial acknowledgment of the constitutional right to privacy. In 1928 Justice Brandeis wrote:
It was not until three-quarters of a century later, in 1965, that the Supreme Court of the United States first recognized a constitutionally predicated right of privacy. In *Griswold v. Connecticut*, 381 U.S. 479 (1965), the medical director of Connecticut’s chapter of Planned Parenthood was convicted of violating a state criminal statute making it illegal to prescribe birth control pills or other contraceptive devices. The director’s defense was that he prescribed contraceptives to married persons only, and that married couples had a constitutionally protected right to be free from government interference in matters as fundamentally private as conception and reproduction. The Supreme Court, in a decision written by Justice William O. Douglas, struck down the Connecticut statute and declared broadly that individuals have a fundamental constitutional right that protects “the sanctity of a man’s home and the privacies of life.” 381 U.S. at 484, quoting *Boyd v. U.S.*, 116 U.S. 616, 630 (1886). In one of the most famous passages in all of American constitutional law, Justice Douglas surmounted the practical problem of deriving a right to privacy from a Constitution that didn’t use the word by advancing the theory of “penumbral” rights, rights grounded, not in the literal words of the Bill of Rights, but in the “penumbras”—the shadows—“formed by emanations from those guarantees that help give them life and substance.” 381 U.S. at 484.

*Griswold* and a small number of Supreme Court cases decided in its wake stand for the proposition that the Constitution protects the privacy rights of individuals in matters relating to some—but not all—aspects of personal life. The right to privacy includes freedom of choice in matters relating to marriage,7 child bearing,8 and child rearing.9 But, as noted in one leading constitutional law treatise, “the list of [privacy] rights which the Court has found to be fundamental … is not a long one.” Ronald D. Rotunda & John E. Nowak, *TREATISE ON CONSTITUTIONAL LAW: SUBSTANCE AND*...

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 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. [277 U.S. at 478.]


9 See, e.g., *M.L.B. v. S.L.J.*, 519 U.S. 102 (1996) (filing fees preventing indigent mothers from appealing custody determinations are an unconstitutional interference with the right to raise children).
PROCEDURE, Vol. 2, at 633 (3d ed. 1999). It is restricted, by and large, to the most traditional of family functions—marriage and parenthood—and carries with it the faintly anachronistic aroma of 19th-century notions of American family life.\(^\text{10}\)

(4) In the years immediately following *Griswold*, litigants pressed the argument that Justice Douglas’s penumbral right to privacy encompassed the general freedom to engage in consensual, private behavior involving no demonstrable harm to third parties. The argument went nowhere. In a series of cases in the 1970s and 1980s, the Court refused repeated invitations to recognize privacy-based limitations on the government’s power to collect data on private individuals. In *Whalen v. Roe*, 429 U.S. 589 (1977), for example, litigants used privacy arguments in an attack on a New York anti-drug law that required physicians and pharmacists to forward information to state authorities when filling prescriptions for drugs containing narcotics. While observing that the reporting requirement posed a threat to individual privacy, the Court nevertheless upheld the statute on the ground that it furthered the legitimate state goal of controlling illegal drug distribution. In another case, this one involving an institution of higher education, the Court refused to quash a warrant allowing police officers to search the offices of a campus newspaper for potentially incriminating photographs and photographic negatives that could be used to glean the identity of students who had participated in a campus demonstration. *Zurcher v. Stanford Daily*, 436 U.S. 547 (1978). Finally, in a heart-wrenching case involving perhaps the most fundamental privacy right of all—the right to die—the Court in *Cruzan v. Director, Missouri Dep’t of Health*, 497 U.S. 261 (1990), found it unnecessary to determine as a matter of Constitutional law whether an individual has a protected privacy right to refuse medical treatment, and instead ruled “vague[ly],” in the word of two distinguished commentators, that any right to reject medical treatment would have to be balanced against society’s interest in protecting the sanctity of human life. 497 U.S. at 277-79. See Ronald D. Rotunda & John E. Nowak, *TREATISE ON CONSTITUTIONAL LAW: SUBSTANCE AND PROCEDURE*, supra, § 18.30 (“That vague reference to a balancing test provides no basis for predicting how the Court would decide specific issues if there were a right to die”).

(5) Against this backdrop, federal courts have consistently rebuffed efforts to restrict the unauthorized use of personal information and have repeatedly resisted invitations to recognize what one scholar called “the right to information privacy.” (That phrase was used by UCLA Law School Professor Eugene Volokh in *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People From Speaking About You*, 52 STAN. L. REV. 1049, 1050 (2000).) See generally Cate 2003 (page 5 of this outline, supra) at 10-12.

Professor Cate discusses one exemplary case: *U.S. West, Inc. v. Federal Communications Comm’n*, 182 F. 3d 1224 (10th Cir. 1999), cert. denied, 528 U.S.

\(^{10}\) *But see Lawrence v. Texas*, 539 U.S. 558 (2003) (homosexual acts undertaken in the privacy of the home are entitled to constitutional protection). *Lawrence* is discussed on pages 13-14 of this outline.
In 1996, Congress enacted omnibus telecommunications reform legislation, the infamous Telecommunications Act of that year. The Act contained provisions designed to safeguard the privacy of “customer proprietary network information,” or “CPNI”—defined by statute as “information that relates to the quantity, technical configuration, type, destination, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier” (47 U.S.C. § 222(f)(1)(A)). Like other telecom giants, U.S. West surreptitiously gathered its customers’ CPNI and used the information to offer special deals, packages and incentives tailored to the individual customer’s telephone utilization patterns. Following the enactment of the ’96 legislation, however, the Federal Communications Commission adopted a so-called “opt-in” regulation that prohibited telecoms from gathering CPNI from any customer who did not affirmatively consent to the practice. U.S. West filed suit alleging that the FCC regulation violated the company’s First Amendment right to “solicit[ ] … customers to purchase more or different telecommunications services ….” (182 F. 2d at 1232.) The court agreed with U.S. West and invalidated the FCC regulation:

Although we may feel uncomfortable knowing that our personal information is circulating in the world, we live in an open society where information may usually pass freely. A general level of discomfort from knowing that people can readily access information about us does not necessarily rise to the level of a substantial state interest … for it is not based on an identified harm. [Id. at 1235.]

See also Bartnicki v. Vopper, 532 U.S. 514 (2001), holding that a radio station could broadcast the recording of a private, illegally intercepted cell phone conversation. Wrote Justice Stevens for a seven-member majority of the Court, “Exposure of the self to others in varying degrees is a concomitant of life in a civilized community. The risk of this exposure is an incidental incident of life in a society which places a primary value on freedom of speech and of press.” Id. at 534 (quoting Time, Inc. v. Hill, 385 U.S. 374, 388 (1967)).

(6) Does the recent Lawrence decision presage a change in direction? Lawrence, decided on the last day of the Supreme Court’s 2002-03 Term, struck down a Texas statute making it a crime for two persons of the same sex to engage in certain forms of intimate sexual conduct. Lawrence v. Texas, 539 U.S. 558 (2003). In his opinion for a six-Judge majority, Justice Anthony Kennedy—not one of the Supreme Court’s unabashed liberals, to be sure—took the rare step of overruling one of the Court’s earlier decisions (Bowers v. Hardwick, 478 U.S. 186 (1986)) and declared that the Constitution “protects the right to define one’s own concept of existence, of meaning, of the universe, and of the mystery of human life”—language broad enough to cause several commentators to wonder whether the decision might usher in an era of greater judicial solicitude for individual privacy rights. See Patty Reinert, Court’s Decision Viewed as Step Toward Equal Treatment for Gays, HOUSTON CHRONICLE, June 28,
(7) The Lawrence case notwithstanding: The constitutional right of privacy derived from Justice Douglas’s tantalizing decision in Griswold appears, almost forty years later, to be limited in scope and lacking in persuasive power to a new generation of federal judges. It is not a concept that makes the transition easily to contemporary threats to privacy posed by computers, computerized surveillance technologies, and other defining characteristics of the digital age.

IV. PROTECTING PRIVACY IN THE DIGITAL AGE

A. If the concept of a wide-ranging constitutional right to privacy predicated on “penumbral” rights has proven inadequate to the realities of the technological age, it doesn’t follow that privacy advocates have no weapons at their disposal with which to defend the privacy rights of individual citizens. In this section, we consider three other approaches to the protection of privacy rights—one premised on the Constitution (the Fourth Amendment guarantee of protection against unreasonable searches), one derived from common law (the tort of invasion of privacy), and one just emerging from the nascent national and international law of information technology.

B. Search and Seizure Law

(1) While no general right to privacy protects against intrusive surveillance, the Fourth Amendment guarantees an individual’s right to be “secure … against unreasonable searches and seizures,” and the Fourth Amendment has long provided protection against violations of individuals’ reasonable expectations of physical privacy.

(2) Under the Fourth Amendment, searches cannot be conducted unless the state actor performing the search obtains a warrant upon a showing of probable cause that a crime has been committed. Katz v. United States, 389 U.S. 347, 356 (1967). But in the context of an administrative search—a search undertaken, not to enforce criminal laws, but to assure compliance with institutional regulations, such as health codes, safety standards, or rules against drugs and alcohol—courts employ a balancing test under which the landlord’s interest in enforcing its standards is weighed against the intrusion on individual privacy interests. Camara v. Municipal Court, 357 U.S. 523, 536-37 (1967); New Jersey v. T.L.O., 469 U.S. 325, 336 (1985). See generally Kristal Otto Stanley, The Fourth Amendment and Dormitory Searches—A New Truce, 65 U. Chi. L. Rev. 1403, 1413-14 (1998). Courts are sympathetic to claims that warrantless searches were necessitated by the imperative of enforcing institutional policies and standards, particularly drug and alcohol policies. E.g., Moore v. Student Affairs Committee of Troy State Univ., 284 F. Supp. 725 (M.D. Ala. 1968).
C. Tort Actions for Invasion of Privacy

(1) According to the facts alleged in the complaint in Doe v. High-Tech Institute, Inc., 972 P. 2d 1060 (Colo. App. 1998), John Doe enrolled in a medical assistant training program offered by a private institution in Colorado called Cambridge College. Shortly after the course began, Doe disclosed to the course instructor that he was HIV-positive and requested the instructor to treat the information as confidential. A short time later, the instructor informed the class that all students at Cambridge were required to be tested for German measles. Each student was given a consent form indicating that a blood sample would be drawn for the purpose of performing the German measles test. Doe signed the form. Without his knowledge, the instructor ordered the laboratory to test Doe’s blood sample for HIV. When the test returned a positive result, the laboratory reported Doe’s name and address to the Colorado Department of Health and Cambridge College, all as required under state law. Doe subsequently sued Cambridge for invasion of privacy.

(2) Invasion of privacy, as the court observed in Doe, is the name given to a family of closely related common-law causes of action under the law of tort. A claim for invasion of privacy exists under any of the following circumstances:

- **False publicity**: If one is subject to publicity that places one in a false light in the public eye.

- **Appropriation of name or likeness**: If one’s name or likeness is appropriated without permission for another’s benefit.

- **Public disclosure of private facts**: If information or activities that one has held private are communicated or published to third parties.

- **Intrusion upon seclusion**: If private facts which would not otherwise be of legitimate concern to the public are disclosed in a manner that would be deemed highly offensive to a reasonable person.

The court in Doe focused on the third of these potential causes of action. The court held that a person has a privacy interest in his or her blood sample and in the medical information that can be obtained by testing it. A college that conducts unauthorized tests on blood samples or disseminates the results of unauthorized tests is liable for invasion of privacy. As the court continued in provocative dictum, the general tort of invasion of privacy would comprehend “repeated and harassing telephone calls, … [and] eavesdropping by wiretapping,” among other forms of conduct. Doe, 972 P. 2d at 1067, citing W. Prosser & W. Keeton, TORTS § 117 (5th ed. 1984).

(3) Courts have exhibited virtually no interest in protecting electronic privacy rights. In In re Doubleclick Privacy Litigation, 154 F. Supp. 2d 497 (S.D.N.Y. 2001), computer
users filed a class-action lawsuit against Doubleclick, Inc., one of the nation’s leading marketer of Internet advertisements, alleging that Doubleclick invaded their privacy by placing cookies on hard drives and harvesting—without the user’s knowledge or acquiescence—information about the user’s name, e-mail address, phone number and surfing habits. But the action was dismissed on the ground that the use of cookies did not violate federal cyber-privacy laws and wasn’t actionable under state invasion-of-privacy law. See also Note, Keeping Secrets in Cyberspace: Establishing Fourth Amendment Protection for Internet Communication, 110 Harvard L. Rev. 1591 (1997).\(^{11}\)

(4) So far, at least, courts have been unsympathetic to claims by the victims of surreptitious recording that their privacy rights have been invaded. In Desnick v. American Broadcasting Cos., 44 F. 3d 1345 (7th Cir. 1995), for example, the ABC-TV investigative show Prime Time Live send bogus patients equipped with hidden cameras into an eye clinic to gather evidence of allegedly deceptive marketing practices. The court held that the clinic, by opening its office to anyone expressing a desire for ophthalmologic services, passively consented to the videotaping of professional (as opposed to personal) interactions with clinic staff, and could not for that reason sue ABC for invasion of privacy. See also Medical Laboratory Management Consultants v. American Broadcasting Companies, Inc., 306 F. 3d 806 (9th Cir. 2002) (a television network did not violate the privacy rights of a medical laboratory when a producer posing as a patient surreptitiously filmed interviews with laboratory employees using a camera hidden beneath a wig); People for the Ethical Treatment of Animals, Inc. v. Berosini, 895 P. 2d 1269 (Nev. 1995) (barring an animal trainer from suing a co-worker who supplied secret videotape to PETA to substantiate allegations of cruelty to animals).\(^{12}\)

D. The Nascent Effort to Address Digital Privacy Issues in Federal Laws and Regulations.

(1) Although the legally enforceable right to privacy originated in the United States almost forty years ago in Griswold, the first and most comprehensive efforts to establish a legislative right of privacy were European. In 1995, the Council of Ministers of the European Union adopted a sweeping directive on The Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. The EU Directive, which became effective on October 24, 1998, provides broad protections against unauthorized “processing of personal data,” a term inclusively defined to cover the collection and storage of any information

\(^{11}\) But see Theofel v. Farey-Jones, 341 F. 3d 978 (9th Cir. 2004), a factually unusual case in which an Internet Service Provider was held to have violated the plaintiff’s privacy by complying with a subpoena for e-mail messages when the ISP constructively knew the subpoena was “patently unlawful.”

\(^{12}\) But see Food Lion v. Capital Cities/ABC, Inc., 194 F. 3d 505 (4th Cir. 1999) (allowing a grocery store chain to recover damages from ABC following broadcast of an investigative series based in part on the work of reporters who concealed their employment with the network and used miniaturized cameras and other forms of surreptitious recording).
relating to an identified or identifiable natural person. Declaring in its preamble that privacy is a basic human right, the EU Directive requires any company that collects personal data to inform subjects of the purposes for which the data will be used, and prohibits resale of data without the express permission of the individual data subject. The Directive holds companies strictly liable for unauthorized disclosure of personal data, and requires each member country in the European Union to designate a government agency with the power to investigate data processing that “poses specific risks to the rights and freedoms of individuals.”

The EU approach to electronic privacy is frequently invoked by privacy advocates in the United States as an aspirational model; as one observer noted, “[it] is difficult to imagine a regulatory regime offering any greater protection to information privacy, or any greater contrast to U.S. law.” Cate 1997 (see page 4 of this outline), page 48. The text of the EU Directive is reproduced as an appendix in Cate’s book, and is analyzed extensively on pages 34-48 of that book.

(2) The legal and political approach to privacy protection in this country is significantly different from the European model. In the United States, government agencies largely rely on the computer industry to police itself and—in the past, at least—have been reluctant to create privacy rights by statute or regulation. Reflecting the fact that political power is diffused in the United States among different branches of the federal government and between federal, state and local governments, regulatory efforts have until recently been fitful, uncoordinated, and largely ineffective in this country. At the federal level, Congress’s attention has focused on the federal government’s record access and safekeeping policies; the Privacy Act of 1974, for example, applies only to the recordkeeping practices of federal departments and agencies and does not reach any of the private-sector marketing or surveillance practices mentioned on pages 5-10 of this outline.

(3) Slowly, over the last decade, privacy has emerged as a popular cause on Capitol Hill and Congress has incorporated privacy protections into several federal statutes dealing with the custodianship of sensitive personal information. In 1994, for example, Congress enacted the Driver’s Privacy Protection Act, a law prohibiting state motor vehicle departments from releasing “personal information” from motorists’ driving records.13 Four years later, Congress passed the Children’s Online Privacy Protection Act of 1998, which, among other things, requires operators of Web sites targeted at children under the age of 13 to provide notice to parents of their information-gathering practices and verifiable “opt-in” parental consent before collecting personal information from children.14 In 1999, the Gramm-Leach-Bliley

13 18 U.S.C. § 2721. The law was enacted in response to the grisly murder of a young television actress, Rebecca Schaeffer, by an obsessed fan who allegedly obtained her home address from the California Department of Motor Vehicles.

Financial Services Modernization Act imposed significant restrictions on the ability of financial institutions to transfer “nonpublic personal information” on customers to nonaffiliated third parties.\textsuperscript{15} And although a lucid explanation of the massively complex Health Insurance Portability and Accountability Act—“HIPAA”—is beyond the scope of this outline, mention should be made of the Department of Health and Human Service’s much-maligned privacy regulation designed in a multiplicity of ways to safeguard the confidentiality of sensitive medical records.\textsuperscript{16}

(4) Over the last six or seven years, in response to persistent advocacy by privacy groups, the Federal Trade Commission has shown interest in a more activist approach. Beginning in 1996, the FTC staff prepared a series of reports on privacy issues relating to the use of computers. See www.ftc.gov/reports/privacy/privacy1.htm. In June, 1998, the Commission issued a report that castigated e-commerce companies for “fall[ing] far short of what is needed to protect consumers,” and told the online industry to make the case for effective self-regulation or face FTC rulemaking. Some attributed the FTC’s aggressiveness to signals that the EU would bar American e-commerce sites from soliciting customers in Europe unless the federal government took a tougher position on protecting online privacy – “a dispute,” the NEW YORK TIMES reported, “that threaten[s] to escalate into the first Internet trade war.” Edmund L. Andrews, European Law Aims to Protect Privacy of Personal Data, NEW YORK TIMES, October 26, 1998, page A1.

(5) Prodded by the FTC, the American computer industry made several efforts to forestall federal regulation by establishing industry standards protecting the privacy rights of computer users. In 1997, many of the country’s largest technology companies, including IBM, Compaq, Microsoft, and America Online, organized TRUSTe, a non-profit privacy initiative designed to enhance consumers’ confidence in the Web by awarding a “seal of approval” to sites that agreed to observe rudimentary privacy protections and post privacy policies on their Websites. The Better Business Bureau followed with a “seal of approval” program of its own. (For information on TRUSTe, see www.truste.org; on the Better Business Bureau program, see www.bbbonline.org.)

Although there is no legislative obligation to do so, most commercial Web sites today post privacy policies on their home pages. The typical privacy policy explains to visitors what personally identifiable information is gathered about them, what uses the host site makes of the information, and what steps visitors can take to restrict the dissemination of such information to third parties. According to a survey conducted for the Online Privacy Alliance, 94 of the 100 most frequently visited Web sites in the United States post privacy policies on their home pages, and about two-thirds of all Web sites have privacy policies. Online Privacy Alliance Says Web Sweeps Confirm


\textsuperscript{16} “Standards for Privacy of Individually Identifiable Health Information,” 45 C.F.R. Part 160.

(5) Finally, mention should be made of the privacy provisions in the USA PATRIOT Act, passed by Congress and signed into law by President George W. Bush a month and a half after the attacks of September 11, 2001. Section 215 of the Act significantly broadens the Federal Bureau of Investigation’s power to gain access to electronic records of citizens’ activities in connection with “an[y] investigation to protect against international terrorism.” That provision has been roundly condemned by privacy advocates, who see it as an invitation for “unchecked government power to rifle through individuals’ financial records, medical histories, Internet usage, bookstore purchases, library usage, travel patterns, or any other activity that leaves a record.” American Civil Liberties Union, Surveillance Under the USA PATRIOT Act, www.aclu.org/SafeandFree/SafeandFree.cfm?ID=12263&c=206. Other controversial provisions in the Act allow federal law enforcement officials to conduct warrantless searches of citizens’ homes and electronic records; liberalize the standards under which the FBI can obtain wiretap warrants; and make it easier for law enforcement officials to conduct so-called “pen register” searches of Internet records.

V. PRIVACY RIGHTS ON CAMPUS

A. Let’s test the following set of propositions.

Privacy protection on campus, never rock-solid to begin with, is in jeopardy because:

(1) Rapid advances in potentially threatening technologies have not yet galvanized courts and legislators to develop new standards and new theories for the protection of fundamental privacy rights on campus.

(2) In a counterintuitive but not necessarily illogical way, our own sense of privacy may have eroded. We willingly trade in our privacy to take advantage of the economies of the computer age.

(3) Many members of the campus community, like members of American society in general, exalt other rights—the right to physical security and the right, pernicious as it may be, to be bombarded by advertisements for new products and services—more than the right to privacy. Or, to express the same sentiment more positively and more eloquently:

---

Privacy—like most good things in life—entails costs. ... A premature insistence on regulatory control over market approaches ... may distort or prevent the evolution of initiatives that produce lower prices, increases convenience, provide more secure records, and foster new and widely beneficial civic and political interchange. With those benefits hanging in the balance, individuals, businesses, and regulators should tread carefully in giving privacy an exclusive position at the table.


Keep these points in mind as we explore four contemporary privacy issues on American college campuses: non-consensual searches, the release of hitherto private information about student disciplinary proceedings, the security of personally identifiable information maintained in campus computer systems, and the manner in which privacy concerns are addressed (or not addressed) in campus computer-use policies.

B. Non-Consensual Searches of Dormitory Rooms and Offices

(1) A preliminary consideration: public or private? The Fourth Amendment protects against “unreasonable searches and seizures,” and the Fourth Amendment has long provided protection against violations of individuals’ reasonable expectations of physical privacy. But like the rest of the protections in the Bill of Rights, the Fourth Amendment protects only against searches by government actors, not private ones. For our purposes, that means that the strictures in the Fourth Amendment apply to instrumentalities of the government—state-supported colleges and universities—and not to private institutions of higher education, with one narrow exception. See generally Kristal Otto Stanley, The Fourth Amendment and Dormitory Searches—A New Truce, 65 U. CHI. L. REV. 1403, 1405 (1998). See also Tennessee v. Burroughs, 926 S.W. 2d 243 (Tenn. 1996) (holding that a dormitory director’s warrantless search of a student’s room did not violate the Fourth Amendment because the college was private and the director was not acting as an agent or instrument of the state when he conducted the search).

In general terms, a private college or university has considerably more latitude in conducting unauthorized searches of campus buildings than does a public college or university. The narrow exception alluded to in the previous paragraph is when a search is conducted by a campus police or public safety officer in jurisdictions that by statute or ordinance bestow on private security forces all the powers of municipal, county, or state police officers. Under such circumstances, a search conducted by a campus security officer is governed by Fourth Amendment principles, even if the

(2) Students alleging that their privacy rights were violated by non-consensual searches of their dormitory rooms have fared poorly in court. With only a few exceptions, courts have sustained warrantless searches on one (or both) of two grounds:


(b) Such searches were necessary to enable campuses to enforce laws and regulations concerning the possession of drugs and alcohol. *E.g., Piazzola v. Watkins*, 442 F. 2d 284 (5th Cir. 1971). *But see Devers v. Southern Univ.*, 712 So. 2d 199 (La. App. 1998) (holding that a sweep of a campus residence hall violated students’ rights under the Fourth Amendment).

C. *Loosening Student Privacy Protections Under FERPA*

(1) Until 1998, the Family Educational Rights and Privacy Act of 1974, as amended, 20 U.S.C. § 1232g, contained what some perceived to be a loophole. FERPA, which was enacted in part to protect the privacy of education records by limiting the circumstances under which a record could be disclosed without the permission of the subject of the record, became a barrier to the release of sensitive, highly charged information about student disciplinary proceedings. In 1996, the student newspaper at the University of North Carolina Chapel Hill sued under the state Public Records Law to obtain the record of a disciplinary proceeding against two students accused of removing copies of a student-produced publication, the *Carolina Review*, from magazine racks around campus. The court held that the record was an “education record” under FERPA and that the university was under no obligation to produce it. *DTH Publishing Corp. v. Univ. of North Carolina at Chapel Hill*, 496 S.E. 2d 8 (N.C. App. 1998), review denied, 510 S.E. 2d 381 (N.C. 1998).

(2) That court case and others18 persuaded Congress that legislative clarification was in order. In 1998, as part of the omnibus Higher Education Amendments enacted that year, Congress amended FERPA to make it easier, in several respects, for colleges

---

18 In 1997, the Ohio Supreme Court ruled that records from campus disciplinary proceedings at Miami University were not “education records” protected by the Buckley Amendment. The court ordered the university to release disciplinary records to the student newspaper under a Public Records Act request. Before the university could do so, the United States Department of Education brought suit in federal court to enjoin the university from complying with the Ohio Supreme Court ruling, on the ground that compliance would violate Buckley. The dueling lawsuits, needless to say, caused much confusion. *Education Department Sues to Block Release of Campus Judicial Records*, CHORNICLE OF HIGHER ED., February 6, 1998, page A32.
and universities to release education records hitherto deemed private. Under the 1998 legislation and implementing Department of Education regulations, colleges and universities are permitted—not required, but permitted—to disclose the results of a disciplinary hearing against a student charged with a violent crime to the victim of the crime. In a controversial feature of the new law, colleges and universities are also permitted—again, not required, but permitted—to disclose to the parents of any student under the age of 21 that that student has been adjudged guilty of alcohol or drug offenses. Under prior law, FERPA prohibited colleges authorities from making that information available to parents.

(3) The new law has been controversial on many campuses:

“Not only do we have to consider what’s in the best interest of the students, but now we have to ask ourselves whether we have a legal duty to notify parents,” says Gus Kravas, vice-provost for student affairs at Washington State University, where students rioted last spring to protest strict alcohol rules. ...

William W. Harmon, vice-president for student affairs at the University of Virginia, says if it’s necessary to call parents, the student—rather than an administrator—should do the dialing.

“We have students who say that when they screw up in the larger society, the world isn’t going to call their parents,” Mr. Harmon says. “If I’m 18 years old and someone says, ‘I’m going to tell your mother on you,’ I’m not sure how I would respond to that, as opposed to someone saying, ‘Look, I think you have a problem, let’s see if we could deal with it.’

“In some instances, I think it’s appropriate to call the parent; in others, I’m not so sure, and that’s why we haven’t developed a consistent policy.”


D. Just how secure are those campus mainframes? From Tanya Schevitz, Colleges Leaking Confidential Data; Students Compromised by Internet Intrusions, SAN FRANCISCO CHRONICLE, April 5, 2004, page A1:

Colleges across the country, through computer security failure and human error, have exposed confidential information about hundreds of thousands of students and employees over the Internet, and experts say they expect the problems to continue.

In addition to being targeted by some very savvy hackers, college computer systems have been made vulnerable by the schools themselves through inadequately trained employees who have access to the files.

“It is not an arena where anything stands still,” said security consultant Cedric Bennett, emeritus director of Information Security Services at Stanford University. “You might be doing great work (training people and securing your system); meanwhile, the laws are changing and the bad guys are getting more sophisticated.” ...

The problem has been highlighted in recent months by some high-profile breaches of computer-stored records including names, addresses, Social Security numbers and, in some cases, even credit cards, for applicants, students, alumni and staff.

- San Diego State University reported in March that hackers broke into a server in the Office of Financial Aid and Scholarships, gaining access to names and Social Security numbers for more than 178,000 former and current students, applicants and employees.

- The University of California notified 2,156 applicants a few weeks ago that an overloaded server may have allowed Social Security numbers, test scores and other personal details to be shared over the Internet with competing applicants.

- Some 2,800 applicants of the California State University at Monterey Bay were informed in February that their names, addresses and Social Security numbers were made available on the Internet by an employee who moved the data to a computer folder that was not secure. The data was accessed more than 100 times from around the world before the error was discovered.

- At the Georgia Institute of Technology, a hacker downloaded information that could have included names, addresses, phone numbers, e-mail addresses and credit card numbers for about 57,775 patrons from the campus arts center box office in March.

- At the University of Texas at Austin, 55,200 names and Social Security numbers were downloaded by hackers in March after a similar incident in October.

- At New York University, it was discovered in January that several mailing lists with names, birth dates, addresses, phone numbers, e-mail addresses and some Social Security numbers for at least 2,100 students, alumni and professors were inadvertently posted on a campus Web site, according to the campus newspaper, the Washington Square News.
Computer experts say that data erroneously posted on the Internet could have been copied or accessed before the problem was discovered, leaving individuals vulnerable for years.

“We live in an age now when anything that goes into a database has the potential to be compromised intentionally or unintentionally,” said Chuck Haupt of Pleasanton, whose son was one of the applicants whose data was compromised at CSU Monterey Bay. ...

Although the problem of computer security is not limited to colleges and universities, academic institutions thrive in a culture of openness and the sharing of information, and some see the tightening of security procedures as a threat to that culture, said Bennett, the expert from Stanford.

“At a corporation where, for the most part, they want to keep the information inside the corporation, they put up big fences,” Bennett said. “Universities, because they tend to be relatively open and invite inspection, tend not to put up fences. So it makes it even harder to manage the data which by law needs to be protected.” ...

Privacy experts and college administrators agree that the most sensitive piece of information exposed on campus networks is a student’s Social Security number, and efforts are under way to protect that, at the very least. ...

“Social Security numbers were on ID cards, they were on library cards, they were used in the gym, in every activity on campus,” [said State Senator Debra Bowen, D-Redondo Beach (Los Angeles County)]. “Grades were posted by Social Security number. Items with the Social Security number went to students in the mail. If they have their Social Security number plastered everywhere, they will be at risk.”

See also University of Georgia, Information Regarding Computer Breach, www.uga.edu/inside/fraudconcerns.html. This Web site chronicles the steps the University of Georgia took after discovering in early 2004 that “computer intruders” had hacked into a university server and made off with the names, Social Security Numbers, and credit card account numbers of an undetermined number of students.

E. Privacy: The Great Disappearing Act in Campus Computer-Use Policies

(1) The majority of American campuses today have policies in place that regulate the use of computing facilities. The Institute for Computer Policy and Law, administered by Cornell University and EDUCAUSE, has done a significant public service by collecting policies from several hundred institutions and placing them on a Website (www.educause.edu/icpl/library_resources.asp).
To what extent do these policies address privacy issues? While some institutions go to great lengths to ensure that the privacy rights of computer users are respected, most treat the subject cursorily, if at all. A typical provision is this one, from the Georgia Institute of Technology’s *Computer and Network Usage Policy*:

> To the greatest extent possible in a public setting, Georgia Tech seeks to preserve individual privacy. Electronic and other technological methods must not be used to infringe upon privacy. However, Georgia Tech computer systems and networks are public and subject to the Georgia Open Records Act. All content residing on Institute systems is subject to inspection by the Institute.

(2) Many, perhaps most institutions reserve the right to monitor the computer use of individual members of the campus community. Here is a typical provision, this one from Tufts University’s *Information Technology Responsible Use Policy*:

> The University may also specifically monitor the activity and accounts of individual users of University computing resources, including individual login sessions and communications, without notice, when:

- The user has voluntarily made them accessible to the public, as by posting to Usenet or a web page.
- It reasonably appears necessary to do so to protect the integrity, security, or functionality of University or other computing resources or to protect the University from liability.
- There is reasonable cause to believe that the user has violated, or is violating, this policy.
- An account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns.
- It is otherwise required or permitted by law.

> The University, at its discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual communications, to appropriate University personnel and/or state or federal law enforcement agencies and may use those results in appropriate University disciplinary proceedings or in litigation.

(3) Very few institutional policies limit campus authorities’ use of cookies or other technologies to monitor computer utilization for research or internal administrative purposes, an omission that some privacy proponents regard as indefensible. Vincent Kiernan, *Use of “Cookies” in Research Sparks a Debate Over Privacy*, *Chronicle*
VI. CONCLUSIONS

A. We have not inherited from the pre-digital age a Constitutional regime sympathetic to the privacy rights of individual citizens. The right to privacy is narrower than one might at first blush believe, comprehending at most limited freedom from government interference in sensitive matters relating to marriage and family—but little more. In sphere after sphere of jurisprudence—from search and seizure law to the common law of tort, from the Buckley Amendment to the emerging law of international data collection—privacy rights are fragile and in retreat.

B. Second, self-regulation—by commercial Web sites, by hardware and software companies, even by universities that own centralized computing systems—leaves much to be desired in terms of the protection it affords to individual users’ privacy.

C. Third, in today’s digital world, privacy is under assault. Analog information that formerly vanished the moment it was shared with another has been replaced with digital information that seemingly exists forever. Once created, digital information can be stored cheaply, manipulated, and disseminated with terrifying speed to masses of recipients, some of whom have their own commercial interests in mind when they seek access to it.

D. Fourth and paradoxically—many of us don’t care. We view the loss of privacy as the reasonable cost of efficiencies associated with computerization. According to Professor Alan Westin, one of the great figures in the intellectual development of privacy law in this country and the author of the classic book PRIVACY AND FREEDOM (1967), only about a quarter of the population is vigilant about privacy rights. About the same percentage is indifferent. Dr. Westin refers to the 50 percent of the population in the middle as “privacy pragmatists,” people who are willing to sacrifice their privacy if they understand the benefits. Katie Hafner, Do You Know Who’s Watching You? Do You Care?, NEW YORK TIMES, November 11, 1999, page G1. As if to make the point, the study conducted by Jupiter Research last year (see page 8 of this outline) revealed the startling fact that, although seven out of ten American consumers profess to be aware of, and concerned about, the loss of privacy online, 82 percent of consumers will willingly surrender personal information to shopping sites on the Web if they believe they will receive something of value—even of very modest value—in return, such as a small discount on the cost of a purchase or a chance to win a raffle or a sweepstakes. (www.jupiter-research.com/xp/jmm/press/2002/pr_060302.html.)
In a perceptive law review article that appeared four years ago, hi-tech lawyer Kent Walker argued that privacy protection comes at a societal cost. His article begins with this passage:

Privacy is good and privacy is grand. ... It is perhaps essential to the capacity for creativity and eccentricity, for the development of self and soul, for understanding, friendship, and even love. And it may well be that the struggle over privacy is the preeminent issue of the Information Age.

And yet. And yet . . .

Privacy, construed as the withholding of personal information from others, keeps you from enjoying all that society and the market have to offer. Perhaps more troubling, withholding such information sometimes reduces these benefits for everyone else as well. ... [We should not lose sight of] the ever-increasing individual and community benefits of information exchange and ... the potential costs of regulating how we exchange information about ourselves. My argument is obviously not against privacy, but rather in favor of a sound balance of privacy and other virtues.

Kent Walker, Where Everybody Knows Your Name: A Pragmatic Look at the Costs of Privacy and the Benefits of Information Exchange, 2000 STAN. TECH. L. REV. 4 (footnotes and internal quotations omitted). He goes on to list eight “benefits of information exchange” that represent, in his view, the upside of accepting modest, reasonable limitations on the right to information privacy. Here are the most salient:

- **Cost savings.** “[W]ithholding your contact information typically means that you won’t see the discounts and offers that are most likely to interest you—whether those are free videos, discounts on kids’ toys, a deal on a new computer when you’re in the market to buy one, or a cut-rate airfare to your home town. That kind of tailored discount has real value in reducing the cost of living for millions of Americans.”

- **Convenience.** “Having some information about yourself out there in the world offers real convenience that goes beyond dollars and cents. Many people benefit from warehousing information—billing and shipping addresses, credit card numbers, individual preferences, and the like—with trustworthy third parties. Such storage of information can dramatically simplify the purchasing experience, ensure that you get a nonsmoking room, or automate the task of ordering a kiddie meal every time your child boards a plane. ... Because these types of information and service come secondhand, via computer rather than direct observation, they

---

20 Regrettably, the Lexis version of Mr. Walker’s law review article—the version I used—contains no jump-cite pagination, and for that reason the lengthy quotations in the next few paragraphs lack specific page citations.
can seem spooky or artificial. But the process is the same, and the result is the creation of a ‘virtual small town’ where people know more about each other.”

- Fostering a heightened sense of community.

  In a very real sense, privacy creates a Tragedy of the Commons effect, in which not sharing information imposes costs on others. The most ready example is the unlisted phone number. Unlisting a phone number has the same effect as not having your street address visible from the street: it makes it more difficult for others to find you. You may not care about some of those “others”—say, direct marketers who call during dinner—but some “others” are friends, relatives, or business associates who have mislaid your number or with whom you would have gladly shared your number but just never did. ... Without having information about ourselves out in public, we appear to the outside world as anonymous and interchangeable. Providing such information gives texture to our public persona, permits tailoring of information, and provides traction to others who seek to engage us.

  While community isn't always an unalloyed virtue, the ultimate question is one of balance and flexibility. Privacy reflects an individualistic ethos, openness and disclosure a communitarian one. It would be no better to have everything public than to have everything private.

- Security. “The very identifiers that most concern many privacy advocates—Social Security Numbers, driver’s licenses, or universal health care cards—are the keys to ensuring that the information for John M. Smith isn't confused with the information for John N. Smith. … [A]uthentication of one's identity is essential to combating fraud and confirming the legitimacy of a request. …Distributed information can reduce the costs of fraud and other economic crime. Many websites store passwords and hints to authenticate return visitors. And analysis of patterns of transactions can help to reduce fraud and other sorts of economic crime. For instance, cellular phone companies flag variations from your usual calling patterns in trying to detect whether someone may have surreptitiously stolen your number.”

E. As the baton is passed to Rick Johnson for the presentation after my own, let’s pose once again the policy question that appeared in bold-faced type on page 3 of this outline: “[W]hat Internet architecture—in other words, what set of protocols and rules—best and most appropriately strikes the balance between (on the one hand) minimally regulated access to the Web and (on the other) the protection of the privacy rights of Web users?” It’s a question, truthfully, that few campuses have seen fit to address. It requires the higher education community to calibrate more precisely than it has in the past the very real benefits associated with the protection of personal privacy and the equally real costs that attach when obstacles prevent the free exchange of information about computer use.
Appendix: Privacy Advocacy Organizations

Like the Internet itself, the landscape of organizations dedicated to the protection of online privacy is vast, disorganized, and constantly changing. No organization has assumed a preeminent role representing computer users on the privacy front. Most of the organizations that have achieved some visibility in the last five years are small in terms of both their budgets and their staffs.

The organizations profiled below are arbitrarily divided into three categories. The first group are foundation-supported or membership-supported organizations that focus on general electronic privacy issues, usually as advocates for privacy protection, supporters of government regulation in the European tradition, and skeptics of industry self-regulation. The second group consists of organizations created or financially supported by the technology industry. In the third group are small special-interest organizations that tend to focus on one aspect of privacy.

A. Organizations with a General Focus

American Civil Liberties Union
Cyber-Liberties Project
www.aclu.org/Privacy/PrivacyMain.cfm
New York, NY

The ACLU is the nation's largest and best-known advocate of individual rights. Its Privacy and Technology Project focuses on privacy, censorship, and surveillance issues in cyberspace.

Computer Professionals for Social Responsibility
www.cpsr.org
Palo Alto, CA

CPSR is an alliance of computer scientists and others concerned about the impact of computer technology on society. It was founded in the early 1980s and is one of the nation's oldest organizations dedicated to computer use issues. Its goal is to supply technical expertise on issues affecting the development and use of computers. CPSR’s “Privacy and Civil Liberties Project,” founded in 1986, subsequently reorganized and became the Electronic Privacy Information Center (see below).

Electronic Frontier Foundation
www.eff.org
San Francisco, CA

EFF is a nonprofit organization promoting fundamental civil liberties in cyberspace. Its mission is “to help civilize the electronic frontier; to make it truly useful and beneficial not just to a technical elite, but to everyone; and to do this in a way which is in keeping with our society's highest traditions of the free and open flow of information and
communication.” Founded in 1990, EFF is one of the nation’s largest electronic privacy organizations, with twelve staff members.

**Electronic Privacy Information Center**  
[www.epic.org](http://www.epic.org)  
Washington, DC  
EPIC, founded in 1994 as the reorganized incarnation of the Privacy and Civil Liberties Project of Computer Professionals for Social Responsibility, is a public interest research center focusing on emerging privacy issues relating to the Internet. EPIC’s staff of seven includes two of the most visible proponents of electronic privacy: Marc Rotenberg, the Director, and David Sobel, the General Counsel.

**B. Industry-Sponsored Organizations**

**Center for Democracy and Technology**  
[www.cdt.org](http://www.cdt.org)  
Washington, DC  
This nonprofit organization fosters “democratic values and constitutional liberties in the digital age.” It has a number of projects, one of which focuses on Internet privacy issues. Funding is provided by Internet-related companies, including AOL, AT&T, IBM, Microsoft, and more than 30 others. CDT is a large organization, with a dozen staff members and an elaborate Web page.

**Online Privacy Alliance**  
[www.privacyalliance.com](http://www.privacyalliance.com)  
Washington, DC  
OPA is an industry-funded organization created to head off government regulation of the Internet and promote industry self-regulation. It describes itself as “a diverse group of corporations and associations who have come together to introduce and promote business-wide actions that create an environment of trust and foster the protection of individuals’ privacy online.” Although its staff is small, OPA has already staked out a significant role as a high-visibility player in the electronic privacy arena.

**C. Special Interest Organizations**

**Junkbusters**  
[www.junkbusters.com](http://www.junkbusters.com)  
Green Brook, NJ  
Junkbusters, founded in 1996, arms consumers with software and other weapons to combat the proliferation of computerized junk mail from direct marketers. Its popular, aggressively written Web site includes a page titled “How to Protect Your Privacy from...
Commercial Invasions.” Unlike organizations identified above, Junkbusters is a profit-making site and unabashedly so.

**Privacy Rights Clearinghouse**
www.privacyrights.org
San Diego, CA
PRC is a project of Utility Consumers Action Network, a consumer advocacy group. It focuses on privacy issues of interest to e-commerce customers and functions as an online consumer protection bureau.

**Media Access Project**
www.mediaaccess.org
Washington, DC
MAP is a venerable (30-year-old) public interest law firm that “represents the public’s First Amendment right to have affordable access to a vibrant marketplace of issues and ideas via telecommunications services and the electronic mass media.” In recent years, MAP has become a champion of electronic free speech and has led the effort to have Congressional restrictions on Internet speech declared unconstitutional.

* * * * * * * * * * * * * * * * * * * * * *

This appendix lists nine organizations that are dedicated in one fashion or another to the exploration of electronic privacy issues. They are all small (or small projects of larger organizations); even the biggest of them have staffs of less than 15 people and annual budgets under $1 million, and many of them are one-person operations. For space reasons, I’ve stopped with nine. The EPIC home page alone lists close to fifty organizations and Web sites dedicated to the protection of electronic privacy,21 and it’s safe to say there are scores, perhaps hundreds of others in the disorganized clutter of cyberspace.

---

21 www.epic.org/privacy/privacy_resources_faq.html#Privacy_Organizations.