INTERNET PRIVACY:
THE ELECTRONIC DIMENSION

Presenter:

LAWRENCE WHITE
Program Officer
The Pew Charitable Trusts
Philadelphia, Pennsylvania

Stetson University College of Law:

22nd ANNUAL LAW & HIGHER EDUCATION CONFERENCE
Clearwater Beach, Florida
February 18 - 20, 2001

STETSON UNIVERSITY COLLEGE OF LAW
22nd Annual National Conference on Law and Higher Education

DRIVER EDUCATION FOR THE INFORMATION SUPERHIGHWAY: THE LAW AND POLICY OF THE INTERNET

INTERNET PRIVACY: THE ELECTRONIC DIMENSION

Lawrence White*
Program Officer
The Pew Charitable Trusts
Philadelphia, Pennsylvania

February 18, 2001

Introduction

Americans are slowly discovering that computers pose a threat to their privacy. Computers convert the most intimate of communications – writing letters, speaking on the telephone, filling prescriptions, taking photographs – into electronic records that are easy to store and easy to access. By networking computers and using them to exchange files at high speed, the owner of the network can aggregate electronic information about the private habits of computer users. We are uneasy about the motives of organizations gathering that information and the uses to which information is being put. We fear for our privacy in cyberspace.[1]

This presentation explores some of the privacy problems associated with computer use on college and university campuses at the dawn of the digital millennium. It describes some of the ways in which advances in computer technology jeopardize the privacy rights of campus computer users and those whose movements are tracked by computers. And it examines the

---

* The views expressed in those treatments and in this one are entirely the author's own and should not be attributed to The Pew Charitable Trusts.

This presentation borrows liberally from three prior treatments of this topic by the author: an outline entitled *Is the Right of Privacy Disappearing? Revisiting Issues of Privacy in the College and University Setting*, prepared for the Stetson University College of Law's 21st Annual National Conference on Law and Higher Education in February, 2000; an outline entitled *Surveillance, Search and Seizure: The Electronic Dimension*, prepared for the University of Vermont's Tenth Annual Conference on Legal Issues in Higher Education in October, 2000; and an article entitled *Colleges Must Protect Privacy in the Digital Age* that appeared in the CHRONICLE OF HIGHER EDUCATION on June 30, 2000.

[1] Research conducted last year by the Pew Internet and American Life Project in Washington, D.C., revealed that an overwhelming majority of American computer users are apprehensive about their cyber-privacy. Tracking polls showed that 84 percent of Americans distrust the motives of Web-site operators who collect personal information about visitors to their sites, and two-thirds of all computer users are reluctant to supply credit card information on-line because of misgivings about unauthorized use of credit card numbers. *The Internet Life Report on Trust and Privacy Online: Why Americans Want to Rewrite the Rules*, August 20, 2000 (available on-line at www.pewinternet.org/reports).

various ways – common law, statutory, regulatory, self-regulation – by which campus privacy advocates seek to protect people's privacy in the age of computer technology.

A Crash Course (no pun intended) on Digital Threats to Privacy

A. The last decade has witnessed an explosion in the amount of information available in digital form. As telephones are replaced by computerized telephony, analog television signals by digitized cable transmissions, letter writing by word processing, phonograph records by MP3 files, conventional film by camera diskettes and DVD disks, digitization has revolutionized the way we create and store words, pictures and sounds. Intimate communications that once vanished without a trace after they were uttered can now be recorded, stored inexpensively, and reproduced for audiences of thousands or even millions. Information technologies have spread into every facet of life, from the workplace to the marketplace to the home. "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.

B. At just the moment when the amount of digitized information is exploding, information technology is growing faster, cheaper, and easier to use. Today, 50 percent of American homes have computers that can access the Internet, up from 45 percent a year ago and less than 15 percent in 1995. By the year 2003, 177 million Americans – two-thirds of the country's population -- will be online. Global commerce via the Internet, which stood at $50 billion in 1998, more than doubled in 1999 to an estimated $111 billion, and will increase tenfold over the next three years to $1.3 trillion in 2003.[2]

   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. As former Vice President Al Gore observed last year, "there is more computer power in a Palm Pilot than in the spaceship that took Neil Armstrong to the moon...." LOS ANGELES TIMES, August 18, 2000, page U-8.

C. The proliferation of computers, our growing dependence on them to perform work- and household-related tasks, and the ease and low cost with which data can be collected and shared with third parties have prompted growing concern about the privacy rights of computer users. As long ago as 1996, noted privacy advocate Marc Rotenberg predicted that "privacy will be to the information economy of the next century what consumer protection

[2] The figures in this paragraph are taken from the "Metrics" page on the Web site of *The Industry Standard*. These figures and many others on the Internet economy are available at www.thestandard.com/metrics/archive.

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.) Computer privacy surfaced as an issue in last year's Presidential election and was identified in polls as *the* determinative issue in several races for the United States Senate. *Gore Targets Social Security ID Theft*, WASHINGTON POST, June 9, 2000, page A6; *Washington Race for Senate Heats Up*, PORTLAND OREGONIAN, August 22, 2000, page A4.

Privacy advocates identify two distinct kinds of threats associated with computer technology:

(1) *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 – their e-mail addresses if they expect to receive a response, their credit card numbers if they make a purchase, their fingerprints or photograph if they seek admittance to a secured area. Users are usually 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 us and gives rise to privacy concerns.[3]

(2) *Surveillance concerns.* Computers are increasingly used to track people's movements, both in cyberspace and in real space. "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

[3] Do you want an example that strikes close to home? Lauren Weinstein, publisher of the on-line report *Privacy Forum Digest*, featured a story in the January 6, 2000, edition (www.vortex.com/privacy/priv.09.03) about a new Website, www.anybirthday.com, that has reportedly aggregated information on the date of birth, place of birth, and gender of more than 130,000,000 American citizens. The site is operated by www.locateme.com, one of the many companies on the Web that uses public voter registration and driver's license databases to collect highly personal information (address, Social Security number) about anybody on the face of the planet. I just plugged my own name and Zip code into the anybirthday.com search engine, and a few minutes later the precise date of my birthday, including the year, was displayed. I then put my name and birth date into the locateme.com database and got my Social Security number. Try it with your own name.

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.

Surveillance technology is embedded in the software that runs our computers. Two years ago, two of the country's largest technology companies, Intel and Microsoft, were criticized by privacy groups for offering new products – processing chips in Intel's case, system software in Microsoft's – containing embedded identification numbers that allowed users' individual movements over the Internet to be tracked. At about the same time, a small software company called Andromedia created a stir by introducing a new product that allows Web page retailers to watch the online shopping behavior of individual consumers in real time. Using the new software, companies can watch which items a customer inspects, puts in or removes from a shopping cart, and buys. "We're starting to get into the heads of the shoppers because we're tracking not only purchases but the events around the purchasers," said Kathleen Hayes, director of business development at Andromedia. *Online Data's Fine Line – As the Technology to Gather Customer Data Online Gets More Sophisticated, Businesses Walk a Tightrope Between Use and Abuse*, INFORMATIONWEEK, March 29, 1999, page 18. Privacy advocates immediately objected: one critic "compare[d] the [new] technology to a salesperson who follows shoppers around a store watching everything they consider buying," and asked, "if a shopper won't allow someone to follow him around the store, why would he allow online marketers to observe him shopping online?" *Id.*

Also in 1999, the *New York Times* disclosed that a popular software program called RealJukebox, used to download music files from the Internet, contained a surreptitious code that allowed the manufacturer to track the name of each song downloaded to the user's hard drive, the format used to store the song, the user's preferred music genre, and the type of portable music player attached to the user's computer. Although the company's Web site contained an elaborate privacy notice, the monitoring practices were not disclosed. "CD Software Said to Gather Data on Users," *New York Times*, November 1, 1999, page C1.[4]

[4] 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, 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.

For an astonishing example of the intrusive nature of video surveillance in the workplace, go to www.aclu.org/issues/worker/wkp.mov. This Web page, prepared by the American Civil Liberties Union, shows a 30-second film clip of an employee changing clothes and sitting on a toilet in a workplace locker room. The

D. Computers are part of the landscape on all college and university campuses today. According to a recent report prepared by Dun & Bradstreet, institutions of higher education spent almost $3 *billion* last year on hardware and software to support academic and administrative computing, 28 percent more than the previous year. *Many Colleges Are in a Spending Spree for Information Technology*, CHRON. OF HIGHER ED., March 31, 2000, page A52. When students, faculty and staff use computers, they are often asked to disclose information about themselves. They are usually willing to provide personal information as long as they understand why it's being sought and how it might be used. What they may not appreciate, however, is the extent to which that information can be, and occasionally is, used for unauthorized or unexplained purposes:

(1) Many campuses have replaced traditional student identification cards with so-called "smart cards" containing embedded computer chips. Some colleges have entered into commercial arrangements with vendors, who use the computer records generated by chips to track students' purchasing habits for marketing and advertising purposes. According to a report that appeared in the CHRONICLE in 1999, students at one college with smart cards complained of being "bombarded" with commercial solicitations on the voice-mail systems in their residence halls. *Some Students Think "Smart" Identification Cards Go Too Far*, CHRON. OF HIGHER ED., September 10, 1999, page A39.

(2) Desk-top computers store e-mail messages and Web site caches. Increasingly, campus security personnel enlist information technology personnel in the search for digital evidence that can be used in disciplinary cases against students and faculty members. In one case that occurred in 1998, officials at a public university in North Carolina responded to a student's sexual harassment complaint by seizing a faculty member's office computer and searching the hard drive for e-mail messages between the faculty member and the complaining student. *Professor Cited for "Amorous" Relationship With Student Accuses Appalachian State U. of Violating His Rights*, CHRON. OF HIGHER ED., March 20, 1998, page A13.

(3) As part of their employee health insurance plans, many colleges and universities provide prescription drug cards to their faculty members and staff. When covered employees use their cards to purchase prescription medication, a record of the transaction showing the name of the employee and the prescription drug is generated and stored in the plan manager's database. Through the prescription drug subsidy, colleges and universities can learn which employees take prescription medication for emotional disorders, HIV infection, or other medical conditions. While there is no evidence that any institution has accessed confidential prescription-drug information

---

employee, who did not know he was being videotaped, is heard saying, "When I first saw the video, I was shocked. The first thing that went through my head was, 'How dare they?'"

without an employee's knowledge, nothing in most institutions' plan descriptions prohibits the practice. As the general counsel of one university said to me recently, it would be tantamount to professional malpractice for a lawyer representing an institution in a lawsuit brought by an employee *not* to examine the plaintiff's medical records if the institution were legally entitled to do so.

(4) The unauthorized disclosure of Social Security numbers poses special privacy concerns because, in the wrong hands, they can be used to obtain credit histories, bank statements, driver's license numbers, and other sensitive information about individuals. Federal law prohibits the unauthorized disclosure of Social Security numbers. Notwithstanding that prohibition, many colleges identify students and staff members by their Social Security numbers, even posting those numbers on Web pages. Glen Roberts, a computer consultant and the operator of a privacy protection Web site called "Fulldisclosure.org," created a minor sensation three years ago when he reported that Indiana University had posted the Social Security numbers of almost 3,000 faculty members on a publicly accessible Web page. Mr. Roberts also reported that privacy-protection advocates had easily obtained the last names and Social Security numbers of every student at Keene State College, which they placed on a diskette and delivered to the campus newspaper. *Posting Students' Social Security Numbers on Web Sites Called a Threat to Privacy*, CHRON. OF HIGHER ED., June 12, 1998, page A28.

(5) Many e-commerce sites on the World Wide Web utilize "cookie" technology to learn basic information about people who visit their sites, including Zip code, Internet service provider, what parts of the Web site are visited, and how long each visit lasts. Less well known is the fact that a growing number of colleges and universities are using cookies to gather information about prospective students who visit Web sites. Some university faculty members who do research on Web-related topics use cookies to track the surfing habits of research subjects, sometimes without disclosing that fact – a practice other faculty members have called unethical and improper. *Use of "Cookies" in Research Sparks a Debate Over Privacy*, CHRON. OF HIGHER ED., September 25, 1998, page A31.

(6) Surveillance cameras are ubiquitous on many college campuses, particularly those in urban areas. At one university in New York City, for example, residence hall security systems include guards on duty at the front entrance 24 hours a day, video cameras in the lobby and at locked rear entrances, and a magnetized "swipe" machine for reading bar codes on student identification cards. *See* Robert D. McFadden, *Columbia Student Slain, and Suspect Kills Himself*, N. Y. TIMES, February 6, 2000, page B1. On many campuses, digitized surveillance systems make it possible to track the movements of students and employees into and out of campus buildings, residence halls, parking lots, and other high-security areas.

Protecting Electronic Privacy in the Digital Age

A. In this section, we consider four approaches to the protection of privacy rights – one derived from common law (the tort of invasion of privacy), one based in statute, one just emerging from the nascent national and international law of information technology, and one predicated on the hyper-modern notion of self-regulation.

B. *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 informed the instructor that he was HIV-positive and requested the instructor to treat the information as confidential. Soon afterward, 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:

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

(b) *Appropriation of name or likeness*: If one's name or likeness is appropriated without permission for another's benefit.

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

(d) *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.

A person has a privacy interest in his or her blood sample and in the medical information that can be obtained by testing it, and an institution of higher education 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) But is *Doe* an aberration? *Doe* involved perhaps the most sensitive information imaginable: information about communicable disease status. What about more mundane information? Interestingly, although one would imagine many circumstances in which unauthorized access to computer files might give rise to invasion-of-privacy litigation, the number of reported cases is quite small and parties seeking to vindicate privacy rights have usually failed. Typical is *Battenfield v. Harvard University*, 1993 Westlaw 818920 (Super. Ct. Mass. 1993). The plaintiff, an administrator at Harvard, filed suit on a variety of theories (constructive discharge, sexual harassment, negligent supervision, and many others) following her resignation. As part of her legal action, the plaintiff contended that university officials invaded her privacy by inspecting her computer hard drive, without her permission or knowledge, while she was out on sick leave. The trial court brusquely dismissed her claim, observing that a university employee "has little or no privacy interest in her work files, given that such information is property of her employer."

Under the computer use policies in place at most colleges and universities, computers are supposed to be used for work-related or study-related purposes only. The institution owns computer hardware and software and expressly reserves the right (under most policies) to inspect computer files and drives. With the rules of the road so unambiguously established on most campuses, it is difficult for computer users to prevail on invasion-of-privacy claims.

(4) As one expert on privacy law recently observed:

> Surreptitious taping and filming present especially dicey situations. As the technology to miniaturize cameras, recorders and transmitters has become more affordable, predictions – or fears – of an explosion of litigation may be realized. But until courts decide more cases, the ... limits are hard to discern. [Bruce W. Sanford, LIBEL AND PRIVACY 534.1 (2d ed. 1999).]

Nevertheless, courts have proven surprisingly resistant 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 McCall v. Courier-Journal & Louisville Times Co., 6 Media L. Rep. [BNA] 1112 (Ky. App. 1980), *rev'd on other grounds*, 623 S.W. 2d 882 (Ky. 1981), *cert. denied*, 456 U.S. 975 (1982) (barring a lawyer from suing a woman who posed as a client and secretly tape-recorded a meeting in an effort to aid a newspaper that was investigating the lawyer for jury tampering); *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). *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).

C. *A Statutory Response: The Electronic Communications Privacy Act*

(1) It's hard to believe we're about to mark the *fifteenth* anniversary of Congress's passage of the Electronic Communications Privacy Act, 18 U.S.C. § 2510 *et seq.* Enacted at the dawn of the e-mail and cell-phone age, the ECPA was essentially designed to extend rudimentary privacy protection dating back to the "probable cause" requirement for telephone wiretaps to the new manifestations of the digital age. In Congress-speak, the ECPA amended the 1968 Omnibus Crime Control and Safe Streets Act (commonly known as the "wiretap statute") to extend privacy protections to the electronic transmission and storage of computer data.

(2) The ECPA makes it unlawful for any person to "intercept" – we'll see what that means in a moment – any electronic communication, or to intentionally disclose any electronic communication known to have been obtained by unlawful interception.

(3) *But*: The ECPA creates three major exceptions to the general prohibition against interception of electronic communications, and the courts have created a fourth.

(a) *Public access*: Notwithstanding the prohibitions in the ECPA, it is lawful for a person to intercept or access an electronic communication if the communication is made through a system that "is readily accessible to the general public." This is a longwinded way of saying that the law is not violated when one computer user posts an e-mail message to an on-line chat group, a public Web page, or a generally accessible electronic bulletin board and a second computer user reads the first user's posting.

(b) *Employer-owned system*: When an organization operates its own computer system, it may assign to employees or agents the task of monitoring electronic communications if necessary to the provision of computer services or the protection of computer equipment. The ECPA thus gives a university the right to monitor e-mail files maintained by students, faculty, and staff.

(c) *Consent*: The ECPA permits interception of electronic communications when one of the communicating parties "has given prior consent to such interception...." University computer use policies frequently incorporate consent provisions that give Information Technology personnel broad rights to intercept and monitor computer data traffic.

(d) *The narrow definition of "intercept."* The strictures of the ECPA apply only to one who intercepts electronic communications. The Act defines "intercept[ion]" to mean "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use *of any electronic, mechanical, or other device*. 18 U.S.C. § 2510(4). The issue in *Wesley College v. Pitts*, 974 F. Supp. 375 (D. Del. 1997), *aff'd*, 172 F. 3d 861 (3d Cir. 1998), was whether a university computer technician "intercepted" an e-mail message from the president of the institution when he saw the text of the message on a computer screen.[5] No, ruled the court: "the computer screen [is] just the medium for the information, not an intermediary employed by [the defendant] to receive the information. ... Congress had in mind more surreptitious threats to privacy than simply looking over one's shoulder at a computer screen when it passed the ECPA." 974 F. Supp. at 384.

For good treatments of the ECPA, *see* Lucien Capone III, *Landmines in the Information Highway: Academic Computing and the Law*, a presentation at the National Association of College and University Attorneys' 40th Annual Conference, June 25-28, 2000; *Electronic Communications Privacy Act*, www.digitalcentury.-com/encyclo/update/ecpa.html.

D. The Nascent Effort to Protect Digital Privacy by Federal Regulation

(1) The first and most comprehensive efforts to establish a legislative right of privacy were European. In Europe, legislation defines privacy as a fundamental civil right and protects citizens from unauthorized uses of electronic data. In 1995, the Council of

[5] The factual backdrop – *why* the employee happened to read the e-mail message – is too complex to do justice to in this outline. Trial Judge Murray Schwartz's lengthy opinion reads like a whodunit, and tells the tangled tale of a computer technician who allegedly tried to save his job by claiming that he "knew things" that could cause difficulties for the college in an unrelated lawsuit brought by an unsuccessful candidate for tenure. If one ever needed an object lesson in the perils of e-mail practice, the *Wesley College* decision provides it. The decision is a juicy read.

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 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." Fred H. Cate, PRIVACY IN THE INFORMATION AGE 48 (1997). 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 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 record-keeping practices of federal departments and agencies and does not reach any of the private-sector marketing or surveillance practices mentioned on pages 5 and 6 of this paper. American privacy activists often invoke the more protective European model as a goal worth striving for, and there are some indications that the federal government may be willing to play a more active role in the protection of privacy rights in the future.

Recently, in response to persistent advocacy by privacy groups, the U.S. 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.[6] 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,"

[6] The reports are compiled on the FTC's Web page at www.ftc.gov/reports/privacy/privacy1.htm.

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."[7]

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.[8] 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.[9]

In 1998, shortly after the FTC issued its report on electronic privacy, many of the same companies that organized TRUSTe met in Washington to establish a lobbying organization to press the case for self-regulation. The Online Privacy Alliance, as the organization was christened, has become a major force in jawboning companies to post codified privacy policies on their Websites and to "foster consumer confidence

---

[7] A key provision in the EU Directive prohibits any company doing business in an EU country – which of course includes virtually every company of any size in the United States – from transmitting personal data to any country that does not guarantee "an adequate level of protection" for such data. EU Directive, Art. 25, Sec. 1. (The full text of the Directive is reproduced as an appendix in the Cate book.) Two years ago the EU informed the United States that this country does not have adequate safeguards for personal data, raising at least the possibility that transatlantic commerce could be disrupted by an EU prohibition on data transmissions by multinational companies from Europe to the U.S. *See* "European Law Aims to Protect Privacy of Personal Data," *New York Times on the Web*, October 26, 1998 (www.nytimes.com/-library/tech/98/10/biztech/articles/26privacy.html).

[8] For information on TRUSTe, see www.truste.org; on the Better Business Bureau program, see www.bbbonline.org.

[9] According to a recent 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 Significant Progress in Privacy Self-Regulation, May 12, 1999 (www.privacyalliance.com/-news/05121999.shtml). For a typical privacy policy, see the one on the L.L. Bean Web page (www.llbean.com/customerservice/privacy/index.html).

by protecting personal privacy in cyberspace."[10] Notwithstanding the well publicized work of the Online Privacy Alliance and member companies, privacy advocates remain skeptical that self-regulation will work: "Poll after poll shows that people want legislation, not fine print, to protect privacy on the Internet," said Marc Rotenberg, a well-known privacy advocate, in testimony before the House of Representatives two years ago. "Testimony on the European Union Data Directive and Privacy before the Committee on International Relations, U.S. House of Representatives," May 7, 1998, www.epic.org/privacy/intl/-rotenberg-eu-testimony-598.html.

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. Cornell University's Computer Policy and Law Program has done a significant public service by collecting policies from several hundred institutions and placing them on a Website (www.cornell.edu/CPL/policies).

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 we want to preserve the individual's privacy. Electronic and other technological methods must not be used to infringe upon privacy. However, users must recognize that Georgia Tech computer systems and networks are public and subject to the Georgia Open Records Act. Users, thus, utilize such systems at their own risk.

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 (a) the user has voluntarily made them accessible to the public, as by posting to Usenet or a web page; (b) 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; (c) there is reasonable cause to believe that the user has violated, or is violating, this policy; (d) an account appears to be engaged in

[10] See "Privacy Initiatives by the Private Sector," at www.privacyalliance.org/resources/privinit.shtml.

> unusual or unusually excessive activity; as indicated by the monitoring of general activity and usage patterns; or (e) it is otherwise required or permitted by law.

> I did my own survey of the Web home pages of the universities on the list of U.S. News & World Report's top 25 national research universities. Not a single one of them includes a link to the institution's privacy policy on its home page, and virtually none of them appears even to have an institutional privacy policy establishing standards for the storage and use of information on members of the university community. Very few institutional policies prohibit campus authorities from using "cookies" or other technologies to monitor computer utilization for research or internal administrative purposes, an omission that some privacy proponents regard as indefensible.[11]

Conclusions

Like cyberspace itself, this presentation bombards the reader with hyperlinks as it jumps from one datum and one concept to another. Let's take a beat. What can we conclude?

First, lawyers would conclude that 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. Privacy rights are fragile and in retreat.

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

Third, in today's digital world, privacy is threatened as never before. 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.

Fourth and paradoxically – many of us don't care. Privacy protection on campus, never rock-solid to begin with, is more perilous than ever because rapid advances in threatening technologies have not yet galvanized courts and legislators to develop new standards and new theories for the protection of fundamental privacy rights. But, in an odd way, we exalt other

---

[11] *Use of "Cookies" in Research Sparks a Debate Over Privacy*, CHRON. OF HIGHER ED., September 25, 1998, page A31. *See also Colleges Get Free Web Pages, but With a Catch: Advertising*, CHRON. OF HIGHER ED., September 3, 1999, page A45 (reporting that some commercial "portals" that provide Web home pages to colleges at no charge are surreptitiously using cookies and other technologies to monitor the surfing habits of students).

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. Our own sense of privacy may have eroded; we willingly trade in our privacy to take advantage of the economies of the computer age. We view the loss of privacy, in some perverse way, as the cost of efficiencies associated with computerization. Professor Alan Westin, one of the great figures in the intellectual development of privacy law in this country, told the New York Times that 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.[12] To be truthful, there is no constituency on college campuses clamoring for the inclusion of privacy protections in computer policies. Most of us are dimly aware that our movements across the World Wide Web may be tracked for reasons that aren't clearly explained to us, but for the time being at least many of us don't seem to care.

[12] Katie Hafner, *Do You Know Who's Watching You? Do You Care?*, New York Times on the Web, November 11, 1999 (http://www.nytimes.com/library/tech/99/11/circuits/articles/11priv.html).