Washington Law Review

Volume 63 | Number 4

10-1-1988

Privacy Regulation of Computer-Assisted Testing and Instruction

Charles R. Tremper

Mark A. Small

PRIVACY REGULATION OF COMPUTER-ASSISTED TESTING AND INSTRUCTION

Charles R. Tremper*
& Mark A. Small**

I. INTRODUCTION

• Seated in a second grade classroom, Jason begins to read the story shown on his microcomputer screen. As he reads, he occasionally points to words on the screen, thereby requesting the computer to pronounce them. Jason selects some of the words because they are unfamiliar; others he chooses because he is entertained by the sound of the computer's voice. Whatever the reason for Jason's choice, the computer compiles a record of each word he selects. This record is stored initially in a temporary file the computer uses to customize the lesson it will present to Jason. At the end of the day, the classroom computer uses this information to update Jason's permanent record in the school's central computer.

• Brenda arrives for an interview at a large employment agency. As she is seated, a man informs her that the interview will be conducted by computer. He further explains that sensors connecting her to the computer will monitor her physiological reactions as she answers the questions. The interview begins with the computer presenting a series of questions about previous work experience, which Brenda easily answers using a keyboard. The computer then poses a series of questions that are less directly related to employment qualifications, including one asking about employee drug testing. Brenda, whose brother died of an overdose, interprets the question as inquiring into her attitude toward experimenting with drugs. Becoming anxious, she answers that she objects "very strongly" to employee drug testing. At the end of the session, the computer analyzes all data gathered during the interview and constructs a personality profile. Among other things, the profile characterizes Brenda as a probable drug user.

As the above examples illustrate, using computers to assist in testing and instruction creates privacy concerns that were absent or less consequential prior to the computer age. Not only does computer-assisted

* Assistant Professor of Law and Psychology, University of Nebraska; B.A. 1978, J.D. 1981, Ph.D. Education Policy 1983, University of California, Los Angeles. The authors thank Don Bersoff and Paul Hofer for providing the impetus to write this article and Steve Willborn and Rob Denicola for their helpful comments.

** B.A. 1983, M.A. Psychology 1985, University of Nevada, Las Vegas.

testing and instruction (CATI)[1] threaten to invade privacy insidiously,[2] its use with young schoolchildren poses the additional threat of arresting development of their privacy expectations.[3] In light of the significance of "reasonable expectations of privacy" in constitutional[4] and tort[5] law, as well as privacy's role in resisting totalitarianism,[6] widespread and routine use of CATI may profoundly alter the balance between public and private realms.

---

1. Computer-assisted testing and instruction techniques are discussed in COMPUTERS IN EARLY CHILDHOOD EDUCATION (J. Hoot ed. 1986); N. EVANS, THE FUTURE OF THE MICROCOMPUTER IN SCHOOLS (1986); G. KLEIMAN, BRAVE NEW SCHOOLS: HOW COMPUTERS CAN CHANGE EDUCATION (1984); S. PAPERT, MINDSTORMS (1980); YOUNG CHILDREN AND MICROCOMPUTERS (P. Campbell & G. Fein ed. 1986); and *Tests Can't Solve Every Problem,* U.S. NEWS & WORLD REP., May 19, 1984, at 84.

The prototypical CATI applications envisioned in this article use programming techniques that vary the stimuli they provide based on responses from the person interacting with them. Such sophisticated applications make use of artificial intelligence procedures and other techniques that require more computer processing power than currently available in the schools. *See* J. CHAMBERS & J. SPRECHER, COMPUTER-ASSISTED INSTRUCTION 114–18 (1983); S. POGROW, EDUCATION IN THE COMPUTER AGE 26 (1983). Thus, the discussion here concerns not the rudimentary computer-assisted methods in use today, but the forthcoming computer applications that have been imagined by the authorities cited in this note.

2. *See infra* notes 30–78 and accompanying text.

3. *See infra* notes 33–39 and accompanying text. In a seminal study on the topic, Richard Diem examined how 8 and 12-year-old students regarded the computerized work-products of other students at a computer day camp. Diem, *A Study of Children's Attitudes and Reactions to the New Technology,* 49 SOC. EDUC. 318 (1985). According to Diem, "[a]t no time during the camp sessions did any student question his or her right to look at another's information. It was as though all information were open and accessible to anyone who wished to view it." *Id.* at 319. Although no general conclusions can be drawn from this single instance, the finding suggests a need to assist young children in developing an appropriate regard for privacy. Pervasive CATI in elementary school may undermine that process.

4. Since the Supreme Court's decision in Katz v. United States, 389 U.S. 347 (1967), reasonable expectations of privacy, to which subjective expectations contribute, have been critical to defining the scope of the fourth amendment's protection against unreasonable searches and seizures. *See* California v. Ciraolo, 476 U.S. 207, 211–12 (1986) (aerial surveillance); Smith v. Maryland, 442 U.S. 735, 751 (1979) (pen registers) (Marshall, J., dissenting); United States v. Miller, 425 U.S. 435, 442 (1976) (bank records); Ashdown, *The Fourth Amendment and the "Legitimate Expectation of Privacy,"* 34 VAND. L. REV. 1289 (1981); Levin & Askin, *Privacy in the Courts: Law and Social Reality,* J. SOC. ISSUES, Fall 1977, at 138, 140–42; Wilkins, *Defining the "Reasonable Expectation of Privacy": An Emerging Tripartite Analysis,* 40 VAND. L. REV. 1077 (1987).

5. *See* PROSSER AND KEETON ON THE LAW OF TORTS § 117 (W. Keeton 5th ed. 1984). For examples of how reasonable expectations of privacy affect the outcome in intrusion cases, see Phillips v. Smalley Maintenance Servs., 435 So. 2d 705, 711 (Ala. 1983); Lewis v. Dayton Hudson Corp., 128 Mich. App. 165, 339 N.W.2d 857 (1983); and Jeffers v. City of Seattle, 23 Wash. App. 301, 315–16, 597 P.2d 899, 907 (1979).

6. Numerous authors have commented that individual privacy impedes totalitarian rule. *See* A. MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS 38–46 (1971); B. MOORE, PRIVACY: STUDIES IN SOCIAL AND CULTURAL HISTORY 74–75 (1984); J. RULE, PRIVATE LIVES AND PUBLIC SURVEILLANCE 338–43 (1973); Bazelon, *Probing Privacy,* 12 GONZ. L. REV. 587, 592–93 (1977).

Measured against the capacities of CATI technologies for invading students' and test-takers' privacy, the governing law is becoming ever less adequate. Current regulation consists of a fragmentary set of principles and provisions that apply rather obliquely to CATI.[7] Virtually all of these rules were formulated without reference to CATI and are not proving flexible enough to keep pace with advancing technology. Even some of the rules created within this decade are predicated upon visions of the future that largely failed to imagine the sociological changes brought about by widespread microcomputer use.[8]

To act upon the recognition that "personal privacy can no longer exist by yesterday's standards alone,"[9] we must undertake a critical analysis of the privacy issues inherent in CATI and update the regulatory structure accordingly.[10] To further these essential tasks, this article examines the privacy implications of CATI,[11] assesses the adequacy of current law,[12] and recommends strategies for achieving a satisfactory balance between the benefits of CATI and the loss of privacy it may entail.[13]

7. *See infra* notes 88–97 and accompanying text.

8. Observers commenting just eight to ten years ago did not envision the proliferation of microcomputers in offices, schools, and homes. The number of individuals interacting with computers greatly exceeds what the trend-line predicted absent the advent of the "personal" computer. For relatively recent predictions that missed the significance of the microcomputer, see Andersen & Rasmussen, *Sociological Implications of Computer Systems,* in HUMAN INTERACTION WITH COMPUTERS 97 (H. Smith & T. Green ed. 1980); Noll, *Regulation and Computer Services,* in THE COMPUTER AGE: A TWENTY-YEAR VIEW 254 (M. Dertouzos & J. Moses ed. 1979); and Westin, *The Long-Term Implications of Computers for Privacy and the Protection of Public Order,* in COMPUTERS AND PRIVACY IN THE NEXT DECADE 167 (L. Hoffman ed. 1980).

9. Linowes, *Must Personal Privacy Die in the Computer Age?,* 65 A.B.A.J. 1180, 1184 (1979).

10. Because the technologies Jason and Brenda are pictured using in the introductory vignettes have not yet become commonplace, action can be taken prospectively rather than remedially as is often the case. In the 20 years or more since concerns began appearing in the legal literature about high technology's potential for privacy invasion, an adequate legal response has yet to develop. For the flavor of the early literature, see Michael, *Speculations on the Relation of the Computer to Individual Freedom and the Right to Privacy,* 33 GEO. WASH. L. REV. 270 (1964) (predicting that the dazzle of computerization might blind society to its dangers); and Note, *Anthropotelemetry: Dr. Schwitzgebel's Machine,* 80 HARV. L. REV. 403 (1966) (warning that computer technology used to monitor humans' whereabouts would blur the distinction between liberty and confinement).

11. *See infra* notes 30–78 and accompanying text.

12. *See infra* notes 79–140 and accompanying text.

13. *See infra* notes 141–177 and accompanying text.

II. PRIVACY ISSUES IN CATI

Philosophers and social scientists have given considerable attention to the importance of privacy for human well-being.[14] Privacy has been described as "an instrument for achieving individual goals of self-realization"[15] and as necessary to "define the limits and boundaries of the self."[16] It has been credited further with enabling people to cope with the pressures of everyday life,[17] permitting emotional release and self-evaluation,[18] and providing people with an essential sanctuary in which to develop their identities.[19] Using similar language that the Supreme Court has quoted, Charles Fried has characterized Jeffrey Reiman's conception of privacy as embodying "the moral fact that a person belongs to himself and not to others nor to society as a whole."[20]

In analyzing the multidimensional nature of the apparent human need for privacy,[21] many writers have identified control over personal information and access to the self as the most important dimensions.[22] Some have argued that loss of control over personal information

14. For a representative sample of recent commentary, in addition to the works cited infra notes 15–19, see B. Moore, supra note 6; PRIVACY: A VANISHING VALUE? (W. Bier ed. 1980); PRIVACY (J. Young ed. 1978); PRIVACY (J. Pennock & J. Chapman ed. 1971); C. SCHNEIDER, SHAME, EXPOSURE AND PRIVACY (1977); D. SEIPP, THE RIGHT TO PRIVACY IN AMERICAN HISTORY (1981); P. WEISS, PRIVACY (1983); *Privacy as a Behavioral Phenomenon*, 33 J. SOC. ISSUES 1 (1977); PRIVACY, 31 LAW & CONTEMP. PROBS. 251 (1966); *The Law and Economics of Privacy*, 9 J. LEGAL STUD. 621 (1980); Fischer, *Privacy as a Profile of Authentic Consciousness*, 11 HUMANITIES 27 (1975); McCloskey, *Privacy and the Right to Privacy*, 55 PHIL. 17 (1980); Parent, *Recent Work on the Concept of Privacy*, 20 AM. PHIL. Q. 341 (1983); Rachels, *Why Privacy Is Important*, 4 PHIL. & PUB. AFF. 323 (1975); Schwartz, *The Social Psychology of Privacy*, 73 AM. J. SOC. 741 (1968).

15. A. WESTIN, PRIVACY AND FREEDOM 39 (1967).

16. I. ALTMAN, THE ENVIRONMENT AND SOCIAL BEHAVIOR 50 (1975).

17. Jourard, *Some Psychological Aspects of Privacy*, 31 LAW & CONTEMP. PROBS. 307, 310 (1966).

18. Ingham, *Privacy and Psychology*, in PRIVACY 35, 45–46 (J. Young ed. 1978).

19. Laufer & Wolfe, *Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory*, 33 J. SOC. ISSUES 22, 26–28 (1977).

20. American College of Obstetricians v. Thornburgh, 476 U.S. 747, 777 n.5 (1986) (Stevens, J., concurring); Fried, *Letter*, 6 PHIL. & PUB. AFF. 288, 288 (1977).

21. Not everyone agrees that privacy is conceptualized best as a basic human need. *See, e.g.*, Epstein, *A Taste for Privacy? Evolution and the Emergence of a Naturalistic Ethic*, 9 J. LEGAL STUD. 665 (1980) (privacy is an individual taste without a biological basis); Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 394 (1978) (privacy is an intermediate good). A compromise view of sorts is that privacy is a socially created need, albeit one that appears to be universal. B. MOORE, *supra* note 6, at 73–74, 274; Altman, *Privacy Regulation: Culturally Universal or Culturally Specific*, J. SOC. ISSUES, Summer 1977, at 66.

22. A. MILLER, *supra* note 6, at 25; Beaney, *The Right to Privacy and American Law*, 31 LAW & CONTEMP. PROBS. 253, 265 (1966); Fried, *Privacy*, 77 YALE L.J. 475, 493 (1968). Westin defines privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." A.

imperils mental health because sense of self-worth largely depends upon the perceptions of others.[23] Other writers have noted that being able to control access to the self is critical to feelings of well-being and efficaciousness.[24]

As useful as these various ruminations may be for understanding the functions and importance of privacy, little of what has been written is specifically applicable to CATI. Even forward-looking discussions of privacy in the computer age generally have not dealt with the range of privacy issues involved in CATI.[25] With few exceptions, these analyses have pictured the computer as an enormous, efficiently-indexed filing cabinet filled with electronic facsimiles of pre-existing paper records.[26]

Although this filing cabinet model fits many computer applications and has served as a good starting point for privacy regulation,[27] in several ways it is inadequate for CATI. First, the filing cabinet model does not account for user interaction. Under the filing cabinet model, the computer receives all its data from records made independently of the computerized process. In CATI, a test-taker or learner sitting at a computer terminal generates his or her own computer records during testing and instruction. By bypassing the third party input stage that is a hallmark of the filing cabinet model, CATI creates new opportunities for privacy invasion.

Second, the very nature of testing and instruction compounds the privacy invasiveness of interactive computer use. The main purpose of most testing is to find out about a test-taker's capabilities, potentially

---

WESTIN, *supra* note 15, at 7. This definition captures the information control aspect particularly well.

23. I. BERLIN, FOUR ESSAYS ON LIBERTY 156 (1969) ("the only persons who can so recognize me, and thereby give me the sense of being someone, are the members of society to which historically, morally, economically, and perhaps ethnically, I feel that I belong"); E. GOFFMAN, RELATIONS IN PUBLIC (1971); Gross, *Privacy and Autonomy,* in PRIVACY 169, 172–73 (J. Pennock & J. Chapman ed. 1971); Huff, *Thinking Clearly About Privacy,* 55 WASH. L. REV. 777, 779–81 (1980).

24. Jourard, *supra* note 17, at 310; Shils, *Privacy: Its Constitution and Vicissitudes,* 31 LAW & CONTEMP. PROBS. 281, 286 (1966).

25. *See, e.g.,* Freedman, *The Right of Privacy in the Age of Computer Data and Processing,* 13 TEX. TECH L. REV. 1361 (1982) (focusing exclusively on mainframe computer records); Soma & Wehmhoefer, *A Legal and Technical Assessment of the Effect of Computers on Privacy,* 60 DEN. L.J. 449, 452–54 (1983) (CATI is not listed among the seven major areas of computer technology predicted to affect privacy).

26. *See generally* Noll, *supra* note 8, at 265 (critiquing filing cabinet model by showing that proposals to regulate computer services industry to protect privacy interests have been rendered obsolete by data sharing among services).

27. *See generally* S. MANDELL, COMPUTERS, DATA PROCESSING, AND THE LAW 172 (1984) (using the filing cabinet paradigm).

revealing information the test-taker would prefer not to divulge.[28] In the elementary and secondary school classroom, the educational mission includes shaping students' values, manners and self-concepts, as well as teaching them facts and skills.[29] Finally, in both testing and instruction, computer techniques exponentially increase the quantity of information that teachers and psychometricians can collect and analyze.

For analysis in this article, the various privacy threats CATI poses are organized into three categories: Computerized information gathering, management of the information collected, and misperceptions resulting from interpretation of that information. Each category is discussed below in the same order as it occurs in the CATI process.

A. Computerized Information Gathering During Testing and Instruction

An initial privacy invasion may occur any time personal information is collected. Depending on the technique used and the information sought, information gathering practices differ in invasiveness. From simple questioning to surreptitious observation and involuntary extraction of information by physical or psychological means, the degree of invasiveness rises and the ability of individuals to withhold information and thereby protect their privacy diminishes.

As the introductory vignettes suggest, computers can be used in several ways during testing and instruction to penetrate an individual's normal defenses against revealing personal information.[30] In so doing, CATI imperils what Oscar Ruebhausen and Orville Brim identify as the very essence of individual privacy: "[T]he freedom of the individual to pick and choose for himself the time and circumstances under which, and most importantly, the extent to which, his attitudes, beliefs, behavior and opinions are to be shared with or withheld from

28. For discussions of the need in indirect psychological testing to deceive test-takers about the design and perhaps the purpose of the test, see Anastasi, *Psychological Testing and Privacy,* in PRIVACY: A VANISHING VALUE? 348, 350–51 (W. Bier ed. 1980); and Wolf, *Invasion of Privacy,* in CRUCIAL ISSUES IN TESTING 159, 163 (R. Tyler & R. Wolf ed. 1974).

29. The "whole child" approach in American education has led teachers and counselors to involve themselves in students' socioemotional and moral as well as cognitive development. *See generally* S. SARASON, THE CULTURE OF THE SCHOOL AND THE PROBLEM OF CHANGE 203–06 (1971); P. SCHARF, MORAL EDUCATION 109–36 (1978).

30. Certain uses of computers in testing and education constitute what Westin terms "psychological surveillance," which he defines as "scientific and technological methods that seek to extract information from an individual which he does not want to reveal or does not know he is revealing or is led to reveal without a mature awareness of its significance for his privacy." A. WESTIN, *supra* note 15, at 133.

others."[31] The prospect of circumventing normal psychological defenses to probe into an individual's "core self" is the most damaging variety of privacy invasion.[32]

As the process of testing and instruction progresses from marking on paper to tapping on a keyboard, individuals, particularly schoolchildren, may lose much of their ability to conceal information about themselves from observation and collection by others.[33] In the paper and pencil era, students could write a few choice epithets about the school without revealing their contempt to anyone. They could also make innumerable mistakes without fear of reproach. Their counterparts composing at keyboards, whose every keystroke may be observed, recorded, and reviewed, will not have the same freedom.[34]

More intrusive privacy invasions occur when computers are combined with other devices to monitor a test-taker's or learner's previously undetectable biological processes. Microelectronic biomedical devices developed for monitoring such special populations as prisoners, astronauts, and psychiatric patients can be adapted for testing and instruction of the general population.[35] Sophisticated sensors will be able to monitor not only a person's visible activities, but also internal biochemical changes or other unobservable phenomena.[36] At present,

31. Ruebhausen & Brim, *Privacy and Behavioral Research,* 65 COLUM. L. REV. 1184, 1189 (1965).

32. *See* A. WESTIN, *supra* note 15, at 42; Benn, *Privacy, Freedom, and Respect for Persons,* in PRIVACY 1, 7–9 (J. Pennock & J. Chapman ed. 1971).

33. Children may begin using computers even before they can read and write. *See* Hughes & Macleod, *Using Logo with Very Young Children,* in COGNITION AND COMPUTERS 179 (1986). Whether young children doodle with a light pen or use some other input device to respond to images presented on the computer screen, the computer can record and analyze their interactions.

34. Although students' myriad keystrokes would exceed a teacher's ability to review exhaustively, the computer will perform much of the necessary analysis. Not only can the computer be programmed to detect errors, it can also be instructed to alert the teacher if students have entered profane or sexually oriented words, including slang and misspellings! With such assistance teachers will be able to focus their attention more pointedly on the portion of student work that interests them.

35. *See generally* Meindl, *Biomedical Implantable Microelectronics,* 210 SCI. 263 (1980) (noting that innovative applications of microchips in implantable biomedical sensors will improve health care); Weingarten, *Privacy: A Terminal Idea,* HUM. RTS., Fall 1982, at 18, 21 (discussing privacy implications of subcutaneous monitoring and transmitting devices).

36. For example, a sophisticated intelligence test might measure the delay between presentation of a computer-generated stimulus and a test-taker's response and use that measurement as an indicator of information processing speed. For an account of an experiment using such an approach, see Small, Raney & Knapp, *Complex Reaction Time and General Intelligence: A Refinement,* 148 J. GENETIC PSYCHOLOGY 405 (1987). Regarding the relationship between speed of information processing and intelligence, see Jensen, *Chronometric Analysis of Intelligence,* 3 J. SOC. & BIOLOGICAL STRUCTURE 103 (1980).

we can only guess at how successful these techniques will be for generating inferences about the psychological make-up of the subject.[37]

The incessant computerized collection and storage of such data could make CATI much more privacy invasive than conventional testing and instruction. Privacy has long survived in part because we have lacked the ability to intrude as deeply into each other's affairs as we might[38] if we had the necessary means. In the traditional classroom, a teacher who wonders whether young Jessica is performing poorly because she is emotionally distressed may observe only how Jessica appears and acts. If she wishes, Jessica can use a variety of techniques to mask her true feelings and prevent the teacher from discovering what she does not wish to reveal. If a computer is constantly monitoring Jessica's physiology, the teacher can use the resulting data to circumvent Jessica's conventional privacy screens.

Although the advent of such capabilities may be regarded as merely an extension of what teachers and testers have always done, the new technology radically transforms the nature of observation by making it impersonal, invariable, and much more difficult, if not impossible, for the monitored person to influence voluntarily.[39]

B. Inappropriate Management of Personal Information

Once information has been recorded during CATI, the privacy threat shifts from data collection to data management. Release of previously collected personal information further erodes individuals' power to shape their public image. Loss of control over personal information, even if it is not subsequently released to others, reinforces the impression that individuals are powerless to set themselves apart from society.

The predominant concern expressed in the literature and recognized at law regarding release of computerized records has been disclosure to individuals with no legitimate interest in the information.[40] In the CATI context, this concern is joined by two others that rarely arise in other contexts. One is privacy invasive disclosure to the record-subject. An instructional or testing computer may confront people with

37. The vignette with Brenda in the introduction to this article illustrates one potential pitfall.

38. *See* A. WESTIN, *supra* note 15, at 19–22.

39. *See* Anastaplo, *The Public Interest in Privacy: On Becoming and Being Human*, 26 DE PAUL L. REV. 767, 785 (1977).

40. A. MILLER, *supra* note 6, at 26; Trubow, *Information Law Overview*, 18 J. MARSHALL L. REV. 815, 819–20 (1985).

information about themselves that would cause distress.[41] The other is that the extremely sensitive nature of some information a computer may obtain during direct interaction with a record-subject may be inappropriate for release to teachers, employers, and parents, who traditionally have been considered to have a legitimate interest in and right of access to the information.[42] Record-subjects may lose a greater measure of privacy if matters they wish most to hide are revealed to a single person than if some piece of information already known by another person is exposed to a wider audience.

A related problem is the use of a record for a purpose different from the one for which it was created.[43] As with release to unknown parties, inappropriate use decreases record-subjects' ability to shape their public image. Computers increase the likelihood of inappropriate use by isolating information from the context in which it was gathered.[44]

41. Although such revelations may occur in the course of human interactions, the CATI analog differs in two respects. These can be seen clearly in the context of psychotherapy. First, the revelation by a computer need not be mediated by the discretion of a human being familiar with the full dynamics of the situation, i.e., the computer may inform the subject of the revelation indiscriminately. In the absence of a human interface, the mystique of the computer may incline subjects to rely unduly on the assessment. The observations of a fellow, fallible, human may be more easily dismissed.

Second, a psychotherapist's conclusions about a client's unrecognized psychological attributes need not be embodied in a "record." Consequently, information privacy laws granting a legally enforceable right to discover "records" would not apply. On the other hand, such laws typically apply to all entries on a computer's storage medium, and would permit clients to discover the computer-generated inferences about their character. *See, e.g.*, Privacy Act of 1974, 5 U.S.C. § 552a (1982 & Supp. 1986). The mental processes of the psychotherapist, including memories of what the client has said and any inference the psychologist makes, simply are not records in the sense that data in a computer are.

42. Parties permitted access under the Family Educational Rights and Privacy Act of 1974 ("FERPA") are discussed in Cudlipp, *The Family Educational Rights and Privacy Act Two Years Later*, 11 U. RICH. L. REV. 33 (1976); and Schatken, *Student Records at Institutions of Postsecondary Education: Selected Issues Under the Family Educational Rights and Privacy Act of 1974*, 4 J. C. & U.L. 147, 169–74 (1977).

Because most schoolchildren are minors, school counselors face difficult ethical and practical issues in deciding whether to inform parents or school administrators about information gained during counseling sessions. *See* Clarizio, *School Psychologists and the Mental Health Needs of Students*, in SCHOOL PSYCHOLOGY: PERSPECTIVES AND ISSUES 309 (G. Phye & D. Reschly ed. 1979); Wagner, *Confidentiality and the School Counselor*, 59 PERSONNEL & GUIDANCE J. 305 (1981).

43. *See* U.S. CONGRESS, OFFICE OF TECHNOLOGY ASSESSMENT, FEDERAL GOVERNMENT INFORMATION TECHNOLOGY: ELECTRONIC RECORD SYSTEMS AND INDIVIDUAL PRIVACY 37–38 (1986); Corell, *Technological Development and Its Consequences for Data Protection*, COUNCIL OF EUROPE, Proceedings of the 14th Colloquy on European Law 42, 49 (1985); Shattuck, *In the Shadow of 1984: National Identification Systems, Computer-Matching, and Privacy in the United States*, 35 HASTINGS L.J. 991 (1984).

44. P. SIEGHART, PRIVACY AND COMPUTERS 68 (1976); Wheeler, *Problems and Issues in Record-Keeping*, in ON RECORD: FILES AND DOSSIERS IN AMERICAN LIFE 3 (S. Wheeler ed. 1969).

Computerized relational databases permit an educator to search records more efficiently and to use special search strategies that may identify students who would not have been noticed if conventional methods had been used. For example, school records containing socioeconomic data supplied for civil rights compliance might be combined with various test scores and patterns of daily computer use in an attempt to estimate the likelihood that youngsters will become juvenile delinquents.[45] Although such efforts have been undertaken without CATI, the availability of computerized records greatly reduces the requisite effort and thereby makes it more likely that the analysis will be conducted.[46]

Computers also exacerbate the problem of information release because human judgment need not be exercised to effect release. In the past, a teacher had to make a conscious decision about forwarding an assessment of any sort to the schoool records office (a decision that will be influenced by a host of variables other than the simple determination of whether the assessment is correct).[47] The direct-monitoring computer, however, may automatically transmit its records to a central registry.[48] The farther records travel from their original source and the greater the number of copies in existence, the less ability the record-subject has to supervise use of the information or even to know who has access to it.

In addition, parties with no legitimate interest may gain acess to CATI data. While this problem is hardly novel, the nature of CATI

45. Using existing education, health, and justice system records, Norway already has attempted to do this. Bing, *Data Protection and Social Policy,* COUNCIL OF EUROPE, Proceedings of the 14th Colloquy on European Law 82, 91 (1985).

46. The legal implications of computers' increased capacity *per se* are murky. Justice Brennan, who may be the member of the current Supreme Court most concerned with privacy issues, has written, "collection and storage of data by the State that is in itself legitimate is not rendered unconstitutional simply because new technology makes the State's operations more efficient." Whalen v. Roe, 429 U.S. 589, 606–07 (1977) (concurring opinion).

47. *See generally* Groves, *Professional Discretion and Personal Liability of Teachers in Relation to Grades and Records,* 101 EDUC. 335 (1981) (explaining factors influencing decisions to forward grades and reports).

In some instances, e.g., processing of standardized intelligence tests, the action of the teacher and computer would be nearly identical in forwarding the results to an "outside" source. The difference with the computer lies in the potential to drastically increase the volume of routine transmission of information.

48. *See* N. EVANS, *supra* note 1, at 142–44. At some point in the process, humans must have instructed the computer in the general rules it uses in transferring information. A computer's implementation of these a priori decision rules is quite different from humans applying the same rules, however, because of the possibility that a human will not follow the rule in a particular case. The well-recognized difficulty of formulating rules of general application with sufficient sensitivity to account for diverse circumstances ensures that the computer will treat as alike cases which a human would distinguish.

adds new dimensions. As with other computerized information, the possibility of remote access is much greater than it is for paper records.[49]

The linking together of computers by dedicated wiring, telephone lines, microwaves, or other networking technology creates the possibility of someone gaining access to information without being present at the record's physical location. The greater danger in CATI, however, may be posed by on-site system users. Particularly in the classroom setting, databanks will be highly vulnerable to invasion by curious interlopers.[50] The apparent ease with which computer "hackers," including children, have gained access to "secure" systems[51] and the numerous instances of personal materials being released inappropriately[52] suggest the need for caution.

With the potential for obtaining and storing voluminous information about individuals, CATI also raises the specter that record-subjects will be known disturbingly well by parties with authorized access

49. *See* Levine, *Privacy in the Tradition of the Western World,* in PRIVACY: A VANISHING VALUE? 3, 16–17 (W. Bier ed. 1980); Salerno, *Catching Up with the Computer Revolution,* HARV. BUS. REV., Nov.-Dec. 1981, at 8, 16.

50. Students who have access to the system for input may also have a gateway to each other's records. Perhaps this threat to privacy is no greater than the prospect that students will gain access to paper records in their teacher's desk or the principal's office, but the contingency must at least be anticipated.

The findings of Diem's seminal examination of young students' computer use provides support for the assumption that abuse of some sort will occur. Diem found that "[t]he students also learned rather quickly how to abuse the informational systems at hand. A group of older boys, for example, managed to identify one of their colleague's data access codes, and used it to write a derogatory program that appeared when the young man returned to his machine." Diem, *supra* note 3, at 319.

51. Browne, *Locking Out the Hackers,* DISCOVER, Nov. 1983, at 30, 31; Korzeniowski, *All-Star Teen Hacker's Team Beats Hundreds of Systems,* COMPUTERWORLD, July 8, 1985, at 14; Shattuck, *supra* note 45, at 993–94.

52. Churchill & Baratz, *The Illusion of Privacy: Student Records in Los Angeles,* SOC. POL'Y, Mar.-Apr. 1978, at 38; Divoky, *Cumulative Records: Assault on Privacy,* LEARNING, Sept. 1973, at 18. Some of these instances have led to litigation. For example, in York v. Story, 324 F.2d 450 (9th Cir. 1963), *cert. denied,* 376 U.S. 939 (1964), plaintiff was awarded damages based on the actions of police officers gaining consent to take pictures of her in the nude ostensibly for use as evidence and then distributing the pictures among their friends. In Fadjo v. Coon, 633 F.2d 1172 (5th Cir. 1981), individuals who had provided the Florida Attorney General's Office with personal information upon a promise of confidentiality were entitled to damages when that information was disclosed without their consent.

Although the instances cited here do not concern computers, they confirm that no matter how potentially embarrassing or damaging an item may be, once it has passed beyond control of the subject, the possibility of release to others cannot be dismissed.

to the computer.[53] Individuals lose privacy if others know more about them than they would like them to have know, regardless of how well-intentioned the privacy invaders may be.

Because their records may be released to unknown parties or compiled to their disadvantage, people may choose to "base their decisions and fashion their behavior in terms of enhancing their record image in the eyes of those who may have access to it in the future."[54] At the time Arthur Miller described this insidious effect on behavior as "the real evil of a records prison,"[55] the record-keeping process he envisioned was limited to documenting a person's public, observable, performance and status. The potential impact on behavior becomes still more troubling when a computer is recording myriad keyboard interactions during daily classroom activities or monitoring physiolgoical processes that are not normally under the control of conscious choice.[56]

C. *Inaccurate Human Images Based on Computerized Testing and Instruction Records*

Thus far, the potential threats CATI poses to privacy have concerned the loss of a person's control over how information is gathered and managed. To a great extent, the harm associated with this loss of control stems from the prospect that the resulting record will give an inaccurate impression, either because the information is false or because it is taken out of context.[57] Becoming the subject of a computer record that indicates a below average reading speed during a

53. *See* A. NEIER, DOSSIER: THE SECRET FILES *They* KEEP ON *You* 18–20 (1975); Barron, *People, Not Computers,* in PRIVACY 319, 320 (J. Young ed. 1978); Solomon, *Personal Privacy and the "1984" Syndrome,* 7 W. NEW ENG. L. REV. 753, 759 (1985).

Based on far less information than can be obtained in CATI, advertisers already are constructing rudimentary psychographic profiles of consumers that combine such standard demographic variables as age, sex and income, with measures designed to represent potential customers' "dreams, hopes, fears, and beliefs." Townsend, *Psychographic Glitter and Gold,* AM. DEMOGRAPHICS, Nov. 1985, at 22, 23. The advertisers then use these profiles in targeting appeals to specific segments of the buying public. *See* Johnson, *Computer Technology Is Key to Segmentation and Service,* DIRECT MARKETING, June 1985, at 66, 68.

54. A. MILLER, *supra* note 6, at 50. Hubert Humphrey tapped the same vein with his observation that "[w]e act differently if we believe we are being observed. If we can never be sure whether or not we are being watched and listened to, all our actions will be altered and our very character will change." HUMPHREY, *Foreword* to E. LONG, THE INTRUDERS: THE INVASION OF PRIVACY BY GOVERNMENT AND INDUSTRY viii (1967).

55. A. MILLER, *supra* note 6, at 50.

56. *See supra* note 36 and accompanying text.

57. Simitis, *Reviewing Privacy in an Information Society,* 135 U. PA. L. REV. 707, 718 (1987) ("A second, no less important, consequence of automated processing is the loss of context."); Wheeler, *supra* note 44.

verbal skills test may cause distress; becoming the subject of a such a record incorrectly undoutedly magnifies the harm. Not only does it enable some other person to form an impression based on a characteristic that generally is not observable, hence private in at least one sense, it also makes it likely that the impression will be faulty.

Although records invariably are incomplete and reflect some observational bias,[58] the problems of omission and error are particularly acute for computers in general and CATI in particular. Personnel who review these computerized records are unlikely to recognize inaccuracies because they typically have neither personal acquaintance with the record-subject nor any other independent basis upon which to form an impression. The power of computers to abstract and manipulate data exacerbates the problem of inaccuracy by encouraging abstraction and quantification. Although narrative information is likely to give a more complete description of an individual, computers use quantitative and categorical data almost exclusively.

In addition to being wrong or incomplete, a person's record image may be distored if it contains outdated information. Arthur Miller has aptly noted that "a computerized file has a certain indelible quality—adversities cannot be overcome by the passage of time in the absence of an electronic eraser and a compassionate soul willing to use it."[59] The opportunity for a new beginning offered by institutional "systematic forgetting"[60] is a strong theme in American individualism and well respected at law.[61] As their storage capacities increase, computers become ever more capapble of retaining old assessments that

58. PRIVACY PROTECTION STUDY COMM'N, PERSONAL PRIVACY IN AN INFORMATION SOCIETY 3–6 (1977); *see also* U.S. CONGRESS, *supra* note 43, at 5 (noting that the accuracy of most Privacy Act record systems is unknown and the quality of the known systems varies widely); *cf.* Andersen & Rasmussen, *supra* note 8, at 108 (noting the computer's potential to bring more information to bear on bureaucratic decision-making).

59. A. MILLER, *supra* note 6, at 38. The same may be said of paper records. The critical difference is the far superior capacity of the computer to maintain huge numbers of records and provide access to them far into the future. Moreover, with large capacity computers, deleting information is more bothersome and expensive than retaining it. Sardinas, Blank & Spiro, *Data Processing: Towards a Social Responsibility,* J. SYS. MGMT., May 1986, at 14, 16. For paper records, the need for the physical space that files occupy provides an incentive for periodically discarding outdated material.

60. Rule, McAdam, Stearns & Uglow, *Preserving Individual Autonomy in an Information-Oriented Society,* in COMPUTERS AND PRIVACY IN THE NEXT DECADE 65, 75 (L. Hoffman ed. 1980).

61. One of the chief rationales for a separate juvenile justice system with closed proceedings is to give young offenders a chance to reform without being followed through life by a record of their youthful transgressions. *See* McKeiver v. Pennsylvania, 403 U.S. 528, 550 (1970) (avoiding public trials cited as rationale for denying jury trials to juvenile defendants); Larson, *Model Statute on Juvenile and Family Court Records,* JUV. & FAM. CT. J., Feb.-Mar. 1981, at 8, 12–13; Lister, *Privacy, Recordkeeping, and Juvenile Justice,* in PURSUING JUSTICE FOR THE CHILD 205,

may label an individual at a very early age and make change difficult.[62] Even if additional information is input, it will not necessarily be cross-referenced to previous entries.

As CATI technology improves, systems will increasingly use artificial intelligence[63] and expert systems techniques to detect some types of inaccuracy automaticallly. Far from solving accuracy problems, however, the advent of such systems will introduce extra sources of potential distortion, especially in their early years.

One problem is likely to be misplaced reliance on the conclusions resulting from expert systems analysis. An expert system is designed to replicate the analysis of a human expert by applying an inference algorithm to information it has been provided.[64] If the algorithm is faulty, erroneous records may be generated from accurate input. Although anyone who receives a printout from an expert system should be wary of possible error, the "black box" nature of the system may incline users to accept results derived from accurate input, the only element of the system they can verify.[65]

---

206 (M. Rosenheim ed. 1976); Sagatun & Edwards, *The Significance of Juvenile Records,* JUV. & FAM. CT. J., Feb. 1979, at 29, 34.

In some circumstances, adults too have been considered entitled to live their lives without being dogged by reminders of past misdeeds. *See* Melvin v. Reid, 297 P. 91, 93–94 (1931) (damages for privacy invasion awarded based on invasion of privacy resulting from movie about a former prostitute who had married and was living a respectable life) (superceded by statute). Franklin & Johnsen, *Expunging Criminal Records: Concealment and Dishonesty in an Open Society,* 9 HOFSTRA L. REV. 733 (1981); Volenick, *Juvenile Court and Arrest Records,* 9 CLEARINGHOUSE REV. 169, 172–73 (1975).

62. For discussions of the difficulty individuals face in overcoming preconceptions others form based on "labels" for their personal characteristics, see J. BROPHY & T. GOOD, TEACHER-STUDENT RELATIONSHIPS: CAUSES AND CONSEQUENCES 30–32 (1974); E. SCHUR, LABELING DEVIANT BEHAVIOR 38–52 (1971). Although the validity of labeling, or the "self-fulfilling prophesy," as originally understood has been cast into doubt, computerized records that provide the basis for educational placement or other treatment certainly may have a profound effect on the ease with which an individual may overcome an erroneous characterization. Wineburg, *The Self-Fulfillment of the Self-Fulfilling Prophesy,* 16 EDUC. RESEARCHER 28 (1987). *See generally* Barron, *People, Not Computers,* in PRIVACY 319 (J. Young ed. 1978); Coffee, *Privacy Versus Parens Patriae: The Role of Police Records in the Sentencing and Surveillance of Juveniles,* 57 CORNELL L. REV. 571, 591–94 (1972); Goslin & Bordier, *Record-Keeping in Elementary and Secondary Schools,* in ON RECORD: FILES AND DOSSIERS IN AMERICAN LIFE 29, 50–56 (S. Wheeler ed. 1969).

63. Artificial intelligence is the term for programming techniques that enable computers to imitate some aspect of human intelligence, especially deriving conclusions from propositions. *See* P. WINSTON, ARTIFICIAL INTELLIGENCE (1979). Regarding the use of artifical intelligence in computer assisted instruction, see J. CHAMBERS & J. SPRECHER, *supra* note 1, at 108–18.

64. *See generally* Myers, *Introduction to Expert Systems,* IEEE EXPERT, Spring 1986, at 100; Nau, *Expert Computer Systems,* COMPUTER, Feb. 1983, at 63.

65. This problem may be reduced, although not eliminated, by having the computer provide an explanation of its reasoning processes. *See* E. RICH, ARTIFICIAL INTELLIGENCE 201–42 (1983); D. WATERMAN, A GUIDE TO EXPERT SYSTEMS 90–91 (1986).

Given identical information, an error-free expert system likely will perform better than the average practitioner.[66] Therefore, reliance on the computer's assessment might appear sensible. Rarely, however, are human experts limited to the information available to the computer. In any testing or instruction setting, a human may be aware of circumstances that could affect interpretation of the data available to the computer.[67] Furthermore, an expert system may foster distortion by enabling untrained individuals to make decisions based on the apparently straightforward printouts without consulting a psychometrician or other appropriate specialist.[68]

Misguided use of advanced programmming techniques poses an additional threat to privacy that is virtually unique to classroom CATI. Computerized elementary school instruction that adjusts the instructional mode and perhaps even the content to match what the computer infers to be appropriate for the learner has ominous implications for shaping children's images of who they are. For example, a girl's frequent errors on verbally-based lessons may lead the computer to begin offering more visually-oriented materials and commend her for responding appropriately to pictures.[69] In the process, the girl's self-image may change from budding-novelist to artist. The negative implications of this scenario become apparent upon considering the uniformity that computers can bring to public education. Whereas the semi-autonomy of classroom teachers has heretofore precluded appreciable standardization, mass-produced instructional software packages that interact directly with students could achieve a high degree of uni-

66. *See* Myers, *supra* note 64.

67. For this reason, the authors of an article describing an emergency room expert system that diagnoses heart attacks more accurately than doctors were able to do, counseled against relying on the computer's diagnosis without following standard examination procedures as well. Goldman, Cook, Brand, Lee, Rouan, Weisberg, Acampora, Stasiulewicz, Walshon, Terranova, Gottlieb, Kobernick, Goldstein-Wayne, Copen, Daley, Brandt, Jones, Mellors & Jakubowski, *A Computer Protocol to Predict Myocardial Infarction in Emergency Department Patients with Chest Pain,* 318 NEW ENG. J. MED. 797 (1988).

68. The same problem has been observed regarding the output from medical expert systems. Gill, *Medical Expert Systems: Grappling with Issues of Liability,* 1 HIGH TECH. L.J. 483, 493 (1986).

69. Decisions about learning strategies "can all be made contingent upon a model or analysis of the learner's strengths and weaknesses in the domain being taught. Individual students, differing in their styles of learning or their rates of progress can be presented with different materials tailored to their personal skills and proclivities." Lepper & Milojkovic, *The "Computer Revolution" in Education: A Research Perspective,* in YOUNG CHILDREN AND MICROCOMPUTERS 11, 14 (P. Campbell & G. Fein ed. 1986).

formity.[70] This prospect imperils the individualism essential to meaningful privacy.[71]

These new threats to privacy, as well as the benefits that artificial intelligence-based systems will bring to the education process, will materialize slowly over the coming years as the necessary technology evolves. The complexity of most educational settings ensures that systems approaching human capabilities will not be available any time soon and that when systems do become available, they will perform only limited tasks of dubious validity until the experimental phase has passed. After adequate procedures do become available, the higher relative cost of state-of-the-art systems will prevent many institutions from abandoning their less expensive systems.[72]

Ultimately, the potential benefits of gathering as much information as possible from students in order to make the most of their instruction must be balanced against the impact on society of subjecting children to omnipresent surveillance by "teaching machines." Although we cannot know for certain how this process will affect children, research suggests that most young children lack the capacity to recognize and resist these privacy invasive practices and that the concepts of privacy children develop are strongly influenced by their experiences.[73] If children are subject to involuntary computer monitoring throughout their school days, their expectations of privacy in the future may be substantially reduced.

---

70. *Cf.* Steffin, *Fighting Against Convergent Thinking: Using the Micro as a Weapon,* 59 CHILDHOOD EDUC. 255 (1983) (arguing that the microcomputer promotes divergent thinking as well as allows for more privacy).

71. This discussion is not intended to dismiss the potential utility of computer-assisted instruction to produce numerous instructional benefits. Whereas those beneficial possibilities have been extolled elsewhere, the objective here is to draw attention to the less well recognized pitfalls of the enterprise so that the process can be implemented in a way that strikes an appropriate balance between the potential benefits and risks. *See* sources cited *supra* note 1. *See generally* Rule, McAdam, Stearns & Uglow, *supra* note 60, at 70 (discussing the difficulty of resisting computer technology's allure).

72. In Peninsula Counseling Center v. Rahm, 105 Wash. 2d 929, 719 P.2d 926 (1986), a majority of the Washington Supreme Court upheld the Washington Department of Social and Health Services' use of a computerized system that was somewhat more efficient but also more privacy invasive than a proposed alternative. *Id.* at 935–36, 719 P.2d at 929. Only Justices Pearson and Brachtenbach found the cost justification insufficient. *Id.* at 937–49, 719 P.2d at 930–36 (Pearson, J., dissenting).

73. Melton, *Minors and Privacy: Are Legal and Psychological Concepts Compatible?,* 62 NEB. L. REV. 455, 486–92 (1983); Wolfe & Laufer, *The Concept of Privacy in Childhood and Adolescence,* 6 MAN-ENV'T INTERACTIONS 29 (1974).

The dangers here are especially great because most youths under age sixteen are subject to compulsory education[74] and adults rarely acknowledge the legitimacy of children's privacy needs.[75] As recently as 1984, Justice Rehnquist, writing for a majority of the Supreme Court, echoed the traditional view of children as always being in "some form of custody."[76] The efficiency of school administration, on the other hand, appears to be highly valued on the Court[77] and in society.[78] Unless specific legislation prohibits the objectionable practice, the judiciary may regard CATI's efficiency as a sufficient benefit to offset the threat it poses to privacy.

III. CURRENT PRIVACY REGULATION OF CATI

Existing laws and legal principles pertaining to CATI create a patchwork of restrictions reflecting no consistent approach to protecting privacy. Thus, appraising the current status of CATI privacy regulation requires canvassing a wide range of legal sources. To lay the groundwork for the necessary analysis, this Part begins with an overview of the major sources of applicable constitutional, common, and statutory law. The remainder of the Part presents an analysis of how these rules bear on CATI information collection, management, and accuracy.

74. K. ALEXANDER & F. JORDAN, LEGAL ASPECTS OF EDUCATIONAL CHOICE: COMPULSORY ATTENDANCE AND STUDENT ASSIGNMENT 14–17 (1973).

75. *See* H. COHEN, EQUAL RIGHTS FOR CHILDREN 135 (1980); Melton, *supra* note 73, at 488 (privacy inconsistent with society's conception of children); Rosenberg, Schall v. Martin: *A Child is a Child is a Child,* 12 AM. J. CRIM. L. 253 (1984) (Supreme Court gives children's privacy interests little weight in fourth amendment analysis).

76. Schall v. Martin, 467 U.S. 253, 265 (1984). Twenty years earlier, the Court concluded that the Constitution protects minors' liberty against arbitrary deprivation by the state. *In re* Gault, 387 U.S. 1 (1967). Commentary on the Supreme Court's changing conceptualization of children's rights is provided in Rush, *The Warren and Burger Courts on State, Parent, and Child Conflict Resolution: A Comparative Analysis and Proposed Methodology,* 36 HASTINGS L.J. 461 (1985).

77. In rejecting one student's privacy claim under the fourth amendment, the Court noted that school administrators need greater latitude to conduct searches without a warrant or probable cause to believe students have committed a criminal offense. New Jersey v. T.L.O., 469 U.S. 325, 339–43 (1985); *see also* Hazelwood School Dist. v. Kuhlmeier, 108 S. Ct. 562 (1988) (rejecting student's first amendment challenge in part because permitting the speech would have placed an extra burden on school personnel).

78. *See* Lewis, *Misinterpretations of Educational Issues Abound as Election Year Gets Under Way,* 65 PHI DELTA KAPPAN 443, 443 (1984).

A. Overview of Potentially Applicable Law

1. Constitutional Law

As interpreted by the Supreme Court, the United States Constitution affords little if any protection against the types of privacy invasions CATI can entail.[79] Although the Court has interpreted the Constitution as protecting some types of privacy, the objectionable governmental actions in those cases are quite unlike anything CATI involves.[80] The Court's recently expressed unwillingness to extend privacy protection beyond these previously recognized contexts suggests the Constitution may not serve as a material constraint in this area.[81] Nonetheless, the Court has expressed the view that the Constitution limits egregious government information and record-keeping practices.[82] Thus, some CATI privacy invasions, particularly those

79. Regarding the evolving constitutional right of privacy, see Hufstedler, *The Directions and Misdirections of a Constitutional Right of Privacy,* 26 REC. A.B. CITY N.Y. 546 (1971); Posner, *The Uncertain Protection of Privacy by the Supreme Court,* 1979 SUP. CT. REV. 173; and Richards, *Constitutional Legitimacy and Constitutional Privacy,* 61 N.Y.U. L. REV. 800 (1986).

80. Zablocki v. Redhail, 434 U.S. 374 (1978) (marriage); Moore v. City of East Cleveland, 431 U.S. 494 (1977) (right to determine family unit); Roe v. Wade 410 U.S. 113 (1973) (abortion); Griswold v. Connecticut, 381 U.S. 479 (1965) (contraception). These cases rest upon a general constitutional privacy right, the source of which is much debated. *See* Epstein, *Substantive Due Process by Any Other Name: The Abortion Cases,* 1973 SUP. CT. REV. 159; Garvey, *Freedom and Choice in Constitutional Law,* 94 HARV. L. REV. 1756 (1981); Kauper, *Penumbras, Peripheries, Emanations, Things Fundamental and Things Forgotten: The Griswold Case,* 64 MICH. L. REV. 235 (1965).

Specific constitutional provisions that protect privacy, such as the fourth amendment prohibition against unreasonable searches and seizures, are too tangential to CATI to warrant discussion here except as they pertain to the legal significance of privacy expectations.

81. The Court's apparent reluctance to expand the scope of constitutional privacy appears in Bowers v. Hardwick, 478 U.S. 186 (1986). In concluding that criminal prosecution for consensual adult homosexual activity does not invade a zone of privacy protected by the Constitution, the Court emphasized that none of its previous holdings recognized an entitlement to engage in homosexual conduct. This strong attachment to precedent contrasts sharply with the reasoning from constitutional values that marked earlier privacy cases. Regarding the contrast between *Bowers v. Hardwick* and previous privacy cases, see Comment, *Thus Far and No Further: The Supreme Court Draws the Outer Boundaries of the Right of Privacy,* 61 TUL. L. REV. 907 (1987) (reviewing cases which increasingly expanded boundaries of right to privacy). Nor does the Court seem willing to address privacy issues under other amendments. *See* Note, Bowers v. Hardwick*: An Incomplete Constitutional Analysis,* 65 N.C.L. REV. 1100 (1987).

82. Although the Court has yet to vindicate an information privacy claim, it has treated such claims as legitimate. In Whalen v. Roe, 429 U.S. 589 (1977), the Court upheld the constitutionality of a New York state requirement that doctors report the identities of patients receiving certain prescription drugs to a central computerized registry. While finding the safeguards built into the New York system sufficient to warrant upholding the law, the majority opinion explicitly acknowledges that "the individual interest in avoiding disclosure of personal matters" is constitutionally protected. *Id.* at 599. In a concurring opinion, Justice Brennan offered an explanation of constitutional privacy protection that might have more bearing on CATI. In Brennan's view, "the Constitution puts limits not only on the type of information the

involving public school students' private thoughts or psycho-biological functioning, may be constitutionally impermissible.[83]

Unlike the federal version, some state constituions do have explicit privacy provisions.[84] In California, for example, the legislature has proclaimed that under the state constitution "all individuals have a right of privacy in information pertaining to them."[85] How much protection such provisions offer is uncertain, as most state constitution privacy clauses were adopted after 1970 and have yet to be construed authoritatively.

2. *Common Law*

With greater flexibility than constitutional law, common law provides a potentially powerful source of privacy protection. As with constitutional law, however, currently recognized common law causes of action do not clearly apply to CATI privacy invasions. In almost all states, privacy tort law has not moved beyond the four discrete varieties of privacy invasion Dean Prosser delineated almost thirty years

---

State may gather, but also on the means it may use to gather it." *Id.* at 607; *see also* Nixon v. Administrator of Gen. Serv., 433 U.S. 425, 465 (1977); Seng, *The Constitution and Informational Privacy, or How So-Called Conservatives Countenance Governmental Intrusion into a Person's Private Affairs,* 18 J. MARSHALL L. REV. 871, 893 (1985) (arguing that federal judges need to make explicit their reasons for denying informational rights to privacy); Note, *The Constitutional Right to Confidentiality,* 51 GEO. WASH. L. REV. 133 (1982) (differentiating autonomy right from right of confidentiality); Note, *The Constitutional Right to Withhold Private Information,* 77 NW. U.L. REV. 536, 547–57 (1982) (arguing that the Court in *Whalen* established a right to informational privacy which has been misapplied by lower courts); Note, *The Interest in Limiting the Disclosure of Personal Information: A Constitutional Analysis,* 36 VAND. L. REV. 139, 143 (1983) (arguing that an individual "who suffers injury should have standing to contend that the government had no legitimate interest in disclosing his personal information in violation of that original confidence, or that the disclosure did not bear a rational relationship to achievement of a valid governmental objective").

83. In addition to variations of substantive due process arguments that have been offered previously, a first amendment argument may exist for limiting some forms of CATI monitoring that intrude substantially on public school students' opportunities for mental repose. Among the functions of the first amendment, Thomas Emerson has identified restricting the government from interfering unduly with the opportunities an individual may have to "think his own thoughts, have his own secrets, live his own life, [and] reveal only what he wants to the outside world." T. EMERSON, THE SYSTEM OF FREEDOM OF EXPRESSION 545 (1970). CATI could be implemented in ways that would impinge upon such opportunities and perhaps give rise to a first amendment claim.

The outcome of any claim against allegedly unconstitutional practices in the schools is far from certain, however. *See supra* text accompanying notes 76–78.

84. *See, e.g.,* ALASKA CONST. art. I, § 22; ARIZ. CONST. art. 2, § 8; WASH. CONST. art. I, § 7; *see also* Peck, *Extending the Constitutional Right to Privacy in the New Technological Age,* 12 HOFSTRA L. REV. 893, 897 n.25 (1984); Development in the Law, *The Interpretation of State Constitutional Rights,* 95 HARV. L. REV. 1324, 1430–31 (1982).

85. CAL. CIV. CODE § 1798.1 (West 1985) (referring to CAL. CONST. art. 1, § 1).

ago.[86] Unless courts transcend the strictures of Prosser's discrete categories and recognize a more general theory of privacy torts,[87] the common law will afford little protection against the types of privacy invasions discussed in this article as peculiar to the CATI context.

3. *Statutory Law*

Some federal and state statutory provisions afford explicit, albeit limited protection against privacy invasion. The most comprehensive of the federal statutes is the Privacy Act of 1974 ("Privacy Act).[88] Several provisions of this seminal legislation pertain to information in government computers. The Freedom of Information Act,[89] by excluding from disclosure requests for personnel, medical, and similar files that would constitute an invasion of privacy, also bears on the privacy of many federal records. Both acts relate only tangentially to CATI, however. More directly relevant are the Family Educational Rights and Privacy Act of 1974 ("FERPA")[90] and the Education of the Handicapped Act ("EHA").[91] Both of these statutes impose detailed record-keeping regulations on all educational institutions receiving federal funds. FERPA has been credited with virtually eliminating the abuses toward which it was directed;[92] EHA extends the scope of FERPA to additional populations and refines some of its provisions. One other federal law applies to some school-based CATI.

86. Note, *Privacy, Computers, and the Commercial Dissemination of Personal Information,* 65 TEX. L. REV. 1395, 1412–13 (1987). The four categories are appropriation of a person's name or likeness, intrusion upon solitude or seclusion, portraying an individual in a false light, and public disclosure of private facts. RESTATEMENT (SECOND) OF TORTS ch. 28A (1977). Prosser first advanced his typology in *Privacy,* 48 CALIF. L. REV. 383, 389 (1960).

87. Several commentators have advocated such an approach. *See* Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser,* 39 N.Y.U. L. REV. 962 (1964); Gavison, *Privacy and the Limits of Law,* 89 YALE L.J. 421, 423 (1980); Note, *supra* note 86.

An Ohio case attests to the difficulty of persuading a court to recognize a claim that does not fit neatly within one of Prosser's categories. Plaintiffs sought a ruling that selling magazine subscription lists to mass mail merchandisers is tortiously privacy invasive. The court declined the invitation to go beyond settled law, asserting, "[i]t is not within our province to create a specific right which is not recognized at common law." Shibley v. Time, Inc., 45 Ohio App. 2d 69, 341 N.E.2d 337, 340 (1975).

88. 5 U.S.C. § 552a (1982 & Supp. IV 1986). For a review of how the Privacy Act has been interpreted, see Ehlke, *The Privacy Act After a Decade,* 18 J. MARSHALL L. REV. 829, 830 (1985).

89. 5 U.S.C. § 552(b)(6) (1982).

90. 20 U.S.C. § 1232g (1982).

91. 20 U.S.C. §§ 1411–1420 (1982 & Supp. IV 1986).

92. Rudensky, *Buckley Amendment Found Effective in Protecting Student Privacy,* CHRONICLE HIGHER EDUC., May 5, 1982, at 15; Schatken, *supra* note 42, at 150–51.

The Pupil Protection Act limits collection of certain types of information by some federally funded experimental programs.[93]

A number of states have passed laws similar to, and in some cases more extensive than, the federal legislation.[94] For a time in the early 1970's, state legislatures were very active on the privacy front, but that activity largely subsided following congressional approval of the Privacy Act and FERPA. Like the federal statutes, state laws almost uniformly lack specific reference to CATI. A broad interpretation of these laws may be possible in states such as California, though, where the legislature has recognized that the "increasing use of computers and other sophisticated information technology has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."[95]

One limitation of all federal and many state privacy laws is that they apply only to governmental agencies or private enterprises affiliated with the government. Agreements among private parties may fill the gap to some extent. For example, a labor contract may limit employee testing. In the absence of enforceable laws or other legally-binding constraints on privacy invasion, however, CATI practitioners are subject only to the guidelines of professional organizations to which they may belong.[96]

Unfortunately, these various sources of privacy regulation do not combine into an adequate system. Some privacy issues may be governed by several distinct sources of law. Other issues are not addressed at all. Constitutional and common law may evolve to provide more comprehensive coverage, but currently offer no protection against some of the privacy threats CATI poses.[97] Statutes enacted

93. 20 U.S.C. § 1232h (1982). The law prohibits requiring students to participate in certain forms of examination, testing, and treatment, the primary purpose of which is to reveal information about seven listed items including sex behavior and attitudes, income, and political affiliations. *Id.* § 1232h(b); *see* Mesibov, *Protection of Students' Privacy Rights: The Hatch Amendment,* SCH. L. BULL., Fall 1985, at 15.

94. *See, e.g.,* CAL. GOV'T CODE §§ 6250–6267 (West 1980 & Supp. 1988); WIS. STAT. ANN. § 895.50 (West 1983). For a discussion of the potential interplay between federal and state statutes, see Comment, *Access to Student Records in Wisconsin: A Comparative Analysis of the Family Educational Rights and Privacy Act of 1974 and Wisconsin Statute Section 118.125,* 1976 WIS. L. REV. 975. A similar analysis of California law may be found in Comment, *Informational Privacy and Public Records,* 8 PAC. L.J. 25 (1977).

95. CAL. CIV. CODE § 1798.1(b) (West 1985).

96. *E.g.,* AMERICAN ASSOCIATION OF STATE PSYCHOLOGY BOARDS, GUIDELINES FOR COMPUTER BASED ASSESSMENTS AND INTERPRETATION (Mar. 1985) (copy on file with *Washington Law Review*); AMERICAN PSYCHOLOGICAL ASSOCIATION, GUIDELINES FOR COMPUTER-BASED TESTS AND INTERPRETATIONS (Jan. 1986) (copy on file with *Washington Law Review*).

97. In addition to the limitations discussed above, see *infra* text accompanying note 158.

within the past fifteen years fill some of the gaps, but most were passed without reference to CATI technologies and are not designed to deal with privacy problems that arise when individuals interact directly with computers as they may in CATI.

B. Applicability to CATI of Existing Privacy Law

To expose the deficiencies of current law, the following analysis examines the application of the various sources of law reviewed above to the CATI privacy threats discussed in Part II. First, the analysis discusses potential limitations on using computers to collect information. Second, limitations on the use of information gathered are assessed. Third, the analysis examines current safeguards against misperceptions resulting from CATI.

1. Limitations on Using Computers to Collect Information During Testing and Instruction

Aside from prohibiting most secret surveillance, laws place few constraints on either the types of information that can be gathered pursuant to CATI or on the techniques that may be used to gather it. Of the four privacy torts, only intrusion into private affairs[98] has any relevance. Courts have interpreted this proscription primarily as a safeguard against interfering with personal activities by observing such activities without permission or by disrupting an individual's solitude or seclusion.[99] To transfer this protection against meddlesome intrusion to the quite different circumstances of CATI would require a broadening of current doctrine.[100] Even if the doctrine were stretched, consent by the record-subject would limit its utility. Almost all testing and instruction participants voluntarily relinquish control over information the computer collects. Consent, if given knowingly and intelligently, insulates the information collection process from legal challenge.[101]

98. *See* RESTATEMENT (SECOND) OF TORTS § 652B (1976); Comment, *The Emerging Tort of Intrusion,* 55 IOWA L. REV 718 (1969–70).

99. Galella v. Onassis, 353 F. Supp. 196, 241 (S.D.N.Y. 1972) (constant surveillance of celebrity by photographer redressed by injunction prohibiting photographer from approaching within certain distances of celebrity, her home, and her family).

100. *See* Comment, *Informational Privacy and Public Records,* 8 PAC. L.J. 25 (1977). One difficulty is that, under current doctrine, the defendant must know or should know that the intrusion would be offensive to persons of ordinary sensibilities. *See, e.g.,* Bitsie v. Walston, 85 N.M. 655, 515 P.2d 659, 661 (N.M. Ct. App.), *cert. denied,* 85 N.M. 639, 515 P.2d 643 (N.M. 1973). The types of intrusion associated with CATI are not as clearly outrageous.

101. McDaniel v. Atlanta Coca-Cola Bottling, 60 Ga. App. 92, 2 S.E.2d 810 (1939) (plaintiff's authorization to defendant company to investigate his personal injury claim

A few statutes pertaining generally to information collection might include CATI within their scope. A number of the major privacy laws impose a requirement that government agencies collect only information that is relevant to some legitimate, specified purpose.[102] Attempts to gain certain types of information during CATI could run afoul of such provisions.[103] That such laws appreciably limit CATI, though, is doubtful. The purpose of many types of testing and instruction is so broad that almost any information may be deemed relevant.

The prospect that individuals may be compelled to reveal highly sensitive personal data during psychological testing or some similar process has prompted at least a small legislative response. A 1974 congressional limitation on certain federally funded experimental education programs forbids requiring students to submit to psychiatric or psychological examination, testing, or treatment, the primary purpose of which is to reveal psychological problems, sexuality, illegal and anti-social behavior, family relations, or other highly personal matters.[104] Reflecting a similar concern for privacy, a Nebraska law prohibits asking questions during a polygraph or voice stress examination regarding the examinee's sexual practices, labor union, political or religious affiliations, or marital relationship, except when such questions bear on the issues under examination.[105] Such laws logically might be extended to CATI, but do not apply clearly as written.

In the absence of specific legislation, the courts have taken tentative steps toward limiting some forms of data collection. In one case, a federal district court prohibited administration of a paper and pencil survey designed to identify potential drug users among junior high school students.[106] In holding that the survey violated the constitutional right of privacy, the court found that the dangers associated with compelling students to answer sensitive questions about personal matters, such as their relationships with their parents, exceeded any

---

constituted consent to gather personal information about plaintiff); Note, *Jar Wars: Drug Testing in the Workplace,* 23 WILLAMETTE L. REV. 529, 560–61 (1987) (consent, if voluntary, may vitiate objection to drug testing).

102. *E.g.,* Privacy Act of 1974, 5 U.S.C. 552a(e)(1) (1982); *see* Ehlke, *supra* note 88, at 830. Although FERPA contains no similar limitation on collection of information for education records, constraints may be found at the state level. The Illinois School Student Records Act, for example, requires that every entry in a student's file be "of clear relevance to the education of the student." ILL. ANN. STAT. ch. 122, para 50-4(c) (Smith-Hurd Supp. 1988).

103. During a stress or aptitude test, for example, questions might probe into attitudes that are irrelevant to the purpose for which the test is being conducted.

104. General Education Provisions Act, 20 U.S.C. § 1232h(b) (1982).

105. NEB. REV. STAT. § 81-1928(3) (1987).

106. Merriken v. Cressman, 364 F. Supp. 913, 921 (E.D. Pa. 1973).

good the program might accomplish.[107] In an employment context, another court reached the opposite conclusion. Applicants seeking to become fire fighters in Jersey City, New Jersey unsuccessfully challenged mandatory psychological testing that probed into their private affairs.[108] The court held that the interest of the city in screening out applicants who would not be able to handle the psychological pressures of the job was sufficient to justify the intrusion into the applicants' privacy.[109] These cases suggest that judicial protection against information gathering is equivocal and will depend on the context, the potential harm to the individual, and the expected benefits for society.

In addition to these minor limits on the types of information computers may collect, laws also place a few restrictions on the techniques used in gathering information. Most of these limitations are of little value in the typical testing or instruction setting, either because the record-subject consents to the process or because CATI applications do not fit within the definition of the prohibited method. For example, similarities between some aspects of CATI and wiretapping might suggest that limitations on wiretapping should apply.[110] Wiretapping is prohibited largely because it occurs without the target's awareness and violates that person's reasonable expectations about the confidentiality of the communication.[111] The same considerations may apply if computers are used in testing and instruction to monitor subjects without their knowledge or if such computers use algorithms to draw inferences based on information the subject knowingly provides.[112] Despite this similarity, such situations are not within the ambit of wiretapping statutes because the language of those laws is limited to intercepting a communication being transmitted from sender to receiver.[113] The CATI process lacks this feature.

---

107. *Id.* at 918, 920–21.

108. McKenna v. Fargo, 451 F. Supp. 1355, 1381 (D.N.J. 1978), *aff'd,* 601 F.2d 575 (3d Cir. 1979).

109. *Id.* The court was not entirely sympathetic to the requirement, however, noting, "[t]here is good reason to scrutinize a government requirement which joins the words psychology and testing. Psychology is not yet the science that medicine is and tests are too frequently used like talismanic formulas." *Id.* at 1357.

110. For examples of wiretap legislation, see Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848, 1851 (codified in scattered sections of 18 U.S.C.); CAL. PENAL CODE § 632 (West 1970 & Supp. 1988); and MICH. STAT. ANN. § 28.807(3) (Callaghan 1982).

111. Ashdown, *supra* note 4, at 1311–12.

112. Such a possibility may be quite strong where the computer is used in routine instruction.

113. *See, e.g.,* Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2511(1) (Supp. IV 1986); CAL. PENAL CODE § 632 (West 1970 & Supp. 1988).

One other source of law pertaining to an activity similar in some respects to CATI is the restriction some states place on the use of polygraphs.[114] The second vignette described in the introduction to this article envisions a computer functioning as a lie-detector. Statutes and court decisions restricting polygraph use could be invoked when a computer substitutes for a human examiner. To the extent these restrictions are motivated by aversion to the physical intrusiveness of wiring a human to a polygraph machine, though, veracity assessment techniques relying on computer keyboard input alone may be unaffected.[115]

2. *Limitations on the Use of Information Gathered During CATI*

When legislatures first reacted to the existence of massive computer dossiers potentially available to any curious party, they enacted statutes to limit access to government data files.[116] The Privacy Act of 1974,[117] the Federal Educational Rights and Privacy Act of 1976 ("FERPA"),[118] and the Education of the Handicapped Act ("EHA")[119] all restrict record access. Each of these laws prohibits release of specified records without the record-subject's consent, unless the disclosure fits within one of the explicitly permitted exceptions. For FERPA, those exceptions permit access by school personnel with legitimate educational interests, agents of accrediting agencies, and individuals satisfying any of seven other criteria.[120] All of these laws reflect an international public consensus that access to computer files should be limited.[121]

---

114. For reviews of the legal limitations on polygraph testing, see Herron, *Statutory Restrictions on Polygraph Testing in Employer-Employee Relationships,* 37 LAB. L.J. 632 (1986); Nagle, *The Polygraph in the Workplace,* 18 U. RICH. L. REV. 43, 64–76 (1983); and Toomey, *Compelled Lie Detector Tests and Public Employees: What Happened to the Fifth Amendment?,* 21 S. TEX. L.J. 375 (1981).

115. Experimenters are continuing to explore methods of assessing truthfulness without attaching sensors to the body. *See* Kubis, *Some Problems of Privacy and Surveillance in a Technological Age,* in PRIVACY 193, 217 (W. Bier ed. 1980). The computer could be a key component of such a system.

116. Trubow, *Fighting Off the New Technology,* HUM. RTS., Fall 1982, at 26, 51.

117. 5 U.S.C. § 552a (1982 & Supp. IV 1986).

118. 20 U.S.C. § 1232g (1982).

119. 20 U.S.C. §§ 1412–1420 (1982 & Supp. IV 1986).

120. 20 U.S.C. § 1232g(b)(1) (1982).

121. U.S. CONGRESS, *supra* note 43, at 27–29 (reviewing opinion polls showing substantial concern about improper use of computerized information); Gassman & Pipe, *Synthesis Report,* in 10 POLICY ISSUES IN DATA PROTECTION AND PRIVACY: CONCEPTS AND PERSPECTIVES 12, 12–13 (Proceeding of the OECD seminar, June 24-26, 1974) (reporting consensus of European representatives that access should be limited); PRIVACY PROTECTION STUDY COMM'N, *supra* note 58, at 19–21 (offering guidelines to protect the perceived public interest in limited access).

Despite substantial efforts to mandate that information in computer files be secure, these measures have not yet addressed the special security concerns attributable to the special nature of CATI. The highly personal nature of some testing and instruction makes access to some CATI records potentially more privacy invasive than access to other types of records. Although some statutes do specify higher levels of security for particularly sensitive information,[122] the chief federal laws bearing most directly on CATI do not make such a distinction. Thus, for example, under FERPA, the exceptions that permit access without the record-subject's consent do not differentiate between a chemistry grade and a computer-generated personality profile.[123] The capabilities of CATI to create highly sensitive personal records could make the access provisions more privacy invasive than Congress had intended.[124]

The one common law rule that may apply to disclosures of accurate information is the prohibition in many states against public disclosure of private facts.[125] The current utility of this doctrine for the typical CATI situation is quite limited, however, because courts typically have denied recovery unless the disclosure was to a sufficiently large public.[126] Passing the information along to a supervisor or transmitting it from one computer to another, without more, probably would not satisfy this "public disclosure" requirement.

---

122. *See, e.g.*, N.Y. PUB. HEALTH LAW § 3371 (McKinney 1985) (prohibiting disclosure of knowledge of particular patients or research subjects, as well as reports or records of them); WASH. REV. CODE § 71.24.035(5)(h) (1987) (listing statutory references for preventing disclosure by mental health authorities).

123. 20 U.S.C. § 1232g(b)(1)(A) (1982).

124. The same danger does not exist for most other forms of highly sensitive information about students that school personnel may have recorded because written observations of a teacher or school psychologist are likely to fit within the "private records" exclusion from FERPA's definition of education records. *Id.* § 1232g(a)(4)(B)(i). Records a computer generates from student input do not qualify for the "desk notes" exclusion because they are not made by school personnel for the purpose of reminding themselves of the matter noted. For a discussion of FERPA's "private records" provision, see Schatken, *supra* note 42, at 159–61.

125. *See, e.g.*, McSurely v. McClellan, 753 F.2d 88, 112–13 (D.C. Cir.), *cert. denied*, 475 U.S. 1005 (1985). This case provides an example of how a court emphasizes flexibility in the application of the theory behind the tort of disclosure to specific instances of conduct. The court held actionable the conduct of a Senate subcommittee investigator who forced a husband to read through, page by page, documents detailing intimacies of his wife's premarital relationships. The husband, who had been unaware of these activities, was thus forced to discover them. The court held actionable a cause under a theory of invasion of each spouse's seclusion. *See also* RESTATEMENT (SECOND) OF TORTS § 652D (1977).

126. *See, e.g.*, Harrison v. Humble Oil & Ref., 264 F. Supp. 89, 92 (D.S.C. 1967); Timperley v. Chase Collection Serv., 272 Cal. App. 2d 697, 77 Cal. Rptr. 782, 783–84 (1969); French v. Safeway Stores, 247 Or. 554, 430 P.2d 1021, 1022–23 (1967); *see also* PROSSER AND KEETON ON THE LAW OF TORTS 856–59 (W. Keeton 5th ed. 1984).

In recognition that records may be highly sensitive and that their release to inappropriate parties could be damaging to the record-subject, courts and legislatures have substantially restricted the discretion of information managers. The day has long since passed when record custodians could credibly assert an ownership interest in the contents of the files they possessed.[127] The law now recognizes that individual record-subjects retain a measure of control over at least some information about them that has passed into an organization's data banks. One may doubt the adequacy of these limitations, however, in view of the capacity of instructional and testing computers to collect so much information, on so many people, that has such potential for being abused.

3. *Safeguards Against Misperceptions Resulting from CATI Results*

Along with preserving confidentiality, insuring accuracy of computer records has been a major thrust of regulation. The principal means of accomplishing this objective has been to give record-subjects the rights to review their files and to challenge misleading material.[128] Statutes incorporating this feature give public education students and some other individuals a potentially effective means of policing the accuracy of CATI files maintained by government institutions. Similar provisions for the private sector are rare.

Purging information no longer needed for any legitimate purpose is also an essential element of computer privacy regulation. Nonetheless, the major privacy laws have not required systematic removal of outdated data.[129] The more recent Education of the Handicapped Act ("EHA") requires schools to notify parents of handicapped students when records are no longer needed and to destroy those records if the parents so request.[130] Inclusion of this provision may signal increasing legislative concern about the distortions that may result from retention of old records.

A number of states have adopted provisions similar to the EHA limitation, and some have imposed specific time periods after which records must be destroyed.[131] A Massachusetts law reflects particular sensitivity in this regard. In all Massachusetts public schools, "[t]he

127. Cudlipp, *supra* note 42, at 33–34.

128. *See, e.g.*, Privacy Act of 1974, 5 U.S.C. § 552a (1982 & Supp. IV 1986); Federal Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g (1982).

129. Neither the Privacy Act of 1974 nor FERPA restricts retention.

130. 20 U.S.C. §§ 1412(2)(D), 1417(c) (1982).

131. *E.g.*, ILL. ANN. STAT. ch. 122, para. 50-4(f) (Smith-Hurd Supp. 1988) (temporary records must be destroyed within five years of student's last attendance).

score of any group intelligence test administered to a student enrolled in a public school shall be removed from the record of said student at the end of the school year in which such test was so administered."[132]

With regard to the accuracy of records the computer itself has generated, no laws specifically apply. Nonetheless, common law and constitutional principles may afford a basis for a legal claim if someone suffers harm because of a negligently developed or administered CATI system.[133] The possibility of such litigation may motivate CATI operators to proceed responsibly.

Cases challenging alleged inappropriate use of conventional psychological testing might have provided useful guidance in establishing limits on the use of information generated in the course of CATI. The difficulty is that the precedents regarding use of psychological tests are in disarray. Two major cases pertaining to use of intelligence tests in educational placement reveal the depth of disagreement. A district court in California ruled that a standardized test could not be used for placing black children in educable mentally retarded classes because the test was culturally biased and therefore misclassified the students.[134] After reviewing much of the same evidence, an Illinois court held that, when used with other criteria, standardized test results are a permissible basis for special education assignments.[135]

The opposite outcomes of these cases demonstrate not only the legal vulnerability of testing in general, but also the range of judicial opinion on the matter. By analogy to conventional testing, the ability of CATI to withstand judicial scrutiny will depend in part on the sufficiency of empirical research confirming the validity of computer-generated inferences. In contrast to conventional testing cases, however, the outcome for a CATI challenge also may depend on a judge's opinion of the propriety of computers, rather than humans, making the critical inferences.

An important ancillary issue underlying all attempts to safeguard against misperception is the ability of a record-subject to determine

132. MASS. ANN. LAWS ch. 71, § 87 (Law. Co-op. Supp. 1988).

133. Common law tort actions for defamation or portraying a person in a false light may be available. *See generally* Nycum & Lowell, *Common Law and Statutory Liability for Inaccurate Computer-Based Data,* 30 EMORY L.J. 445, 452–62 (1981) (exploring potential liabilities for those charged with maintaining accuracy in asset accounts). Application of these doctrines to CATI records raises no special issues and is not explored at length here.

134. Larry P. v. Riles, 495 F. Supp. 926, 988–89 (N.D. Cal. 1979), *aff'd in part, rev'd in part,* 793 F.2d 969 (9th Cir. 1984).

135. Parents in Action on Special Educ. (PASE) v. Hannon, 506 F. Supp. 831, 882–83 (N.D. Ill. 1980). For a more thorough comparison of *Larry P.* and *PASE,* see Bersoff, *Testing and the Law,* 36 AM. PSYCHOLOGIST 1047 (1981).

how the computer transformed the raw data it collected. Although no legislation addresses this issue directly, FERPA might be interpreted to provide a right of access to a copy of the code comprising the actual computer program. This right might be inferred from the FERPA requirement that educational institutions provide students with an explanation or interpretation of any education record.[136] Trade secrecy, copyright, and other competing considerations, however, may dissuade courts from interpreting the right so broadly.

Furthermore, very little law regulates attribution of the source of computer records, whether accurate or not. An Illinois statute requiring that every entry to a student's cumulative file bear the name and signature of the person responsible for adding the information provides an example of what might be done to ensure that a record can be traced back to its source.[137] Although the Illinois legislature did not contemplate computerized record systems when passing that law, the principle it embodies may be even more important as computer technology makes it harder to determine how a record originated.[138]

Because the harm from inaccuracy is so readily comprehended, legislators and courts have long recognized the propriety of relief. Nonetheless, existing sources of protection against CATI errors are not adequate. Current regulation does not recognize the capacity of sophisticated computer programs to err in new ways. The danger of erroneous records will increase as testing and instruction computers not only record information that users consciously enter, but also draw and record their own inferences from those entries. The potential harm increases as computers tailor interactions dynamically depending upon users' responses.[139] Even if such procedures function flawlessly, they may threaten privacy. The patterns of interaction between young children and a seemingly omniscient computer may seriously distort their developing expectations of privacy and sense of self.[140]

136. 20 U.S.C. § 1232g(a)(2) (1982); *see* Bersoff, *supra* note 135, at 1053–55.

137. *See* ILL. ANN. STAT. ch. 122, para. 50-4(d) (Smith-Hurd Supp. 1988).

138. Fortunately, a computer program can be designed to include procedures that make the origins of many records discernible.

139. *See supra* notes 69–71 and accompanying text.

140. *See infra* note 165 and accompanying text.

IV. TOWARD ADEQUATE PRIVACY LIMITATIONS ON CATI

A. Transcending the Existing Privacy Protection Framework

The principal problem with seeking adequate privacy limits for CATI within current law is that the existing legal framework for privacy protection does not comprehend the most serious threats CATI poses. Since 1977, the de facto standards for privacy protection in the United States have been the three cardinal recommendations of the Privacy Protection Study Commission:

> [T]o create a proper balance between what an individual is expected to divulge to a record-keeping organization and what he seeks in return *(to minimize intrusiveness)*;
>
> [T]o open up record-keeping operations in ways that will minimize the extent to which recorded information about an individual is itself a source of unfairness in any decision about him made on the basis of it *(to maximize fairness)*;
>
> and
>
> [T]o create and define obligations with respect to the uses and disclosures that will be made of recorded information about an individual *(to create legitimate, enforceable expectations of confidentiality)*.[141]

The consensus that has developed around these principles[142] suggests they may reflect a nationally acceptable balance between privacy and efficiency with respect to the matters they address. Thus they must serve as at least a starting point for CATI privacy regulation.

---

141. *See* PRIVACY PROTECTION STUDY COMM'N, *supra* note 58, at 14–15. In passing the Privacy Act of 1974, Congress created the Privacy Protection Study Commission to conduct

> a 'study of the data banks, automatic data processing programs, and information systems of governmental, regional, and private organizations, in order to determine the standards and procedures in force for the protection of personal information' [and] to recommend to the President and the Congress the extent, if any, to which the principles and requirements of the Privacy Act of 1974 should be applied to organizations other than agencies of the Federal Executive branch and to make such other legislative recommendations as the Commission deems necessary to protect the privacy of individuals while meeting the legitimate needs of government and society for information.

Id. at xv.

142. See also U.S. DEP'T HEW, SEC'Y'S ADVISORY COMM. ON AUTOMATED PERSONAL DATA SYSTEMS, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS (1973), which recommends the following principles of "fair information practice":

> There must be a way for an individual to find out what information about him is in the record and how it is used.
>
> There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.
>
> There must be a way for an individual to correct or amend a record of identifiable information about him.

Id. at 41.

With regard to the second and third points, straightforward application of the Commission's information management principles may provide an adequate basis for specifying acceptable limits on the use of information collected in the CATI process. Whether point one is adequate to respond to the remaining CATI privacy threats depends on the meaning given to "intrusion into personal affairs."[143] To date, this phrase has been understood to refer almost exclusively to processes that probe into especially sensitive areas, involve surreptitious data-gathering, or invade an individual's seclusion.[144] But lawmakers must also recognize that depriving people of control over the collection of information about them is inimical to privacy even if the method employed does not intrude into "personal affairs" per se.[145] The more pervasive, mysterious, impersonal, and imperceptible the process, the more objectionable it is according to this alternative view.

The most serious challenge to the Privacy Protection Study Commission's paradigm comes from the use of computers to gather information incident to routine activities. In such instance, the monitoring or information gathering occurs not as the principal objective of the activity, but as a byproduct of an activity undertaken for an independent purpose. A distinguishing feature of this process is that the individual engaging in it has no interest in a record being created, and very often the organization that creates the record needs it only momentarily.[146]

---

143. While legislatures have passed numerous privacy laws directed toward effectuating the second and third points, few measures are designed to limit data gathering in the first instance. *See* Rule, McAdam, Stearns & Uglow, *supra* note 60, at 74–76.

144. 1 PRIVACY LAW AND PRACTICE ¶ 1.06 (G. Trubow ed. 1987).

145. Consensus may exist regarding this proposition, despite its lack of manifestation in the major privacy laws. One group of authors has conjectured that "[e]ven when the ends of surveillance are impeccable and even when the agencies concerned carry out their monitoring with full rectitude and discretion, the monitoring of *every* moment would strike most people as unacceptable." Rule, McAdam, Stearns & Uglow, *supra* note 60, at 74; *see also* Fried, *supra* note 22, at 475. While this may be true, we are less certain that "virtually everyone" will insist on limiting monitoring at the expense of efficiency or other clear benefits, especially if the subjects are children. *See* Miller, *Do Americans* Really *Value Privacy?*, in THE RIGHT TO PRIVACY 40 (G. McClellan ed. 1976) (concluding that the public will pay very little for privacy).

146. Placing local telephone calls is the quintessential example. A caller gains nothing by having the telephone number recorded. The telephone company needs the number only to place the call. Having obtained the number for that purpose, the telephone company typically makes no record of it, although it could.

The reasonableness of a person's expectation that a telephone company will not retain a telephone number after it has been used to place a call divided the Supreme Court in Smith v. Maryland, 442 U.S. 735 (1979). The majority concluded that because the caller must reveal the number to the telephone company in order to place the call, an expectation of privacy is not reasonable. *Id.* at 742. Justice Stewart's dissent analogized the number dialed to the caller's spoken message, which also must be provided to the telephone company for communication to

The generation of a record incident to some activity certainly is not unique to CATI nor even a phenomenon solely of the computer era. By writing checks and placing telephone calls, individuals produce incidental records that may be used for purposes the originator never intended.[147] What computers add is a quantum increase in the pervasiveness of incidental information recording and the possibility of its extension into more personal domains. As has been recognized with regard to interactive cable television[148] and microprocessor-equipped transaction cards,[149] the privacy implications of new technologies that have the capacity to record information about people's daily affairs are not generally appreciated when the technologies are adopted.

In CATI, a classroom computer may monitor a student's keystrokes so it can respond with appropriate instructional displays. In the workplace, a secretary's word processor records keystrokes to create a business letter. Incidentally, both computers can produce a record of errors, interaction time, and other items that may later be analyzed in combination with other information. As these incidental monitoring techniques become part of the daily routines of education and work, the potential for developing detailed character profiles will rise sharply.

Trying to frame objections to any of these privacy invasive processes within the existing legal framework is almost impossible. Although erroneous data processing that results in a defamatory characterization of a person and release of test results to inappropriate parties fits the traditional legal model, use of a test like the one described in the opening vignette about Brenda is not easily challenged through litigation. Aside from the possibility of error that the vignette highlights, Brenda's objection to taking the test may have little to do with this particular instance of intrusion into matters she regards as private, but with the pattern of which it is a part. Perhaps the employer also

---

occur. *Id.* at 747–48 (Stewart, J., dissenting). With digitized communication, the majority's distinction based on whether the "contents" of the communication are acquired is extremely insubstantial.

147. In addition to *Smith*, see United States v. Miller, 425 U.S. 435 (1976) (checks, deposit slips, and other bank related documents considered business records of the bank, not private papers; therefore, respondent had no legitimate expectation of privacy upon which he could argue that such records should be protected from disclosure by subpoena) (superceded by statute); and Ashdown, *supra* note 4.

148. Meyerson, *The Cable Communications Policy Act of 1984: A Balancing Act on the Coaxial Wires,* 19 GA. L. REV. 543, 612–18 (1985); Note, *As Interactive Cable Enters, Does Privacy Go Out the Window?,* 4 COMM/ENT L.J. 781 (1982); Comment, *Interactive Cable Television: Privacy Legislation,* 19 GONZ. L. REV. 709 (1983–84).

149. Peck, *supra* note 84, at 896; Weingarten, *supra* note 35, at 20.

makes use of drug testing,[150] criminal record checks,[151] genetic screening,[152] video surveillance,[153] polygraph tests,[154] background checks,[155] and computerized productivity monitoring.[156] In combination, these measures may reduce individual privacy below an acceptable threshold.[157] The panoply of privacy invasions in Brenda's off-the-job environment may also contribute to the perceived offensiveness of the employment screening test. From Brenda's perspective, this one test may push the cumulative assault on her privacy over the limit. Isolated as a single legal claim, however, Brenda's complaint is but an individualized dissatisfaction a court has no power to remedy.[158]

Brenda's next challenge would be to formulate a legal theory that would provide an exception to employers' traditional discretion to hire

150. *See generally* Rothstein, *Drug Testing in the Workplace: The Challenge to Employment Relations and Employment Law,* 63 CHI.-KENT. L. REV. 683, 743 (1987) (arguing that "a facile solution to the problem of workplace drug abuse will not be found in a specimen jar or a million specimen jars"); Comment, *Unrestricted Private Employee Drug Testing Programs: An Invasion of the Worker's Right to Privacy,* 23 CAL. W.L. REV. 72 (1986).

151. For an example of a law prohibiting most employers from requesting arrest information, see CAL. LAB. CODE § 432.7 (West Supp. 1988).

152. For an overview of the current debate on genetic testing in the workplace, see Peirce, *The Regulation of Genetic Testing in the Workplace—A Legislative Proposal,* 46 OHIO ST. L.J. 771 (1985).

153. *See* I. SHEPARD & R. DUSTON, WORKPLACE PRIVACY: EMPLOYEE TESTING, SURVEILLANCE, WRONGFUL DISCHARGE, AND OTHER AREAS OF VULNERABILITY 63–64 (1987) (discussing invasive nature of video surveillance).

154. *See* Nagle, *supra* note 114 (invasive quality of polygraph tests).

155. *See* I. SHEPARD & R. DUSTON, *supra* note 153, at 47–48 (invasive quality of background checks).

156. *See* 9 TO 5, NAT'L ASS'N OF WORKING WOMEN, Computer Monitoring and Other Dirty Tricks 3–4 (April 1986) (copy on file with *Washington Law Review*); Sherizen, *Work Monitoring: Productivity Gains at What Cost to Privacy?,* COMPUTERWORLD, July 7, 1986, at 55.

157. Aside from dissatisfaction with the requirements of a particular employer, the job applicant may be seeking to construct some barrier against the panoply of privacy invasions in her environment.

158. For tactical purposes, a litigant may need to isolate a single element of a complex system as being particularly objectionable—the screening test in Brenda's case. The trade-off of focusing on a single element, however, is likely to be that the potential harm appears insignificant in isolation and that the litigation will not provide an opportunity to present the totality of the potential harm.

Challenging an entire system or pattern of operation in court, while possible, is unwieldy. The litigation campaigns to improve conditions in prisons and mental health facilities demonstrate that courts can deal with systemic wrongs and fashion sufficiently detailed remedies to redress identifiable harms. *See, e.g.,* Wyatt v. Stickney, 325 F. Supp. 781 (M.D. Ala. 1971), *aff'd in part, rem'd in part sub nom.* Wyatt v. Aderholt, 503 F.2d 1305 (5th Cir. 1974). In light of the difficulties encountered in *Wyatt,* however, it may be the exception that proves the rule that courts are not well suited for such functions. For an account of the problems that dogged the decade-long litigation effort to improve conditions at the Willowbrook mental institution in New York, see D. ROTHMAN & S. ROTHMAN, THE WILLOWBROOK WARS (1984).

upon whatever nondiscriminatory grounds they choose.[159] Brenda would also need to overcome the judiciary's natural reluctance to grant claims based on allegations of contingent or remote harm.[160]

The inadequacy of current law for protecting privacy interests against invasive CATI practices leaves the developers and users of these techniques with de facto authority to balance the benefits of each CATI practice against the damage individuals and society may suffer from loss of privacy. Ideally, this discretion will be used to adopt standards that respect privacy. Prospects for adequate self-regulation, however, are slim.[161] The diversity of CATI users in education and employment makes it unlikely that professional organizations will provide the requisite leadership and uniformity. Even if a mechanism develops for promulgating and enforcing industry-wide standards, lack of consensus about what those standards should be will impede action. Given the industry's self-interest in the matter and the profound societal ramifications of the outcome, government intervention offers the only feasible method of insuring adequate privacy protection.

B. A Statutory Response

1. General Features of an Adequate Law

If the law is to respond, the statutory route offers the best method of regulating CATI. Not only can statutes be written with sufficient precision and revised as necessary in light of future developments, they can afford practitioners a clear source of guidance. Leaving the matter to further constitutional or common law development risks sacrificing important societal interests that individual litigants are poorly suited to raise.[162] Relying on the limited class of individuals who would have standing to sue could result in poor policy for everyone. Most

159. *See* M. ROTHSTEIN, A. KNAPP, & L. LIEBMAN, EMPLOYMENT LAW 191–92 (1987); *see also* Hermann, *Privacy, the Prospective Employee, and Employment Testing: The Need to Restrict Polygraph and Personality Testing*, 47 WASH. L. REV. 73 (1971) (reviewing the panoply of laws and legal theories pertaining to employment screening and concluding that there are few constraints on employers' discretion to require applicants to take tests).

160. *See, e.g.*, Laird v. Tatum, 408 U.S. 1 (1972) (dismissal of a claim against the Army based on its conducting surveillance of lawful peace movement activities upheld because plaintiffs failed to show actual or imminent harm). The paucity of empirical research on the effects of privacy deprivation may incline courts to adopt a wait and see attitude.

161. Self-regulation has long been recommended. *See, e.g.*, Grenier, *Computers and Privacy: A Proposal for Self-Regulation*, 1970 DUKE L.J. 495 (suggesting self-regulation with oversight by the federal government).

162. *See* Simitis, *supra* note 57, at 709. In the employment context, the decision to sue may come at the cost of a workplace confrontation between one or more employees and an employer. For CATI used in the schools, a court challenge will occur only if interested adults decide to sue

importantly, enacting suitable legislation seizes the opportunity to act prospectively before privacy invasive CATI procedures become widespread.[163]

To derive the benefits CATI offers and still protect privacy, safeguards as novel as the dangers must be devised.[164] For example, in classroom settings, students might be empowered to opt out of computerized monitoring whenever they press a button. This mechanism would provide tomorrow's students with a shield from observation similar to what we enjoyed when writing in a notebook we did not intend to give to the teacher.

Based on the meager research findings on children's development of privacy expectations, putting the burden on the student to withdraw from monitoring may be an unrealistic approach for young children who have not internalized privacy values.[165] To assist primary school students in developing a sense of privacy, structuring their computer interactions to include periods that are clearly exempted from teacher monitoring would be more effective. For this purpose, the children's terminals might be programmed to display a picture of the teacher when their keystrokes were being monitored. Such a visual representation would provide the electronic equivalent of the teacher's physical presence that put previous generations of children on notice that they were being observed. Another novel limitation would be to limit both the creation of permanent records based on students' daily interactions with classroom computers and the routine transmission of student records from instructional to administrative computers.

Formulating specific rules to implement these principles and otherwise to provide adequate privacy protection promises to be difficult because of the unique privacy problems presented and the diversity of the CATI field. Ideally, attention would be paid to several factors:

---

on behalf of the children whose privacy is invaded. Furthermore, the cost of litigation may be considered excessive relative to the benefits of a single litigant.

163. Declaratory relief may be available in some situations, but the remoteness of the conjectured harm will constrict the availability of this avenue. *See, e.g.*, FED. R. CIV. P. 57.

164. *See generally* Sterling, *Stressing Design Rather Than Performance Standards to Ensure Protection of Information: Comments*, in COMPUTERS AND PRIVACY IN THE NEXT DECADE 103 (L. Hoffman ed. 1980) (emphasizing that rules will not effectively limit information abuse and recommending that safeguards be built into the technological elements of the system instead of relying on human compliance with promulgated limitations).

165. *See* Diem, *supra* note 3, at 319; *cf.* Sherrer & Roston, *Some Legal and Psychological Concerns About Personality Testing in the Public Schools*, 30 FED. B.J. 111, 114 (1971) (children typically trust school personnel and will do whatever they are asked); Wolfe & Laufer, *supra* note 73. More specifically-focused research in schools experimenting with computer-assisted instruction could help to clarify this issue. *See generally* Caporael & Thorngate, *Introduction: Towards the Social Psychology of Computing*, J. SOC. ISSUES, Spring 1984, at 1.

Purpose of the testing or instruction; context in which it occurs; type of information recorded and generated; qualifications of the administrator; characteristics of the subject; use of any resulting records; and reliability and validity of the process.

To meet the evident need for specificity and technical expertise in creating an appropriate set of rules, the best approach would be to enact general legislation and grant authority to one or more administrative agencies to promulgate regulations and perhaps monitor compliance.[166] This has been the preferred approach in Canada and a number of European countries that have established data protection commissions with authority to particularize and enforce privacy laws.[167]

Although the European model of a comprehensive privacy protection commission that exercises jurisdiction across domains offers some advantages,[168] the same fear of totalitarianism that provides one of the strongest rationales for protecting privacy also counsels against centralizing the responsibility for regulation. Moreover, the existence in the United States of regulatory agencies with authority in related areas creates an opportunity to build upon established mechanisms rather than starting afresh.

To extend privacy protection comprehensively, parallel action is needed at the state level.[169] Federal legislation may serve as a model for states to build upon in adopting provisions governing CATI in the private sphere that is beyond federal regulation. In addition, states should be free to adopt measures that are more protective of individual privacy.

2. *Amending FERPA: A Model Approach*

For CATI in education, Congress could amend the Family Educational Rights and Privacy Act ("FERPA")[170] to include adequate

166. *See* Comment, *The Use and Abuse of Computerized Information: Striking a Balance Between Personal Privacy Interests and Organizational Information Needs,* 44 ALB. L. REV. 589, 615–18 (1980) (recommending creation of a data protection agency).

167. *See* Hondius, *Data Law in Europe,* 16 STAN. J. INT'L L. 87 (1980); Simitis, *supra* note 57.

168. Spiros Simitis, the data protection commissioner for the West German state of Hesse, points to total autonomy and insularity from the influence of other agencies with potentially inconsistent purposes as the chief advantage of the comprehensive independent agency approach. Simitis, *supra* note 57, at 742–46.

169. The importance of state legislation is emphasized in Everest, *Nonuniform Privacy Laws: Implications and Attempts at Uniformity,* in COMPUTERS AND PRIVACY IN THE NEXT DECADE 141 (L. Hoffman ed. 1980).

170. 20 U.S.C. § 1232g (1982).

standards. The FERPA Office within the Department of Education could be empowered to act as the implementing body.[171] Modifying the Act would require only a few simple amendments.

Currently, section (a) of the Act requires the Secretary of Education to withhold certain federal funds[172] from institutions that improperly deny record access to parents or students, and section (b) authorizes the same withholding of funds if an institution improperly releases student information to a third party.[173] Following the format of these provisions, a new section (c) might read:

No funds shall be made available under any applicable program to any educational agency or institution which has a policy or practice of either

(1) using computer-assisted processes to monitor students' performance continuously or without their consent or

(2) creating permanent education records[174] directly from students' interactions with a computerized device.

In addition, current section (e), which deals with notifying students and parents about their rights under the Act, could be amended to require that the notice include a description of computerized methods the institution uses to collect information about students and to explain how students may opt out of computerized monitoring.

These two changes should provide the Department of Education with a sufficient basis for developing specific regulations that could keep pace with evolving technologies. In particular, the regulations would need to elaborate on the meaning in subsection (c)(1) of "continuously" and the consent requirement. "Continuously" should be defined as applying to the period during which students are using their computers, i.e., students should be allowed substantial periods when monitoring will not occur. The consent provisions should include both

171. For the workplace, the equivalent statute probably would be the Occupational Safety and Health Act of 1970, Pub. L. No. 91-596, 84 Stat. 1590 (codified as amended in scattered titles of U.S.C.), with the OSHA Office given the associated administrative responsibilities. Alternatively or additionally, the Fair Labor Standards Act of 1938, ch. 676, 52 Stat. 1060 (codified as amended at 29 U.S.C. §§ 201–19) could be amended and the National Labor Relations Board designated as the administrative body.

172. All funds administered by the Department of Education are potentially at stake. *See* Privacy Rights of Parents and Students, 34 C.F.R. § 99.1 (1987).

173. For an explanation of FERPA's details, see 1 PRIVACY LAW AND PRACTICE § 6.03 (G. Trubow ed. 1987).

174. A satisfactory definition of "education records" exists in the regulations, 34 C.F.R. § 99.3 (1987) (elaborating 20 U.S.C. § 1232g(a)(4) (1982)). A definition of "permanent" would need to be added. "Permanent education records" here would refer to "records that will remain in existence beyond the current academic year or which will be used in an automated process to generate other records that will remain in existence beyond the current academic year."

an annual request for permission from the parent or student and a means by which the student in the course of daily affairs can deactivate the monitoring process. In combination with the formal notice required in section (e), the annual consent requirement will keep the citizenry informed of the extent of computer monitoring. The "electronic shield" part of the consent requirement will give students a measure of control over their privacy.

V. CONCLUSION

If CATI is not regulated, members of future generations who grow up with incessant computer monitoring may develop a very weak expectation of privacy against government surveillance. At the extreme, routinization of computerized privacy invasions may reduce resistance to a regime that abuses computer-based technologies to control the population.[175] Less cataclysmically, psychological distress may rise and the sense of individualism that has been a hallmark of the national character may diminish. As monitoring capabilities increase and privacy expectations decrease, the eerie vision of Pink Floyd's lyrics may approach reality.

> Welcome my son. Welcome to the machine.
> Where have you been? It's all right, we know where you've been.
> Welcome my son. Welcome to the machine.
> What have you dreamed? It's all right, we told you what to dream.[176]

Certainly such a specter is remote, yet eerily conceivable. Fifteen years ago Arthur Miller advised that

> [a]ny attempt to appraise the implications of the new information technologies should consider the potential psychological impact on our citizenry of the unchecked computerization and dissemination of personal data. But virtually nothing is known about the psychology of privacy and the ways in which contemporary information practices may affect us.[177]

---

175. The control might come from use of the collected information or from combining the information with other known data. *See* Simitis, *supra* note 57, at 714–18. Computers used in instruction and testing may someday have on file fairly comprehensive information regarding individuals' reinforcement preferences. During instruction, the computer would use this information to provide rewards or inform a teacher of strategies for behavioral management. One implication of amassing such information is that a repressive regime might use it as a basis for manipulating individual behavior. The prospect of manipulation of this type is considered in J. RULE, *supra* note 6, at 19–31.

176. Pink Floyd, *Welcome to the Machine,* on WISH YOU WERE HERE (CBS Records 1975). Pink Floyd's lyrical prophesy echoes the prosaic accounts of A. HUXLEY, BRAVE NEW WORLD (1932); G. ORWELL, 1984 (1948); and other foretellers of technology's dark side.

177. A. MILLER, *supra* note 6, at 47.

Since Miller made this observation, technological capabilities have expanded exponentially while our understanding of privacy, how CATI affects it, and the results for human well-being, have increased only slightly. At a minimum, our ignorance about the costs of privacy invasion suggests that we should proceed cautiously in adopting new technologies with tremendous potential for reducing privacy.

Time is growing short. If we are to seize the opportunity to shape the process rather than accept whatever its proponents deem acceptable, we must act soon. Acting preventively to restrict CATI while conducting empirical studies to support more informed policy-making is the best course.