Hastings Law Journal

Volume 35 | Issue 6 Article 4

1-1984

In the Shadow of 1984: National Identification Systems, Computer-Matching, and Privacy in the United States

John Shattuck

In the Shadow of *1984*: National Identification Systems, Computer-Matching, and Privacy in the United States

By JOHN SHATTUCK*

> There was of course no way of knowing whether you were being watched at any given moment . . . . It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live—did live, from habit that became instinct—in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized.[1]

The Diminishing Right of Privacy

The politics and technology represented in George Orwell's *1984* reduced to zero any reasonable expectation of privacy. In late 1984 several political and technological trends in the United States appeared to be driving toward the same result. In this Commentary I discuss the privacy implications of some current developments in the public and private sectors of American society.

Recent actions by the federal government have brought the technology of privacy invasion from the realm of science fiction into the world of public policy. For example, in August 1983 it was revealed that the Internal Revenue Service was planning to estimate the income of millions of American households, based upon a system of computerized information about "life styles." Such information would be used to identify persons who fail to pay or who underpay their taxes. The information would be compiled by private companies and purchased by the federal government.[2]

Another invasion of privacy is made possible by a White House

* Vice President, Harvard University; Director, American Civil Liberties Union, Washington Office, 1976-1984. B.A., 1965, Yale College; M.A., 1967, Cambridge University; LL.B., 1970, Yale Law School.

1. G. ORWELL, 1984, at 6-7 (1949).

2. N.Y. Times, Aug. 29, 1983, § 1, at 1, col. 3.

directive issued in March 1983, "Safeguarding National Security Information," which authorized all federal agencies using classified information to require employees to submit to lie detector tests "when appropriate," and to dismiss or to demote any employee who refuses to submit.[3] The directive eliminated any pretense that lie detectors will be used only on "volunteers," and has the potential of imposing what Senator Sam Ervin once called an instrument of "20th Century witchcraft"[4] on hundreds of thousands of federal employees.

In May 1983 the Justice Department implemented a proposal by the Secret Service to use the giant National Crime Information Center (NCIC), a computerized national network, for the dissemination of information about the non-criminal activities of persons under surveillance by the Secret Service. If the NCIC is used to disseminate non-criminal "intelligence" files, police in squad cars all over the country will have routine access on a daily basis to sensitive personal information.[5]

An additional source of privacy invasion is the increasing use over the last several years by the federal government of "computer-matching" investigations to detect fraud, abuse, and waste in the administration of federal programs. These computerized general searches of personal data have been conducted in the files of welfare and medicaid recipients, draft-aged taxpayers, veterans, federal employees, persons entitled to supplemental security income, and thousands of other government files.[6] The computer-matching technique is an effective way of combining personal data from a wide variety of separate record systems and using it to keep track of individuals.

Finally, for several years Congress has been considering a proposal to require all persons in the United States to carry a fraud-proof work authorization card in order to obtain and hold employment.[7] The card, backed by a national databank of personal information concern-

3. Safeguarding National Security Information, National Security Directive (Mar. 11, 1983) (copy on file with *Hastings Law Journal*). *See also* N.Y. Times, Mar. 12, 1983, § 1, at 1, col. 4.

4. 117 CONG. REC. 21,997, 22,004-06 (1971).

5. *See The United States Secret Service and Its Use of the National Crime Information Center: Hearings Before the Subcomm. on Civil and Constitutional Rights of the House Comm. on the Judiciary*, 98th Cong., 1st Sess. 27, 43-45 (1983).

6. *Oversight of Computer Matching to Detect Fraud and Mismanagement in Government Programs: Hearings Before the Subcomm. on Oversight of Government Management of the Senate Comm. on Governmental Affairs*, 97th Cong., 2d Sess. 1-76 (1982) [hereinafter cited as *Hearings*].

7. S. 529 & H.R. 1510, 98th Cong., 1st Sess. (1983). *See infra* notes 47-55 & accompanying text.

ing all persons lawfully in the United States, would constitute a secure national identification system that could block the employment of illegal aliens. The proposal has sparked controversy because the identification system could become a vehicle for the violation of civil rights if used by the police to conduct wide-ranging searches and investigations or by other government agencies to keep track of private, law-abiding citizens.[8]

These examples demonstrate that the technological capability to collect, maintain, cross-index, and disclose vast quantities of information about private lives has far outpaced the legal protection of privacy in the United States. Many information systems containing sensitive data are being constructed to facilitate important social objectives, such as better law enforcement, faster delivery of public services, more efficient management of credit and insurance programs, improvement of telecommunications, and streamlining of financial activities. Nonetheless, these high technology systems are also being used at an increasing rate by large public and private agencies to enhance their control of the lives of individuals.

In recent years the private sector has rapidly increased its use of such technology. For example, interactive cable television systems are capable of gathering vast amounts of personal data, not only on the viewing habits of consumers, but also on their buying and banking habits, as more services are added to the cable system. Cable companies, for example, will soon offer burglar alarm systems which will tell the company when a consumer is at home. This sensitive personal information is a valuable commodity which cable companies can sell to credit reporting companies and other interested buyers in order to finance their corporate growth.[9]

Private companies as well as the federal government often require employees to submit to lie detector tests. Employees have no clear understanding of what rights, if any, they have to refuse to take a test, or to control the verification, storage, and dissemination of records generated by a test if they submit to it.[10]

The technology for information collection, storage, and retrieval has outpaced the technology for safeguarding databanks of personal information. Stories are legion about the fifteen year old computer

8. STAFF OF COMMITTEES ON THE JUDICIARY, 97TH CONG., 1ST SESS., U.S. IMMIGRATION POLICY AND THE NATIONAL INTEREST 343-55, 357-64 (Joint Comm. Print 1981).

9. See the proposed privacy protections in S. 66, 98th Cong., 1st Sess., § 610 (1983).

10. *See* T. Hayden, Lie Detectors and Employment, Report for the New York Civil Liberties Union (June 1981).

wizard who can crack the most secure computer system. Computer security is largely unregulated, and the penalties for stealing personal data are unclear.[11]

All of these developments have an impact on the lives of real people. Several examples from the files of the American Civil Liberties Union reveal the Kafkaesque problems that may result from the unregulated use of personal information:

> In New Orleans, a mother on welfare was arrested and jailed for eighteen hours on the basis of an inaccurate crime report resulting from programming errors in police computers. She has sued the police department for false arrest and for failing to audit their computerized files for erroneous information.[12]
>
> In New York, a middle-aged man was denied a license to drive a taxi because a computerized credit report showed that when he was thirteen years old in Massachusetts he temporarily had been placed in a mental institution. What the files did not show was that he was an orphan and the institution was the only home the state authorities could find for him for a period of four years.[13]
>
> In Massachusetts, the medicaid benefits of an elderly woman in a nursing home were ordered terminated after a computer-match of welfare rolls and bank accounts in the state revealed that she had an account above the medicaid assets limit. The termination order was improper because the woman's bank account contained a certificate of deposit in trust for a local funeral director, to be used for her funeral expenses, an exempt resource under federal regulations. The computer-match did not reveal this fact.[14]
>
> In Akron, Ohio, five employees of a clothing store were dismissed after they were forced to take a psychological stress evaluation test. Following the dismissals the employer spread reports that the test proved that the employees had been stealing, although none were ever charged with theft. These reports sharply curtailed further employment opportunities for them.[15]

The American public is concerned about these developments. The results of a nationwide poll indicated that in 1979 thirty-three percent of the public believed that the United States was "very close" or "somewhat close" to becoming the kind of society "in which the gov-

11. SUBCOMM. ON TRANSPORTATION, AVIATION AND MATERIALS OF THE HOUSE COMM. ON SCIENCE AND TECHNOLOGY, 98TH CONG., 2D SESS., COMPUTER AND COMMUNICATIONS SECURITY AND PRIVACY 17-19, 24-27 (Comm. Print 1984). *See also Youths at Home Tap Nuclear Lab Computer*, L.A. Times, Aug. 12, 1983, § I, at 5, col. 1.

12. Documents on file at American Civil Liberties Union of Louisiana, New Orleans, Louisiana.

13. A. NEIER, DOSSIER 73-74 (1975).

14. *Hearings*, *supra* note 6, at 80 (testimony of John Shattuck, Nat'l Legis. Dir., ACLU).

15. T. Hayden, *supra* note 10.

ernment knows almost everything about everyone."[16] Two-thirds of those polled expressed concern that government agencies, such as the Internal Revenue Service, and private organizations, such as finance companies, were violating their privacy.[17]

Privacy Protection in the United States: A Brief Review of the Last Two Decades

The constitutional problem concerning the protection of privacy is the difficulty of applying the principles of an eighteenth-century document, the Bill of Rights, to late twentieth-century life. The fourth amendment to the Constitution was adopted to protect "persons, houses, papers and effects" against unreasonable search and seizure by the government. Massive collection and dissemination of sensitive personal information by private entities was unimagined at that time because personal information was difficult to collect and files were handwritten, rarely reproduced, and easily lost.[18] Furthermore, the fourth amendment generally limited government intrusion to situations involving criminal investigations.

Today, the capacity to collect and to preserve information has been radically altered by the relentless growth of an information technology that permits virtually unlimited permanent storage and retrieval of personal information. Most personal information is now maintained outside the home and therefore generally falls outside fourth amendment protection.[19] Individuals have almost no dominion over such information. They cannot prevent it from being collected; they often have no access to it and thus cannot challenge its accuracy; and they cannot prevent its dissemination. As a result, what once was gossip today may become part of the permanent record.

Over the last two decades, efforts in the United States to secure the right of personal privacy against modern information practices have resulted in a string of fragile and generally short-lived victories. Although the growth of information technology and the corresponding pressure to make use of that technology have created an increased public awareness of privacy issues, few effective limitations have been imposed on intrusive governmental or commercial information practices.

Several of the major legislative and judicial developments con-

16. Burnham, *Poll Finds Increasing Concern Over Threats to Privacy*, N.Y. Times, May 4, 1979, at A19, col. 1.

17. *Id.*

18. J. SHATTUCK, RIGHTS OF PRIVACY 4-5 (1977).

19. *See Hearings*, *supra* note 6, at 151-56 (testimony of Ronald Plesser).

cerning privacy have compromised privacy interests while appearing to protect them. For example, a successful battle in Congress against the creation of a comprehensive national databank in the mid-1960's fostered the growth of a separate personal data system for each federal agency.[20] Information that had been collected for one purpose could not be used for another purpose. Ultimately, however, as more federal agencies computerized their records, they informally began to share and to exchange personal information.[21] The increasing use by many agencies of the social security number, originally intended to be used solely in administering the social security system, made cross-indexing among various systems relatively easy. The merger of these apparently separate personal record systems has therefore become possible without the creation of physically centralized records. Today, unregulated computer-matching at all levels of government has created a *de facto* national databank.

Similarly, two United States Supreme Court decisions in 1967[22] sustaining constitutional challenges to warrantless bugging and wiretapping quickly led to the enactment in 1968 of a federal statute authorizing various forms of electronic surveillance.[23] In addition, a proposal for strict procedural controls over the maintenance and dissemination of arrest records—suggested in 1969 by Project Search, a pilot study of the Justice Department's Law Enforcement Assistance Administration—was shelved as a result of a persistent campaign waged by the FBI to create a National Crime Information Center in the early 1970's.[24]

Short-lived victories for privacy have occurred in the private sector as well. In 1970 the Fair Credit Reporting Act[25] was proposed as a result of a strong effort by consumer and civil rights organizations to regulate the collection and dissemination of information by the credit reporting industry.[26] The Act ratified by Congress, however, was considerably weakened by amendments drafted primarily by the credit re-

20. *See* D. BURNHAM, THE RISE OF THE COMPUTER STATE 189 (1983); *see also* A. MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS 204-05 (1971); A. WESTIN & M. BAKER, DATABANKS IN A FREE SOCIETY: COMPUTERS, RECORD KEEPING, AND PRIVACY 3-4, 14-20 (1972).

21. *See generally* D. BURNHAM, *supra* note 20, at 105.

22. Berger v. New York, 388 U.S. 41 (1967); Katz v. United States, 389 U.S. 347 (1967).

23. Omnibus Crime Control and Safe Streets Act of 1968, 82 Stat. 212-23 (current version at 18 U.S.C. §§ 2510-2520 (1982)).

24. D. BURNHAM, *supra* note 20, at 67-69.

25. 84 Stat. 1128-36 (current version at 15 U.S.C. §§ 1681a-1681t (1982)).

26. *Fair Credit Reporting: Hearings on S. 823 Before the Subcomm. on Financial Institutions of the Comm. on Banking and Currency*, 91st Cong., 1st Sess. (1969).

porting industry.[27]

In the post-Watergate era, efforts to ensure the confidentiality of personal information have gained support in Congress, but have lost it in the courts. The Supreme Court, in particular, has generally declined to adapt the protections of the fourth amendment to modern conditions and has failed to construct a constitutional basis for the protection of personal privacy.[28]

As part of the Privacy Act of 1974,[29] Congress created a Privacy Protection Study Commission, which issued a report in 1977 calling for a variety of legislative initiatives.[30] In 1976 Congress reacted to the Supreme Court's refusal to recognize a constitutional right to the privacy of financial information kept by third parties, particularly banks,[31] by enacting a provision of the Tax Reform Act limiting access to such information by Internal Revenue Service agents.[32] In 1978 the Right to Financial Privacy Act[33] extended the same limitations to all federal investigations, but added a provision giving agencies the power to make investigative demands for financial records.[34] At the same time, Congress extended the wiretap provisions of the 1968 Omnibus Crime Control and Safe Streets Act by requiring a warrant from a special court even for electronic surveillance designed to obtain foreign intelligence information.[35] In 1980 Congress enacted the Privacy Protection Act, setting forth a ban on police searches of newsrooms in the course of investigations in which journalists are suspected of possessing information about crimes committed by others.[36] The same year Congress narrowly defeated other legislation that ensured the confidentiality of medical records.[37]

Since 1980, however, efforts to initiate privacy legislation in the Congress have been thwarted by the Reagan Administration. The Office of Management and Budget, whose director is appointed by the President, has failed to fulfill its mandate under the Paperwork Reduc-

27. 115 CONG. REC. 33,410 (1969).

28. *See generally* J. SHATTUCK, *supra* note 18, at 145-94.

29. 5 U.S.C. § 552a (1982).

30. Privacy Protection Study Commission, Personal Privacy in an Information Society (July 1977).

31. United States v. Miller, 425 U.S. 435 (1976).

32. 90 Stat. 1667 (current version at 26 U.S.C. § 6103 (1982)).

33. 92 Stat. 3697-3710 (current version at 12 U.S.C. §§ 3401-3422 (1982)).

34. 12 U.S.C. § 3405 (1982).

35. Foreign Intelligence Surveillance Act of 1978, 92 Stat. 1783-96 (current version at 50 U.S.C. §§ 1801-1811 (1982)).

36. 94 Stat. 1879-83 (current version at 42 U.S.C. 2000aa-2000aa-12 (1982)).

37. S. 865 & H.R. 3444, 96th Cong, 2d Sess. (1980).

tion Act to propose legislation for the supervision of agency procedures in this area.[38] The Administration's aggressive and unrestricted use of lie detector testing, computer-matching, and federal undercover operations is symptomatic of its attitude toward privacy.[39] In its first two years the Reagan Administration persuaded Congress to loosen the privacy protections of individual tax returns held by the IRS and to open the files of persons in debt to the federal government to credit reporting companies.[40] The Administration also broadened the authority of the CIA and the FBI to spy on the lawful activities of Americans,[41] sharply curtailed enforcement of the Privacy Act inside the federal government,[42] and emasculated the one federal agency charged with developing privacy protections inside the federal government, the National Telecommunications and Information Administration.[43]

The level of privacy protection in the United States today is perhaps best evidenced by the recent action of the Council of Europe requesting that the United States create legal safeguards for personal data or face the prospect of restrictions by European nations on the flow of such information into the United States.[44] Ignoring this warning, the Reagan Administration asserted in March 1983 that the American legal structure provides adequate safeguards for the protection of personal privacy.[45]

Toward a National Identification System

There is perhaps no better example of the encroachment on the rights of privacy and anonymity in the United States than the proposal to establish a computerized national identification system. This proposal has been put forward as part of the effort to restrict immigration into the United States.[46] In order to accomplish this objective, it is argued, the United States must implement a comprehensive work-eligibility verification system which would require employees to provide

38. *See* H.R. REP. No. 455, 98th Cong., 1st Sess. 27-28 (1983).

39. D. BURNHAM, *supra* note 20, at 180-82, 211-13.

40. N.Y. Times, Apr. 8, 1984, § 1, at 23.

41. Exec. Order No. 12,333, 3 C.F.R. 200 (1981).

42. Kirchner, *A History of Computer Matching in the Federal Government*, COMPUTERWORLD, Dec. 14, 1981, In Depth, at 15.

43. *See* H.R. REP. No. 455, *supra* note 38.

44. *See* N.Y. Times, Mar. 13, 1983, § 3, at 1, col. 3.

45. *See* Boston Globe, Mar. 13, 1983, § 1, at 45.

46. S. 529, 98th Cong., 2d Sess. § 274A (1984).

documentation of their eligibility to work in the United States.[47]

The development of a national identification system can be approached in two different ways. The first approach is to create a counterfeit-resistant identity document, such as an improved version of the social security card.[48] Such a document would contain the bearer's photograph, signature, perhaps other identifying data, and a code indicating citizen or alien status, all verified by information in government computers. A second approach would dispense with the identity document, relying instead on a government databank of personal information filed under individual social security numbers. Employers would submit a form on each person they seek to employ, which the government would compare with the records in the databank.[49]

How would these identification systems threaten civil liberties? The greatest danger of any mandatory identity document is that it tends to become a form of domestic passport. Certainly no one intends this result, and proponents of the identity card believe that they can take steps to prevent it.[50] What they do not realize, however, is that the government's police powers to stop and search are already sufficient to transform the identity document into a major threat to privacy and freedom of movement.

A review of two Supreme Court decisions of the last decade illustrates the point. In 1973 the Court ruled that an officer arresting a motorist for driving without a license may search both the driver and the car without a warrant.[51] In both cases the search was precipitated by the driver's failure to carry a valid license. Although five years later the Court struck down random spot checks of drivers' licenses,[52] it qualified this holding by distinguishing random searches from searches conducted at the borders or at specific checkpoints within the country.[53] In these cases the Court defined the police power as allowing government agents to stop people without any particular suspicion of a crime, to request identification, and to search, detain, or arrest people

47. STAFF OF COMMITTEES ON THE JUDICIARY, 97TH CONG., 1ST SESS., U.S. IMMIGRATION POLICY AND THE NATIONAL INTEREST 66-69 (Joint Comm. Print 1981).

48. *Id.* at 68.

49. *Id.*

50. *See* S. 529, 98th Cong., 2d Sess. § C-G (1984) (barring use of national identification system for purposes other than immigration control).

51. United States v. Robinson, 414 U.S. 218 (1973); Gustafson v. Florida, 414 U.S. 260 (1973).

52. Delaware v. Prouse, 440 U.S. 648 (1978).

53. *Id.* at 663.

who cannot produce proper documents.[54] Thus, because the police powers to stop and question people and to check identification are already very broad, a national identity document would serve as a blanket invitation for the police to exercise these powers frequently and to their fullest extent in the name of immigration control but at the expense of civil liberties.

The alternative suggestion, a databank *without* an identity card, also has the potential to be abused. If such a databank is to serve as a reliable means of checking employment eligibility, it must contain current and verified personal information on each person authorized to work. In addition to the social security number and other items commonly used to establish identity, this information would probably include a physical description such as height, coloring, and race, perhaps some unique identifier such as a signature or photograph or even fingerprints, and a notation of status as a citizen or alien with permission to work.

The history of computerized data systems over the last decade shows one clear trend: they have always been adapted to purposes other than their originally intended use. There are dozens of examples of new uses for once-restricted personal data systems:[55]

> Social Security Administration files are now used routinely to identify "illegal aliens."
>
> The federal Parent Locator Service allows child support enforcement officials to search virtually all government and private record systems in order to trace absent parents who owe child support.
>
> Numerous state laws allow or actually require public and private employers to use criminal history databanks, compiled originally for police use, in order to screen out applicants convicted of certain crimes, or simply to ascertain if applicants have arrest records.
>
> Internal Revenue Service records are now used to screen prospective jurors and to locate non-registrants for the draft.
>
> The records of hundreds of federal and state public assistance programs have been matched against each other and against public and private employment rolls, to identify people receiving multiple benefits or benefits for which they are ineligible because of their earnings.

Although the expanded uses of personal data cited above are for purposes that most people would find rational and even commendable,

54. *See, e.g.*, Delaware v. Prouse, 440 U.S. 648, 663 (1978).

55. *See The Social Security Number as a Universal Identifier: Hearings Before the Subcomm. on Social Security of the House Comm. on Ways and Means*, 97th Cong., 2d Sess. 96-123 (1982) (statement of John Shattuck, Nat'l Legis. Dir., ACLU).

the examples demonstrate that personal data systems often are adapted to a wide variety of purposes beyond their originally intended uses.

A national identification system established to enforce the immigration laws is likely to follow the same course. A system set up to determine eligibility for employment on grounds of citizenship or alien status could easily be adapted, for example, to implement a law restricting the employment of convicted felons for certain kinds of jobs; such convictions could simply be coded into the system's database. The identification system could also be useful in efforts to combat welfare fraud. If the database were expanded to include a notation of status as a welfare recipient, then the databank could automatically identify any welfare recipients who obtain employment and notify the appropriate welfare agency to cut off benefits. If the system included identifiers such as photographs, it could be used, for example, to identify nuclear freeze demonstrators or members of supposed communist-front organizations.

In sum, a national identification system for controlling immigration could quickly become a major instrument for tracking and controlling the private lives of millions of citizens.

Computer-Matching: High-Tech Invasion of Privacy

A national identification system may or may not be adopted in the United States. However, a similar concept, computer-matching—the use of unrelated computer tapes of massive numbers of personal files to conduct government or corporate investigations—has arrived. To understand the impact of computer-matching on civil liberties, it is necessary to grasp the profound difference between a computer-match investigation and a traditional law enforcement investigation.

A traditional investigation is triggered by some evidence that the person targeted has engaged in wrongdoing. The limited resources of law enforcement usually make it impracticable to conduct dragnet investigations. Moreover, the American constitutional system generally bars the government from conducting intrusive investigations of persons it does not suspect of wrongdoing.[56]

A computer-match is not bound by these limitations. It is directed not at an individual, but at an entire category of persons, not because any of them is suspected of misconduct, but because the category is of interest to the government. What makes computer-matching so fundamentally different from a traditional investigation is that its purpose is

56. *See generally* J. SHATTUCK, *supra* note 18, at 1-45.

to generate the evidence of wrongdoing that usually is required before a traditional investigation can be initiated. That evidence is produced by "matching" two sets of personal records compiled for wholly unrelated purposes.

The impact of a computer-match on civil liberties differs in at least four ways from that of a conventional law enforcement investigation. The first difference is its impact on fourth amendment rights. The fourth amendment protects against unreasonable searches and seizures, the most blatant of which have been fishing expeditions directed at large numbers of people on the chance that something will turn up. From the royal writs of assistance used in the eighteenth century for the enforcement of oppressive British tax and tariff laws[57] to the municipal code inspections used today for the enforcement of health and safety standards,[58] American law has firmly held to the principle that generalized fishing expeditions violate the right to be free from unreasonable searches and seizures. Although searches of personal records are not physically intrusive, as are door-to-door searches of houses, the result is the same: a massive investigation using private information about huge numbers of people.

That brings us to a second principle of individual rights that is squarely at odds with computer-matching. Generally, people in the United States are not forced to bear a continuous burden of demonstrating to the government that they are innocent of wrongdoing.[59] Although people are obliged to obey the law, the presumption of innocence is intended to protect them against having to prove that they are free from guilt whenever the government chooses to investigate them.

Computer-matching can turn the presumption of innocence into a presumption of guilt. In Massachusetts thousands of welfare recipients were summarily removed from the state welfare rolls in 1982 due to a computer-match of welfare records with bank accounts in the state, and many had to fight for reinstatement based on information the state neglected to take into account after their names appeared as "hits" in the match.[60] A similarly striking example of this "presumption of guilt" occurred four years ago in Florida, when the state's attorney for the

57. J. SHATTUCK, *supra* note 18, at 3.

58. Camara v. Municipal Court, 387 U.S. 523 (1967). *See also* J. SHATTUCK, *supra* note 18, at 31.

59. The presumption of innocence is a fundamental element of Anglo-American criminal law and procedure. *See* J. GORA, DUE PROCESS OF LAW 1-15 (1977).

60. *Hearings*, *supra* note 6, at 78, 80, 83 (testimony of John Shattuck, Nat'l Legis. Dir., ACLU).

Jacksonville area obtained the case files for all food-stamp recipients in the area and then launched fraud investigations against those who had received allotments of $125 or more per month. A federal court of appeals invalidated the file search and enjoined the investigation on the ground that the food-stamp recipients were put in the impossible and unfair position of having to prove that the food-stamps they had received were not obtained by fraud.[61]

The third way in which computer-matching erodes civil liberties involves the most important principle governing the collection and use of personal information by the government: the individual has a right to control information about himself and to prevent its use without his consent for purposes unrelated to those for which it was collected. This principle is embodied in the Privacy Act of 1974.[62] The Privacy Act restricts disclosure by federal agencies of personally identifiable information, unless the subject consents. A major exception to this rule is disclosure for a "routine use," which is defined as "the use of [a] record for a purpose which is compatible with the purpose for which it was collected."[63]

When computer-matching was in its infancy at the federal level, the Privacy Act was correctly perceived by several federal agencies to be a major stumbling block. Thus, in 1977 the Civil Service Commission balked at the plans of Joseph Califano, Secretary of Health, Education and Welfare in the Carter Administration, to institute a match of federal employee records and state welfare rolls, on the ground that the use of employee records for such a purpose would violate the Privacy Act.[64] But this assessment of the Privacy Act soon gave way to a succession of strained administrative interpretations by agencies seeking to square computer-matching with the Act's prohibition of the use of personal records unless the purpose is compatible with that for which they were collected.[65] Because enforcement of the Privacy Act is left almost entirely to the federal agencies themselves, it is hardly surprising that they have bent the Act to their own purposes and have now miraculously established that any computer-matching is a "routine use" of personal records.[66] All that is required to satisfy the policy of the Act, the agencies say, is to publish each new computer-matching "routine

61. Roberts v. Austin, 632 F.2d 1202 (5th Cir. 1980), *cert. denied*, 454 U.S. 975 (1981).
62. 5 U.S.C. § 552a (1982).
63. *Id.* § 552a(a)(7).
64. *Hearings, supra* note 6, at 122 (letter from Charles Goodman, Gen. Counsel, U.S. Civil Service Comm'n, to Charles Ruff, Acting Deputy Inspector Gen., HEW).
65. *See Hearings, supra* note 6, at 104.
66. Kirchner, *supra* note 42, at 15.

use" in the *Federal Register*.[67] Thus, the safeguards of the Privacy Act have been effectively eroded.

The final civil liberties issue raised by computer-matching involves due process of law. Once a match has taken place it results in a series of "raw hits." At this point all persons identified as "hits" are in jeopardy of being found guilty of wrongdoing. To the extent that they are not given notice of their situation and an adequate opportunity to contest the results of the match, they are denied due process of law.[68]

Precisely this result has occurred in several of the best known matching programs conducted to date. The results of Secretary Califano's Project Match were kept secret from the federal employees whose records were matched with welfare rolls, because the Justice Department viewed the investigation as "a law enforcement program, designed to detect suspected violations of various criminal statutes."[69] For this reason the Department ordered the Civil Service Commission not to notify any of the federal employees whose names showed up as "hits," since "[t]he premature discussion of a specific criminal matter with a putative defendant is in our view inimical to the building of a solid prosecutorial case."[70] In Massachusetts the welfare authorities went one step further by terminating benefits of persons showing up as "hits" without even conducting an *internal* investigation of the accuracy of the computer-match results.[71]

Conclusion

Franz Kafka would feel quite at home in the world of computer-matching, national identification systems, and other technological and bureaucratic instruments of privacy invasion that are coming into use in the United States. The growing public interest in regulating these new technologies to protect the integrity of the individual may exert political pressure to check this disturbing trend. In this respect the words of those who drafted the Privacy Act of 1974 provide both a warning and a hope:

> [I]f one reads Orwell . . . carefully, one realizes that "1984" is a state of mind. In the past, dictatorships always have come with hobnailed

67. *Id.*

68. *See, e.g.,* Goldberg v. Kelly, 397 U.S. 254 (1969) (welfare recipients are entitled to notice and hearing before termination of benefits).

69. Hendricks, *How Not to Catch Welfare Cheaters*, Washington Post, July 1, 1979, § C, at 8, col. 1. *See also* Kirchner, *supra* note 42, at 7, 10.

70. Letter from Benjamin Civiletti, Asst. Attorney Gen., to Raymond Jacobson, Civil Service Comm'n Exec. Dir. (October 7, 1977). *See* Kirchner, *supra* note 42, at 10.

71. *Hearings, supra* note 6, at 129-39 (affidavit of Allan G. Rodgers).

boots and tanks and machineguns, but a dictatorship of dossiers, a dictatorship of data banks can be just as repressive, just as chilling and just as debilitating [to] our constitutional protections.[72]

72. S. REP. No. 1183, 93d Cong., 2d Sess. 7 (1974).