REVIEWING PRIVACY IN AN INFORMATION SOCIETY*

SPIROS SIMITIS†

I. THE QUEST FOR A CONCEPT

Privacy is an old and venerable subject.[1] Generations of lawyers, judges, and legal scholars have explored its different aspects. The number of cases is countless, the list of statutes long and impressive.[2] Yet,

---

* Originally delivered as the second Thomas Jefferson Lecture at the University of Pennsylvania Law School on October 28, 1985.

The University of Pennsylvania Law Review would like to thank Hermann Knott and Franz Tepper, 1987 LL.M. candidates at the University of Pennsylvania Law School, for reviewing most of the German language material cited in this article.

† Professor of Civil and Labor Law, Johann Wolfgang Goethe-Universität, Frankfurt am Main; Data Protection Commissioner, State of Hesse, Federal Republic of Germany.

[1] *See, e.g.,* Griswold v. Connecticut, 381 U.S. 479 (1965) (identifying zones of individual privacy guaranteed by the United States Constitution); Millar v. Taylor, 98 Eng. Rep. 201, 242 (K.B. 1769) ("It is certain every man has a right to keep his own sentiments, if he pleases: he has certainly a right to judge whether he will make them public, or commit them only to the sight of his friends."); B. MOORE, PRIVACY: STUDIES IN SOCIAL AND CULTURAL HISTORY (1984) (examining the concepts of public and private in various societies including 4th century B.C. Athens, ancient Hebrew society as reflected in the Old Testament, and ancient China at the age of the "hundred philosophers," 551 B.C. to 233 B.C.). *See generally* Warren & Brandeis, *The Right to Privacy,* 4 HARV. L. REV. 193 (1890) (tracing the development of protection for the individual's person and property and advocating recognition of the right to privacy and of remedies for its violation).

[2] In American law, recent discussion of the individual's right to privacy has arisen in cases involving sexual and reproductive matters, *see, e.g.,* Bowers v. Hardwick, 106 S. Ct. 2841 (1986); Roe v. Wade, 410 U.S. 113 (1973), and in cases concerning collection or disclosure of information, *see, e.g.,* Department of State v. Washington Post Co., 456 U.S. 595 (1982); Nixon v. Administrator of Gen. Servs., 433 U.S. 425 (1977); Whalen v. Roe, 429 U.S. 589 (1977); United States v. Miller, 425 U.S. 435 (1976); Department of the Air Force v. Rose, 425 U.S. 352 (1976). Other cases have involved the individual's right as to personal appearance, Kelley v. Johnson, 425 U.S. 238 (1976), as well as the right of privacy with regard to publicity upon arrest, Paul v. Davis, 424 U.S. 693 (1976), with both cases illustrating the tendency to restrict privacy to family, sexual, and reproductive matters. As to the individual's right of privacy in the context of criminal investigation, "[c]ases are legion that condemn violent searches and invasions of an individual's right to the privacy of his dwelling." *Miller,* 425 U.S. at 451 (Brennan, J., dissenting) (quoting Burrows v. Superior Court, 13 Cal. 3d 238, 247, 529 P.2d 590, 596, 118 Cal. Rptr. 166, 172 (1974)).

As to statutes, *see, e.g.,* Freedom of Information Act, 5 U.S.C. § 552 (1982), *amended by* 4 U.S.C. § 402(2) (Supp. III 1985 & West Supp. 1986); Privacy Act of 1974, 5 U.S.C. § 552a (1982), *amended by* 1 U.S.C. § 107(9) (Supp. III 1985 & West Supp. 1986); Privacy Act, B.C. Stat. ch. 39 (1968) (British Columbia); CODE CIVIL [C. CIV.] art. 9 (Fr.); Loi relative à l'informatique, aux fichiers et aux libertés, Loi No. 78-17 of 6 January 1978, 1978 Journal Officiel de la République Française [J.O.] 227,

"privacy research" was recently described as being in "hopeless disarray"[3] and the whole debate characterized as "ultimately, futile."[4] Indeed, the more the need for a convincing definition of privacy based on criteria free of inconsistencies has been stressed, the more abstract the language has grown.

Rather than looking to the specific societal, political, and economic factors triggering the controversy, commentators (and courts) have constantly invoked notions of rights, natural or otherwise,[5] "fundamental values,"[6] or "human dignity"[7] to determine the meaning and extent of the right of privacy. Even where an apparently far more earthy approach, such as economic analysis, is chosen,[8] the degree of abstraction

---

1978 Bulletin législatif Dalloz [B.L.D.] 77 (Fr.) (French data protection law); SCHWEIZERISCHES ZIVILGESETZBUCH [ZGB] art. 28 (Switz.); Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz), Jan. 27, 1977, 1977 Bundesgesetzblatt [BGBl] I 201 [hereinafter BDSG] (West German data protection law); *see also* REPORT OF THE COMMITTEE ON PRIVACY (1972) (Younger Committee) (U.K.).

[3] *See* Parent, *Recent Work on the Concept of Privacy,* 20 AM. PHIL. Q. 341, 341 (1983).

[4] *See* Wacks, *The Poverty of "Privacy,"* 96 L.Q. REV. 73, 76-77 (1980).

[5] *See, e.g.,* Negley, *Philosophical Views on the Value of Privacy,* 31 LAW & CONTEMP. PROBS. 319, 319-20 (1966) (asserting that past efforts of moralists to establish a value judgment on the moral options of the individual led them to discuss privacy as a "natural right," a view rejected by modern thinkers).

[6] *See, e.g.,* Moore v. City of E. Cleveland, 431 U.S. 494, 503-05 (1977) (stating that the sanctity of the family is protected because it is a basic value, a part of the nation's history and traditions); Roe v. Wade, 410 U.S. 113, 152-53 (1973) (stating that the right of privacy found to exist under the Constitution includes fundamental personal rights relating to marriage, procreation, contraception, family relationships, child rearing, and education).

[7] *See, e.g.,* Judgment of Apr. 2, 1957, 24 Bundesgerichtshof in Zivilsachen [BGHZ] 76 (W. Ger.) (referring to both human dignity and the constitutional right for free development of the individual's personality as the origin of the privacy right); Schacht case, 13 BGHZ 334 (1954) (invoking the constitutional right of respect for human dignity as basis of the privacy right); P. PERLINGIERI, LA PERSONALITÀ UMANA NELL'ORDINAMENTO GIURIDICO 14 (1972) (The Italian constitution, recognizing that the individual can only develop as a part of the community, places respect for individual human dignity on a par with the life of the community, not subordinate to it.); Bloustein, *Group Privacy: The Right to Huddle,* 8 RUT.-CAM. L.J. 219, 278 (1977) ("The right to be let alone protects the integrity and the dignity of the individual."); Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser,* 39 N.Y.U. L. REV. 962, 1000-07 (1964) (arguing that "all of the tort privacy cases involve the same interest in preserving human dignity and individuality").

[8] *See, e.g.,* Posner, *The Right of Privacy,* 12 GA. L. REV. 393 (1978) (suggesting that privacy and prying are intermediate economic goods used only to acquire other final goods or utility); Epstein, *Privacy, Property Rights, and Misrepresentations,* 12 GA. L. REV. 455 (1978) (a response to Posner, arguing that Posner's conclusions about privacy based on economic analysis could be more firmly grounded in traditional tort theories, although admitting that privacy is a value that cannot be obtained "solely as of legal right"); Posner, *Privacy, Secrecy, and Reputation,* 28 BUFFALO L. REV. 1 (1979) (1978 James McCormick Mitchell lecture) (continuing the economic analysis of privacy and extending it to address seclusion of the individual, defamation, and the role of

remains considerable. Consequently, the boundary between a permissible exchange of facts about people, necessary to avoid misrepresentation, and an impermissible intrusion and surveillance is entirely unclear.[9] Whether, for example, credit reports, medical records, personnel information systems, social security data bases, police files, or subscriber profiles established in connection with interactive cable television services are legitimate sources of information cannot be decided by simply pointing to the impact of misrepresentation on economic efficiency and hence at the corrective function of prying. The answer depends essentially on the particular purposes of each data collection as well as on the mode of the information process and the potential implications of the data use for the persons under scrutiny.

The increased access to personal information resulting from modern, sophisticated techniques of automated processing has sharpened the need to abandon the search for a "neutral" concept[10] in favor of an understanding free of abstractions and fully aware of the political and societal background of all privacy debates.[11] Modern forms of data collection have altered the privacy discussion in three principal ways. First, privacy considerations no longer arise out of particular individual problems; rather, they express conflicts affecting everyone. The course of the privacy debate is neither determined by the caricature of a prominent golfer with a chocolate packet protruding out of his pocket,[12] nor by the hints at the use of a sexual stimulant by a respected university

---

government as invader of the privacy of its citizens).

[9] *See* Posner, *The Right of Privacy, supra* note 8, at 394-406.

[10] *See* Gavison, *Privacy and the Limits of Law,* 89 YALE L.J. 421, 423, 425-28 (1980) (arguing for a neutral concept of privacy that would facilitate both clear identification of losses of privacy and intelligible discussions of privacy and claims thereto).

[11] For a critical approach, see S. RODOTÀ, ELABORATORI ELETTRONICI E CONTROLLO SOCIALE 27-33, 125-32 (1973) (presenting a history of the privacy right and discussing both unitary and multifaceted conceptualizations of privacy); J. RULE, D. MCADAM, L. STEARNS & D. UGLOW, THE POLITICS OF PRIVACY 21-24 (1980) (suggesting a global definition of privacy as "the restriction of others' access to information about oneself" to encompass both aesthetic privacy, restriction of personal information as an end in itself, and strategic privacy, restriction of such information as a means to some other end); Rodotà, *Verletzlichkeit des Individuums und der Gesellschaft,* in 1984 UND DANACH: DIE GESELLSCHAFTLICHE HERAUSFORDERUNG DER INFORMATIONSTECHNIK 194, 199-204 (1984) [hereinafter 1984 UND DANACH] (Internationale Konferenz der Regierung der Bundesrepublik Deutschland und des Senats von Berlin in Zusammenarbeit mit der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung, Berlin, Nov. 28-30, 1984) (favoring a data protection policy based not only on statutory regulation but also on private rules created by the industries concerned, e.g., the Warner Code of Privacy).

[12] *See* Tolley v. J.S. Fry & Sons, Ltd., 100 L.J.K.B. 328 (1931). In this action for libel, the plaintiff, an amateur golfer, objected to the defendant's use of his (plaintiff's) picture in an advertisement for the defendant's chocolate candy. The plaintiff claimed that the advertisement "prostituted his reputation" and invaded his privacy.

professor,[13] but by the intensive retrieval of personal data of virtually every employee, taxpayer, patient, bank customer, welfare recipient, or car driver. Second, smart cards[14] and videotex[15] make it possible to record and reconstruct individual activities in minute detail. Surveillance has thereby lost its exceptional character and has become a more and more routine practice. Finally, personal information is increasingly used to enforce standards of behavior. Information processing is developing, therefore, into an essential element of long-term strategies of manipulation intended to mold and adjust individual conduct. All three aspects are illustrated by a wide range of experiences.

II. Examples of Information Gathering

A. *The Transparent Patient*

Medical expenses in most countries have risen sharply in recent years.[16] No medical care system, whatever its organizational structure, can ignore these exploding costs without endangering its own existence. Both government agencies and the health care industry, therefore, have concentrated their efforts on developing and implementing cost-saving policies.[17] The result is a growing interest in the individual patient's behavior. Because the patient triggers the cost chain, her behavior influences, to a decisive extent, the expenditure.

All insurance reimbursements presuppose a minimum of personal information about the insured in the hands of the insurer. Some information has already been collected at the establishment of the insurance relationship. The more comprehensive the coverage, the more detailed the information stored. In addition, the record is supplemented by the information provided in connection with every new claim. Yet, what at first seems to have no other purpose than to permit the due fulfillment

---

[13] *See* Ginseng case, 35 BGHZ 363 (1961) (holding that mention of a law professor's name in an advertisement for sexual stimulants constitutes a serious and compensable violation of the privacy right).

[14] "Smart" or "intelligent" cards are microprocessors within credit cards. The most familiar example is an automated banking card. For a description of smart cards, see Weingarten, *Information Technology and Privacy Trends in Products and Services,* in Invited Papers on Privacy: Law, Ethics, and Technology 15, 17-18 (1982) (National Symposium on Personal Privacy and Information Technology, Oct. 4-7, 1981).

[15] Videotex is a broad term that embraces several kinds of video technologies. *See id.* at 19-21; *infra* text accompanying notes 93-98.

[16] *See, e.g.,* U.S. Comm'n on Civil Rights, Health Insurance: Coverage and Employment Opportunities for Minorites and Women 1 (1982); Comment, *Containment of Hospital and Health Care Costs—The Regulated Marketplace,* 13 Fla. St. U.L. Rev. 795 (1985).

[17] *See* Comment, *supra* note 16, at 796-97.

of an existing commitment may be transformed into valuable material for review of the insurer's policies. The insurer may use the data to identify both the sources of additional expenses and patients that are particularly costly. Modern technology facilitates such identification because computers can store a virtually unlimited amount of data and permit endless variation in the kinds of retrievals performed. The reasons for which the information was originally collected become irrelevant. Once the data have been stored, insurers can use the information for a variety of purposes unconnected with the initial purpose of the data collection.

In West Germany, for instance, medical cost data were scanned systematically to detect the main cost-raising factors and to outline the profile of the ideal cost-saving patient.[18] The findings led to a series of corrective measures directly affecting the patients. For example, the social security agencies developed a new form that must be presented to the doctor at the beginning of each consultation. The form explicitly requires that the doctor confine her services to "strictly necessary" treatments and enumerates therapeutic measures as well as certain medication that cannot be prescribed without prior approval of the agency.[19]

Some private insurers have also matched the computer-calculated cost optimum against patient data in order to determine which patients had proven more costly than this optimum and under what circumstances. Deviations from the optimum were then brought to the patient's attention in personal letters that also asked them to discuss, with a doctor named by the insurance company, ways and means of reducing future costs. None of these programs was developed in order to identify fraudulent claims. The sole aim of such programs was to measure the behavior of all the insurance beneficiaries against the computer-designed model behavior.[20]

Another equally significant example is "Gériatrix," an information system developed in France to determine the degree of "autonomy" of the elderly institutionalized in nursing homes and hospitals.[21] An individual's degree of autonomy is established by using data provided

---

[18] *See* 12 TÄTIGKEITSBERICHT DES HESSISCHEN DATENSCHUTZBEAUFTRAGTEN 73-82 (1983) [hereinafter TB HDSB].

[19] *See id.* at 73-74.

[20] *See id.* at 78-82.

[21] The system was reported to the Commission Nationale de l'Informatique et des Libertés ("CNIL"). *See* CNIL, Rapport sur une demande d'avis présentée par les établissements hospitaliers de Bischwiller et relative à un traitement automatisé dénommé "Gériatrix" dont la finalité principale est l'évaluation d'une échelle d'autonomie des personnes âgées 2 (Sept. 12, 1985).

by the personnel at the nursing home or hospital; the data are then evaluated by computer according to twenty-seven criteria that relate to, among other factors, the patient's mobility, sensory and mental capacity, and physical as well as intellectual activities. The result is integrated into a rough visual sketch of a person (the "géronte") showing the relevant autonomy zones and indicating by three different colors the actual state of the patient, so that the degree of autonomy can be judged, roughly, at a glance.[22] Hospitals and nursing homes consider this continually updated, individualized information to be an important tool in reducing their personnel costs because it enables them to establish care needs better and to allocate various tasks among their personnel. At the same time, the sketch aids them in lowering their total expenditures by helping them calculate more precisely the necessary expenses for each institutionalized person.[23] Such a system is not without danger to the individual patient's privacy. As the government report to the Commission Nationale de l'Informatique et des Libertés recognized, there is the risk that such a system becomes the sole evaluative factor, rather than one element to be used in the patient's prognosis.[24] There are also dangers to the confidentiality of the information and to its use without the knowledge of the patient or the patient's family.[25]

Automated processing thus serves control as well as planning functions. It guarantees transparency and maximizes flexibility. Insurers can not only detect deviant behavior but also can more effectively tailor cost-saving programs to the needs and demands of the insured, the doctors, the hospitals, and the pharmaceutical industry. The other side of the coin is, however, no less obvious: such data use results in an entirely transparent patient who becomes the object of a policy that deliberately employs all available information on her habits and activities in order to adapt her to insurers' expectations.[26] The patient is seen and treated as the sum of constantly increasing, strictly formalized, and carefully recorded data that can, at any moment, be combined and compared according to criteria fixed by insurers. Hence, as automated processing is perfected, the patient's position is increasingly determined by a computer-made and insurer-approved, secondhand identity.

---

[22] *See id.*

[23] *See id.* at 4.

[24] *See id.* at 5.

[25] *See id.* at 6-7.

[26] *See* 12 TB HDSB 77; 13 TB HDSB 86 (1984).

B. *The Righteous Citizen*

1. Prevention of Anti-Social Activity by Children

In 1982, a research project designed by the Health Council of Oslo was submitted for approval to the Norwegian Data Inspectorate.[27] Its purpose was to identify behavioral patterns of small children that might indicate psychological problems or later lead to "anti-social" activities.[28] In order to obtain the necessary information, police files were to be scanned for children who had exhibited delinquent behavior. Authorities next would examine the school and health authorities' records of these same children and would use this information to identify "typical danger signals." They then would perform a second, far more detailed search of the school and health authorities' records to establish a list of all children satisfying these criteria. Finally, a special assistance program would be developed to aid the risk group identified by this search.[29]

Although this kind of study may at first appear to be an exception rather than the rule, it is by no means unusual. In 1973, the information system "Gamin," covering sixty percent of the children in thirty-four French départements went into effect.[30] The system collected data provided mainly by a series of medical examinations; its goal, like that of the Norwegian program, was the reduction of social and medical risks.[31] Hence, risk profiles were outlined on the basis of nearly 170 factors and then used as search criteria to identify other children needing preventive social and medical surveillance.[32] A similar example is the recent attempt by the city of Bremen, West Germany, to establish an automated file of children exhibiting obviously "odd behavior." Thefts, excessive aggressiveness, or repeated lying were the identifying signs. Once again, the aim was therapeutic: to treat and to inhibit "dangerous" behavior and thus to guide the child to adapt better to societal expectations.[33]

---

[27] *See* Bing, *Data Protection and Social Policy,* in BEYOND 1984: THE LAW AND INFORMATION TECHNOLOGY IN TOMORROW'S SOCIETY 82, 91 (Council of Europe 1985) [hereinafter BEYOND 1984] (Proceedings of the 14th Colloquy on European Law, Lisbon, Sept. 26-28, 1984).

[28] *See id.*

[29] *See id.*

[30] *See* CNIL, 2ÈME RAPPORT D'ACTIVITÉ, 1ER OCTOBRE 1980 - 15 OCTOBRE 1981, at 28-29 (1982) [hereinafter CNIL, 2ÈME RAPPORT].

[31] *See id.* at 29.

[32] *See id.* at 30; *see also* CNIL, BILAN ET PERSPECTIVES 1978-1980, at 84 (1980). In June, 1981 the CNIL rendered an unfavorable opinion on the program. *See* CNIL, 2ÈME RAPPORT, *supra* note 30, at 28.

[33] *See* BREMISCHE BÜRGERSCHAFT LANDTAG, 7 JAHRESBERICHT DES

In all three cases discussed above, automated processing is regarded as an aid to prevent deviations from socially acceptable behavioral patterns. The righteous citizen is both the incentive and the goal of the retrieval. It is therefore not surprising that the attention focuses on children: they are the ideal object of a preventive policy. Society has, it seems, the chance to intervene before the risk becomes so great as to necessitate repressive correction. In these instances, automated processing is used to render individual behavior as transparent and understandable as possible in order to develop a series of measures anticipating reactions and adjusting them to a predetermined model. The computer matches the existing files, retrieves the necessary data, and restructures these data for purposes entirely different from the original collection aims.

2. Control of Adult Behavior

While prevention of anti-social behavior prevails in the case of children, behavioral control constitutes an equally strong goal when the attention focuses on adults. Social security again presents a good example. The gradual expansion of social assistance systems to include various educational programs, professional aids, and protective services has been one of the outstanding features of state activity in the past years. In fact, a continuously growing welfare administration is probably the most characteristic feature of an activist welfare state.[34] As long as social policies were designed and implemented against the background of a prosperous or at least stable economy, only the administrative details of implementation seemed to matter. As economic conditions have changed, however, governments have adopted clearly restrictive attitudes. One result has been cutbacks in financial assistance, accompanied by increasingly sharpened attempts to control the behavior of the

---

LANDESBEAUFTRAGTEN FÜR DEN DATENSCHUTZ 56-58 (1985) (Drucksache 11/365).

[34] *See, e.g.*, B. ACKERMAN, RECONSTRUCTING AMERICAN LAW (1984) (discussing the activist American legal culture since the New Deal); M. DAMASKA, THE FACES OF JUSTICE AND STATE AUTHORITY: A COMPARATIVE APPROACH TO THE LEGAL PROCESS 80 (1986) (stating as a general characteristic of the activist state the development of programs encompassing all aspects of life); DILEMMAS OF LAW IN THE WELFARE STATE (G. Teubner ed. 1986); F. SCHARPF, PLANUNG ALS POLITISCHER PROZESS: AUFSÄTZE ZUR THEORIE DER PLANENDEN DEMOKRATIE 114 (1973) (discussing the growing complexity of the administrative system); R. TITMUSS, ESSAYS ON "THE WELFARE STATE" (1958); Simitis, *The Juridification of Labor Relations,* 7 COMP. LAB. L. 93, 100 (1986) (discussing effect of social legislation on scope and conditions of state intervention in labor relations). *See generally* Ackerman, *Foreward: The Law in an Activist State,* 92 YALE L.J. 1083 (1983) (arguing that the development of the activist state since the New Deal has fundamentally transformed legal discourse).

social programs' beneficiaries.

In the United States, the social security number ("SSN") has become the master key to all information considered necessary for control purposes. Most of the nearly 500 computer matching programs carried out at the federal and state levels depend on the SSN.[35] For example, section 2651 of the 1984 U.S. Deficit Reduction Act[36] requires that applicants for all programs of the federal Social Security Administration supply their social security number. The reason is obvious: the number provides a reliable and timely means for identification of ineligible persons and incorrect payments.[37] The SSN permits the correlation of data held by different agencies and transforms government into a permanently accessible information unit. More importantly, the SSN bridges the gap between the public and the private sector. For instance, computer matches of the SSN conducted on recipients of federal Aid to Families with Dependent Children ("AFDC") used data from state income tax, motor vehicle registration, school records, correction files on inmate status, veteran records, worker's compensation, and low income home compilations together with bureau records from employers, banks, and credit agencies.[38]

Once the emphasis is placed on control, neither the sensitivity of the data nor the existence of access barriers, otherwise considered insurmountable, comes into play. The Inspector General's Office for the

---

[35] For a discussion of both the matching practices in the social security field and the key function of the SSN, see D. BURNHAM, THE RISE OF THE COMPUTER STATE 182-83 (1983) (discussing the Social Security Administration's plan to examine IRS records to determine whether those receiving supplemental benefits had received dividend and interest payments); PRIVACY PROTECTION STUDY COMM'N, PERSONAL PRIVACY IN AN INFORMATION SOCIETY 605-18 (1977); Langan, *Computer Matching Programs: A Threat to Privacy?*, 15 COLUM. J.L. & SOC. PROBS. 143, 169-71 (1979).

[36] Deficit Reduction Act of 1984, Pub. L. No. 98-369, § 2651, 98 Stat. 494, 1147 (codified at 42 U.S.C. § 1320b-7(a)(1) (Supp. III 1985 & West Supp. 1986)).

[37] HOUSE CONFERENCE REPORT ON THE DEFICIT REDUCTION ACT OF 1984, H.R. CONF. REP. NO. 861, 98th Cong., 2d Sess. 757, 1410-12, *reprinted in* 1984 U.S. CODE CONG. & ADMIN. NEWS 1445, 2098-2100.

[38] CONTROLLER GENERAL, REPORT TO CONGRESS: ELIGIBILITY VERIFICATION AND PRIVACY IN FEDERAL BENEFIT PROGRAMS: A DELICATE BALANCE 5-18, 22-32 (GAO/HRD-85-22, Mar. 1, 1985)); *see also Oversight of Computer Matching to Detect Fraud and Mismanagement in Government Programs, 1982: Hearings Before the Subcomm. on Oversight of Government Management of the Senate Comm. on Governmental Affairs*, 97th Cong., 2d Sess. 222-50 (1982) [hereinafter *1982 Senate Hearings*] (testimony of William T. Hogan, Jr., Secretary, Massachusetts Executive Office of Human Services) (discussing data matches, with particular reference to use of bank asset data, on Massachusetts recipients of AFDC and other welfare benefits).

Since September 1986, the duty to conduct regular matches has shifted to the states. In order to receive federal funds they must operate a State Income Eligibility Verification System ("SIEVS") that permits continuous control of the recipients. *See "SIEVS" Creating Headaches in the States*, 12 PRIVACY J. 6 (June 1986).

United States Department of Health and Human Services, for instance, did not hesitate to design computer programs that identify "illogical billing situations" in the case of abortions and sterilizations.[39] The attitude of the West German authorities is no less significant. The range of the "social security secret" established by law and explicitly excluding a free flow of social security data has been restricted: use of such information is permitted for purposes as different as pursuing moonlighters, controlling the work permits of foreigners, or uncovering fraudulent activities in general.[40] In addition, some of the West German social security agencies have begun to compile a list of characteristics of potential "assistance-chiselers" and to distribute "warning lists" to the other branches of government, as well as to private institutions such as the Salvation Army.[41]

Similar tendencies have been observed in the taxation field. A government's financial resources depend to a decisive extent on punctual and correct tax payments by citizens. Governments will be tempted to use all available information to secure payment, particularly in economically critical situations. Automated processing again serves as a most welcome tool. For example, the United States Internal Revenue Service tries to identify underpayers or evaders of federal taxes by matching its own data against state, municipal, and private business records.[42] Its regional office in Texas has sought to establish electronic links with eighty counties and thereby gain instant access to local tax, voter registration, and automobile ownership files.[43]

Other countries also have viewed identification systems as a solution to information problems in dealing with their citizens. In a White Paper published in 1985, the Australian Federal Government advo-

---

[39] *See* OFFICE OF THE INSPECTOR GEN., DEP'T OF HEALTH & HUMAN SERVS., 1 COMPUTER APPLICATIONS, in *1982 Senate Hearings, supra* note 38, at 287, 334-35.

[40] *See* Simitis, *Reicht unser Datenschutzrecht angesichts der technischen Revolution?—Strategien zur Wahrung der Freiheitsrechte,* in INFORMATIONSGESELLSCHAFT ODER ÜBERWACHUNGSSTAAT: STRATEGIEN ZUR WAHRUNG DER FREIHEITSRECHTE IM COMPUTERZEITALTER: PROTOKOLL 33 (1984) [hereinafter INFORMATIONSGESELLSCHAFT] (Symposium der Hessischen Landesregierung, Wiesbaden, Sept. 3-5, 1984) (noting that measures to reduce administrative expenses contract protection afforded by the "social security secret," because cost reduction is only possible through exact knowledge about the effect of a particular welfare program).

[41] *See* 13 TB HDSB 21 (1984) (giving examples of the categories of people the government has warned against).

[42] *See Computer Matching: Taxpayer Records: Hearings before the Subcomm. on Oversight of Government Management of the Senate Comm. on Governmental Affairs,* 98th Cong., 2d Sess. 25-31 (1984) [hereinafter *1984 Senate Hearings*] (statement of Roscoe L. Egger, Jr., Commissioner of Internal Revenue).

[43] *See* Burnham, *I.R.S. Seeks Links to County Computers in Texas to Find Debtors,* N.Y. Times, Mar. 13, 1984, at A23, col. 1.

cated the introduction of an "Australia Card."[44] The government hoped that such a unique personal identifier substantially would improve the access of the Taxation Office to needed information, particularly by permitting it to link the various records containing data concerning taxpayers. The data matching initially would be restricted to government records. Yet, this limitation may be short-lived. Experience has shown that national identification systems quickly become integrated into the private sector, either, as in the case of employees, because of legislative requirements, or because of peculiar interests of private organizations.[45] Thus, in Canada, for example, the identifier is required for activities as different as opening a bank account, renewing a magazine subscription, applying for union membership, or borrowing books from a library.[46] The more widespread the use of the identifier, the better the chances of creating an exhaustive information base through an electronic linkage of the files.

Sweden provides a good example of a country's attempts to connect data and their implications.[47] In Sweden, there is virtually no information irrelevant to the evaluation of the tax duty. Nearly every available datum is gathered in order to estimate the amount of the payment due, including different sources of income, various property items, buying habits, memberships in professional organizations, charities and clubs, or vacation travel.[48]

In both social security and taxation, automated processing helps to define "suspect populations," to identify "hits," and to conduct systematic follow-ups.[49] At the same time, however, the burden of proof is

---

[44] *See* REFORM OF THE AUSTRALIAN TAX SYSTEM 39-40 (1985) (draft White Paper). For a critical appreciation, see PRIVACY COMMITTEE, PRIVACY ISSUES AND THE PROPOSED NATIONAL IDENTIFICATION SCHEME: A SPECIAL REPORT (Mar. 1986) (New South Wales).

[45] *See* CANADIAN HUMAN RIGHTS COMM'N, REPORT OF THE PRIVACY COMMISSIONER ON THE USE OF THE SOCIAL INSURANCE NUMBER 26-28 (1981) [hereinafter PRIVACY COMMISSIONER REPORT] (Some organizations stated that they used social insurance numbers simply to facilitate activities required by law. Others admitted using the numbers for additional purposes, arguing that such uses were in society's best interests and therefore should not be hindered by legislative pronouncement or proscription.); D. FLAHERTY, THE ORIGINS AND DEVELOPMENT OF SOCIAL INSURANCE NUMBERS IN CANADA (1981).

[46] *See* PRIVACY COMMISSIONER REPORT, *supra* note 45, at 27-28.

[47] *See* Freese, *Verletzlichkeit des Individuums und der Gesellschaft,* in 1984 UND DANACH, *supra* note 11, at 154, 176; Thoor, *Orwell's 1984: The Computer Threat,* 7 TRANSNAT'L DATA REP. 139, 139 (1984) (discussing the Swedish social code number, which "follow[s] every Swedish citizen from his first day of life forever" and is used for a wide variety of private and public purposes).

[48] "Sweden—compared with many other countries—has developed into a transparent aquarium." Freese, *supra* note 47, at 177.

[49] The processing of personal data is indeed symptomatic of a "new awakened morality" entailing a "hunt for people not fulfilling their obligations towards society."

reversed. For example, once the computer indicates that a certain person has been receiving benefits without being entitled to them, the benefits may be cut without a hearing. It then falls to the incriminated person to prove the absence of a violation.[50] Instead of requiring the agency to examine the information provided by the retrieval and to prove a violation, it becomes the burden of the individual concerned to explain and justify her behavior. The accusation, therefore, comes very close to being a conviction.

In Sweden, for example, in the course of a "fishing expedition" aimed at detecting fraudulent housing aid recipients, perfectly correct information from a particular file was correlated with equally accurate data contained in another record. As a result of this matching, one thousand persons were suspected of having committed fraud. Some of them were quickly convicted without anyone ever questioning the information processing and its possible implications. Ultimately, however, the government had to admit that only one person out of the one thousand suspects was really guilty.[51]

A second, no less important, consequence of automated processing is the loss of context.[52] The very moment the matching begins, the data are itemized and disconnected from their original collection situation. Yet neither hard facts nor judgments can be separated at will from their context without distorting the information. Consequently, every step toward routinized processing accentuates the danger of misrepresentations and false conclusions. The more complex a case, the greater the danger of an improper result. For example, the Medicaid benefits of an elderly woman living in a Massachusetts nursing home were terminated because, according to a computer match of welfare rolls and bank accounts, her account exceeded the Medicaid asset limit.[53] The account contained, however, a certificate of deposit in trust that was intended to cover her funeral expenses. The computer failed to recognize that under federal regulations the certificate of deposit was an exempt resource not to be included in the calculation of her assets for

---

Freese, *supra* note 47, at 175.

[50] *See* Bing, *supra* note 27, at 89; Freese, *supra* note 47, at 170 (explaining that today authorities do not contact individuals directly for information but instead consult data processing files); Marx & Reichman, *Routinizing the Discovery of Secrets,* 27 AM. BEHAV. SCIENTIST 423, 440-41 (1984).

[51] *See* Freese, *supra* note 47, at 172.

[52] *See Special Report: Sweden's Freese Sees Need for International Privacy Forum,* 2 PRIVACY TIMES 8, 9 (Sept. 22, 1982) (linking data that were collected for different purposes causes a loss of "data quality").

[53] *See 1982 Senate Hearings, supra* note 38, at 80 (statement of John H. Shattuck, National Legislative Director, ACLU).

purposes of Medicaid.[54] The payments, therefore, had been proper.

False conclusions caused by the inaccuracy of files, however, are far more widespread. According to a study initiated by the United States Office of Technology Assessment, only twelve percent of the criminal history record summaries routinely transmitted from North Carolina to law enforcement and other agencies were correct.[55] The figures for California were slightly better, but still not encouraging: nineteen percent.[56] Similarly, the West German experiences demonstrate that German police records also contain obsolete, ambiguous, or incorrect data.[57] Under these conditions, computer matching inevitably leads to a proliferation of false information.[58] Both the error and the implications for the persons concerned are magnified.[59]

Finally, automated processing generates categorizations, especially when hits are assembled under a particular heading. An individual included in the computer-made list is necessarily labeled and henceforth seen as a member of a group, the peculiar features of which are assumed to constitute her personal characteristics. Whoever appears in the lists as "tax-evader," "assistance-chiseler," or "porno-film viewer" must be constantly aware of being addressed as such. She can neither foresee nor prevent situations in which her connection with one of the groups constructed by the computer may be raised.[60] For example, when a movie house operator in Columbus, Ohio, was arrested for showing obscene movies, one of which was also available on the Qube pay adult channel program,[61] the defense subpoenaed the subscriber records of the cable channel to demonstrate that the film did not violate community standards on obscenity. Although Qube refused to reveal individual viewing records, it did supply general viewing statistics on

---

[54] *See id.*

[55] *See* D. BURNHAM, *supra* note 35, at 74.

[56] *See id.*

[57] *See* 11 TB HDSB 70, 126 (1982); 10 TB HDSB 42 (1981).

[58] *See* Bing, *supra* note 27, at 89.

[59] *See* Lowi, *Die dritte Revolution: Eine Überprüfung,* in 1984 UND DANACH, *supra* note 11, at 99, 125; Shattuck, *In the Shadow of* 1984: *National Identification Systems, Computer-Matching, and Privacy in the United States,* 35 HASTINGS L.J. 991, 1001-04 (assessing various dangers of computer matching).

[60] *See* Bing, *supra* note 27, at 87; Simitis, *supra* note 40, at 39 (expressing people's fear of being assigned to a certain group, e.g., porno-viewers, based upon external and possibly irrelevant criteria).

[61] *See* Nash & Smith, Interactive Home Media and Privacy Issues, in REPORT TO THE FEDERAL TRADE COMMISSION, OFFICE OF POLICY PLANNING 52-57 (1981). Qube is an interactive cable system that is capable of tracking viewer reception. Qube offers "adult" channels among its pay cable service selections and can monitor viewer choices and responses. Although Qube attempts to safeguard this information, questions of access may arise under certain circumstances, as the Ohio case illustrates.

the film in question and on general viewing patterns.[62]

C. *Personnel Information Systems: The Well-Adjusted Employee*

In September, 1984, the West German Federal Labor Court decided one of its most interesting cases.[63] Rank-Xerox had attempted to establish an information system, the International Technical Service System, the main purpose of which was to record defects in products, as well as the sources of the defects, and to improve the supply of necessary spare parts. The data were to be provided by salesmen and technicians through the use of computerized forms. In addition to the data necessary to carry out the main purpose of the information system, the firm required technicians to supply certain additional details concerning their activities. These particular data were then to be matched against all other information collected by Rank-Xerox on its employees. In light of the West German Works Constitution Law, which prescribes that all decisions on technical devices entailing surveillance must be made jointly by the employer and the works' council,[64] the latter opposed the introduction of the International Technical Service System on the grounds that it infringed the council's co-determination rights. The question before the court in the Rank-Xerox case was whether this admittedly very general bargaining provision is also applicable to an automated retrieval of personnel data.[65]

All legal considerations aside, the case illustrates the ongoing mod-

---

[62] *See* Nash & Bollier, *Protecting Privacy in the Age of Hometech,* TECH. REV., Aug./Sept. 1981, at 67, 70.

[63] Rank-Xerox case (BAG 1984), 38 NJW 450 (W. Ger.).

[64] BETRIEBSVERFASSUNGSGESETZ [BETRVG] (Works Constitution Law), BGBl.I 13 (1972), Jan. 15, 1972, last amended Apr. 26, 1985, BGBl.I 710 (1985), art. 87, ¶ 6 (W. Ger.).

[65] For a detailed discussion, see Simitis, *Mitbestimmung als Regulativ einer technisierten Kontrolle von Arbeitnehmern,* 38 NJW 401-08.

Similar problems have arisen in Norway and Switzerland. The Norwegian Worker Protection and Working Environment Act foresees the employer having a duty to inform the employees, as well as their elected representatives, about any control and planning systems and to provide the opportunity to learn about and understand these systems. *See* Lov. nr. 4 om arbeiderverns of arbeidsmiljo m.v., Feb. 4, 1977, *amended by* Act of 13 June 1980, § 12.3 (Nor.), NORGES LOVER 1685-1985, at 2112 (Oslo 1986), available in English translation from Direktoratet for Arbeidstilsynet, Order No. 330. The law also includes confidentiality rules governing data collected about worker injuries and diseases. *See id.* § 20. As in West Germany, the applicability of these rules to rapidly changing retrieval techniques quickly became an extremely controversial issue. In their agreement covering the years 1983-1988, the Swiss Machine- and Metal-Industry Employers' Association and Unions explicitly stressed the need for regulating and restricting automated retrieval of personnel data. *See* VEREINBARUNG UND VERABREDUNGEN IN DER MASCHINENINDUSTRIE ZWISCHEN DEM ARBEITGEBERVERBAND UND DEN ANGESTELLTENVERBÄNDEN (Vertragsperiode 1983-1988), art. 11.

ification of work conditions through the increasing use of personnel information systems. The development of such systems has been inspired nearly everywhere by purely administrative preoccupations as employers are faced with the need to collect more and more data about employees.[66] The traditional terms of employment already entail a considerable amount of information collection because, for example, of the various forms of remuneration or the exact calculation of leave claims, sickness payments, and pensions. Furthermore, collective agreements tend to regulate all aspects of employment. Work conditions can hardly be "humanized," in the terms of the unions' bargaining policies, without a precise knowledge of the physical and intellectual abilities, the professional training, and the occupational experiences of the employees concerned. The consequence of such regulation is once again an incessant accumulation of personal data about employees.

Finally, the employment relationship has become an indispensable source of information for a whole series of state activities including taxation, occupational health and safety controls, and unemployment aids.[67] None of the traditional manual retrieval means can fully cope with the inflation of data and the constantly varying processing purposes. Personnel information systems therefore constitute the technical answer to an otherwise unsolvable organizational problem. Employers have, however, quickly realized that information systems offer at least two other decisive advantages: better opportunities for control of employees and improved chances for long-term personnel planning.[68] The latter has long been one of the main incentives for collecting personnel data. The information gathered at the beginning of the century by the Ford Motor Company inspectors on workers' habits and living conditions served no other purpose than to facilitate adaptation to the employer's expectations.[69] The same intention has led to more and more

---

[66] For an analysis of the background, the techniques and the implications of the retrieval of personnel data, see S. SIMITIS, SCHUTZ VON ARBEITNEHMERDATEN, REGELUNGSDEFIZITE—LÖSUNGSVORSCHLÄGE (1980) (report made upon order of the German Federal Secretary of Labor, stating the unsuitability of existing legal provisions to meet the needs created by the employer-employee relationship).

[67] In the United States, for example, statutes enacted for the protection of employees such as the Occupational Safety and Health Act (OSHA) and the Employee Retirement Income Security Act (ERISA) have forced employers to gather more information concerning their employees in order to demonstrate compliance with the statutes. *See* PRIVACY PROTECTION STUDY COMM'N, *supra* note 35, at 227-28.

[68] *See* Simitis, *Gesetzliche Regelungen für Personalinformationssysteme—Chancen und Grenzen,* in INFORMATIONSGESELLSCHAFT, *supra* note 40, at 79.

[69] *See* A. NEVINS, FORD: THE TIMES, THE MAN, THE COMPANY 554-55 (1954) (detailing the thorough investigations performed by Ford's Sociological Department, characterized by one head of the department as having "fraternal, not paternal" purposes).

sophisticated questionnaires and psychological tests. Each of these instruments aims, in the words of most personnel management manuals, at ensuring the choice of the right worker for the right workplace.[70]

Personnel information systems represent a further step in this direction.[71] There is also, however, an obvious qualitative change. Never before have employers been able to collect and retrieve so much data about employees. Consequently, the flexibility of personnel policy can be considerably improved and the demands arising out of both the particular structure of the workplace and of market conditions better met. Personnel information systems contribute, therefore, to the rationalization of the production process. They mark, in fact, a new and decisive stage of its taylorization.[72]

The obvious advantages for the employer have, however, a corresponding cost: increased vulnerability on the part of employees. As the Rank-Xerox example shows, reliable planning presupposes close control. The establishment of an information system therefore implies continuous supervision, for only with continual and careful monitoring of employees can the necessary data for a risk-minimizing personnel policy be obtained. Because the system's primary task, however, is an optimal adaptation of the processing to the changing policy aims of the employer, the exact purposes and potential implications of the data collection are deliberately left open. For example, information on employees' particular characteristics gathered initially to permit a better selection of the proper workplace for the employee may, at a later point, serve as a factor in dismissal.[73] Similarly, an employer initially may collect data on employees' means of transportation to the workplace in order to determine whether to provide busing but can use this data later when designing a plan for a reduction in personnel.[74]

The greatest advantage of the personnel information system to the employer—the possibility of using the data for multiple purposes—also poses the greatest threat to the employees. They must deal with a

---

[70] For a critical analysis of management-employee relations, see R. BENDIX, WORK AND AUTHORITY IN INDUSTRY: IDEOLOGIES OF MANAGEMENT IN THE COURSE OF INDUSTRIALIZATION 272-73 (1956).

[71] *See* S. SIMITIS, *supra* note 65, at 3-10 (discussing the development and interconnection of various information sources).

[72] *See* R. BENDIX, *supra* note 70, at 274-81 (discussing the work of Frederick W. Taylor, who advocated "scientific management" through testing of workers in order to place them in positions for which they are best suited and most efficient, a process now known as taylorization).

[73] For a discussion of the use of seemingly harmless data to the detriment of employees, see Simitis, *supra* note 68, at 82, 91; Simitis, *supra* note 65, at 406 (noting as examples data on the employee's working performance as well as his absenteeism).

[74] *See* R. NIEBUR, EDV IN BETRIEB UND VERWALTUNG—EINE GEFAHR FÜR DIE ARBEITNEHMER 60 (1983).

mechanism, inaccessible to them, that institutionalizes control, thereby ensuring constant reevaluation of their individual performance. This surveillance increases the already uncontrollable risk of losing their employment. Even if employees do not realize the exact implications of an information system, the mere awareness of a device that minutely records their activities may be sufficient to influence their behavior. The pressure resulting from employees' need to retain their jobs and from the presence of the information system inhibits critical reactions. The employees tend, instead, to conform to the real or assumed expectations of the employer. Hence, although statutes and collective agreements seek to guarantee a minimum of independence, personnel information systems promote a maximum of adjustment.

Another equally important consequence can be observed where dismissal laws require the employer, especially in cases where the employer is cutting jobs, to select carefully those employees for whom termination of the employment relationship would appear to have the least detrimental effects.[75] Any termination is therefore, in the eyes of the law, a highly personalized process. The opposite occurs when the dismissal is based on an automated retrieval of employee data. An employer can simply have the computerized system produce dismissal lists established with the help of abstract search criteria. The courts then are presented with a machine-made decision that is apparently perfectly objective, precisely because it is machine-made. The responsibility for deciding which employees to terminate is thus shifted to the computer and its "impartiality" invoked as the very best proof of the correctness of the decision.[76] Yet, because neither the courts nor the employees con-

---

[75] *See, e.g.,* Employment Protection (Consolidation) Act 1978, ch. 44, § 57 (U.K.) (presenting general provisions relating to fairness of dismissal); Kündigungsschutzgesetz, Aug. 10, 1951, BGBl.I 499 (1951), *last amended* Apr. 26, 1985, BGBl.I 710 (1985), § 1, para. 2, no. 1, litt. b (West German dismissal protection law); Simitis, *supra* note 34 (comparing the approaches of various countries to labor law).

[76] This is only one more example of the widespread quest for computerized decisionmaking techniques, regarded as the long-awaited instrument that permits a definitive replacement of personal judgment by calculations that exclude ambiguities and divergent interpretations of social and political facts. Joseph Weizenbaum has succinctly described the problem:

> What is happening . . . is that people have turned the processing of information on which decisions must be based over to enormously complex computer systems. They have, with few exceptions, reserved for themselves the right to make decisions based on the outcome of such computing processes. People are thus able to maintain the illusion, and it is often just that, that they are after all the decisionmakers. But . . . a computing system that permits the asking of only certain kinds of questions, that accepts ony certain kinds of "data," and that cannot even in principle be understood by those who rely on it, such a computing system has effectively closed many doors that were open before it was installed.

cerned have the opportunity and the competence to oversee the programs used in generating the lists, there is no guarantee that all relevant factors and circumstances have actually been considered. Furthermore, employees are deprived of the already scant opportunity to discuss their viewpoints with the employer and to refute her arguments directly.

D. *Conclusions*

Although the examples discussed above cover very different areas, a few general conclusions nevertheless can be drawn. First, none of the experiences stated is exclusively typical of a single country. Despite the fact that the conditions under which medical data are retrieved, social security measures designed, or personnel information systems implemented vary according to the particular political, economic, and legal framework, the same problems can be observed in many countries. Each of the examples reflects conflicts characteristic of every industrialized and highly developed technological society. It is, therefore, not surprising that opinion polls reveal a growing concern for individual privacy that clearly transcends national boundaries. In a 1982 poll conducted in Canada on public attitudes toward computer technology, sixty-five percent of the persons surveyed identified invasion of privacy as their main concern.[77] A year later, eighty-four percent of those polled in the United States thought that a file containing credit information, employment data, phone calls, buying habits, and travel could easily be compiled.[78] Also, in 1983, sixty percent of those surveyed in West Germany felt that computers have already given the state too many opportunities for control.[79] Americans were more explicit. Sev-

---

J. WEIZENBAUM, COMPUTER POWER AND HUMAN REASON: FROM JUDGMENT TO CALCULATION 38 (1976); *see also* H. ARENDT, CRISES OF THE REPUBLIC 9-11 (1972) (characterizing the professional "problemsolvers" in the high ranks of government as individuals eager to discover reliable information and laws to explain and predict human affairs).

[77] *See* Diebel, *Privacy and the Computer State,* MACLEAN'S, Jan. 9, 1984, at 34, 35-36; *see also* Vidmar & Flaherty, *Concern for Personal Privacy in an Electronic Age,* J. COMM. 91, 103 (Spring 1985) (presenting other data that "reflect genuine fears and concerns, directed toward both government and private business" concerning the collection of personal information).

[78] *See Privacy and 1984: Public Opinions on Privacy Issues, Hearings Before a Subcomm. of the House Comm. on Government Operations,* 98th Cong., 1st Sess. 16 (1984) [hereinafter *Privacy and 1984*].

[79] *See* Becker, *Bürger in der modernen Informationsgesellschaft,* in INFORMATIONSGESELLSCHAFT ODER ÜBERWACHUNGSSTAAT: STRATEGIEN ZUR WAHRUNG DER FREIHEITSRECHTE IM COMPUTERZEITALTER: GUTACHTEN 414 (1984) (Symposium der Hessischen Landesregierung, Wiesbaden, Sept. 3-5, 1984). At the same time 65% stated that as little information as possible should be given to the state. The percentage

enty percent appear to be convinced that government *will* take advantage of the chances offered by technology in order to intimidate individuals or groups.[80] Hence, both experiences with the retrieval of personal data and the widespread distrust of those with access to personnel information systems demonstrate the universality of the problems created by intensive computerization. They also show that a discussion of its consequences inevitably leads to a debate on the structure and organization of society.

Second, the examples refute the widespread assumption that the implications of automated processing of personal data are only a by-product of the expansionist policies of an activist state. Certainly, the enormous increase in the information collected corresponds to a considerable extent to the changes in state activities. Nearly every new task assumed by the welfare administration multiplies the demand for personal data. It is therefore not surprising that countries like Sweden or Norway, which have well-established interventionist traditions, are particularly inclined to design both preventive and repressive policies with the help of an automated processing system.

Yet, even in the United States, whose traditions are normally not inclined to favor state activism, the federal government has not hesitated to use automated processing in both the taxation[81] and social security fields.[82] There is, of course, one striking difference between the United States and countries favoring more state involvement: the United States' lack of comprehensive state data banks. Yet this difference has never proved to be a serious obstacle. There are enough private files in the United States providing a perfectly satisfactory substitute. Hence, the information can either be obtained by a direct linkage or, as the IRS example shows, by simply buying marketing lists and matching them against the data already collected by the various branches of

---

rose to 76% when the same question was put with regard to private firms. *Id.* at 413.

[80] *See Privacy and 1984, supra* note 78, at 20.

[81] *See, e.g., 1984 Senate Hearings, supra* note 42, at 25-40 (statement of Roscoe L. Egger, Jr., Commissioner of Internal Revenue) (describing the variety of information services used by the IRS to ensure that information voluntarily provided by taxpayers is correct).

[82] In 1974, the same year that Congress was passing the Privacy Act, it

> amended the Social Security Act to require all welfare recipients to disclose social security numbers in order to receive benefits, and to require [the Department of Health, Education, and Welfare] to establish a computerized Parent Locator Service with authority to tap any other federal agency's data banks (notably Social Security and Internal Revenue Service records) to find the last known address of an absent parent not supporting a child.

D. FLAHERTY, PRIVACY AND GOVERNMENT DATA BANKS: AN INTERNATIONAL PERSPECTIVE 285 (1979).

government.[83]

Third, the aim of controlling and adjusting individual behavior is by no means an exclusive attribute of processing activities initiated by the state. Both the retrieval of medical data by insurance companies and the establishment of personnel information systems make it clear that private enterprises and state agencies resort to automated processing for quite similar purposes. Consequently, when the State of Hesse, West Germany, decided to introduce a personnel information system for schoolteachers,[84] techniques corresponding to those used by chemical or automobile firms were adopted. Furthermore, as in the case of employment relationships, data originally collected for the government are to a large extent also retrieved for clearly private purposes. Similarly, information gathered by private firms is, as demonstrated by the experiences of banks[85] and credit card companies,[86] again and again processed by the government. The boundaries between the public and private sectors are thus blurred. Personal data, once stored, tend to become a flexible, common base of information.

Fourth, because of both the broad availability of personal data and the elaborate matching procedures, individual activities can be accurately reconstructed through automated processing. Surveillance becomes the order of the day. Significantly enough, security agencies were among the first to discover the advantages of automated retrieval.[87]

---

[83] *See, e.g., 1984 Senate Hearings, supra* note 42, at 25 (statement of Roscoe L. Egger, Jr., Commissioner of Internal Revenue)

> Commercial lists can reflect a variety of information, but typically they would show such things as the names of heads of households and estimates of household incomes. Private companies prepare these lists using publicly available records, such as telephone listings, motor vehicle registrations, real estate transactions and public/aggregate census data . . . . The IRS is attempting to determine if commercial lists can supplement a variety of other efforts to identify persons who fail to file returns.

Id.; Burnham, *IRS Buys Company's List of Names, Incomes to Track U.S. Tax Evaders,* Int'l Herald Tribune, Dec. 27, 1983, at 3, col.7.

[84] *See* 12 TB HDSB 94-95 (1983); 9 TB HDSB 55 (1980).

[85] *See, e.g.,* PRIVACY PROTECTION STUDY COMM'N, supra note 35, at 103-05 (describing the Bank Secrecy Act of 1970, which requires depository institutions to maintain particular records on individuals and to report specific transactions to the government).

[86] *See, e.g., id.* at 52-55 (describing methods by which a government agency can gain access to a credit card issuer's records).

[87] *See, e.g.,* 6 *Intelligence Activities: Hearings on S. Res. 21 Before the Senate Select Comm. to Study Governmental Operations with Respect to Intelligence Activities,* 94th Cong., 1st Sess. 8 (1975) [hereinafter *Intelligence Activities*] (testimony of Curtis R. Smothers, Counsel to the Minority, Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities) ("The [FBI] with its 59 field offices staffed by more than 9,500 special agents, maintains a data bank on citizens which includes criminal information, and this investigative data bank . . . grows

They not only quickly computerized their own data collections but also sought and obtained access to state and private data banks.[88] Entirely new investigation techniques, such as computer profiling, were developed, enabling the agencies to trace wanted persons by matching a presumptive pattern of consumption habits against, for instance, the records of utility companies.[89] The successful attempts at computer-based voice and picture identification[90] will probably influence the work of security agencies even more.

Although the purposes vary, the surveillance methods used by different institutions are astonishingly similar. "Mobility profiles," for example, were first introduced by the police authorities.[91] Data collected in the course of repeated controls at various selected places were sys-

---

daily . . . ."); Herold, *Künftige Einsatzformen der EDV und ihre Auswirkungen im Bereich der Polizei*, 9 KRIMINALISTIK 388 (1974); Herold, *Organisatorische Grundzüge der elektronischen Datenverarbeitung im Bereich der Polizei*, 18 TASCHENBUCH FÜR KRIMINALISTEN 240 (1968) (stating that use of electronic data processing requires a different organizational structure of police agencies).

[88] *See, e.g.*, 6 *Intelligence Activities, supra* note 87, at 367 (information gathered for FBI data banks was collected 50% of the time from state Motor Vehicles Division confidential sources in utilities, educational institutions, and state employment agencies); 13 TB HDSB 98-99, 117, 119 (1984) (discussing police access to data of federal office of motor traffic and to identity card data, establishment of data bank on activities endangering the security of the state, and the Hessian evidentiary retrieval system); 12 TB HDSB 33 (1983) (noting the establishment of a federal data bank for criminal investigation material); D. BURNHAM, *supra* note 35, at 39, 66, 106, 169-71, 200; CNIL, 2ÈME RAPPORT, *supra* note 30, at 70 (1982) (delineating standards for access to and use of information possessed by the military and police); BUNDESKRIMINALAMT WIESBADEN, POLIZEILICHE DATENVERARBEITUNG (1983) (Arbeitstagung des Bundeskriminalamtes, Wiesbaden, Nov. 2-5, 1982) (discussing development and possible applications of electronic data processing); G. WIESEL & H. GERSTER, DAS INFORMATIONSSYSTEM DER POLIZEI INPOL: KONZEPT UND SACHSTAND 30-32 (1978) (the central information system of the West German police transmits information that is collected and stored by the states and retrieved at the federal criminal office (Bundeskriminalamt)); Herold, *Perspektiven im Bereich der Sicherheitsbehörden*, in INFORMATIONSGESELLSCHAFT, *supra* note 40, at 207, 213 (discussing technical prospects of modern data processing); Note, *Government Monitoring of International Electronic Communications: National Security Agency Watch List Surveillance and the Fourth Amendment*, 51 S. CAL. L. REV. 429 (1978) (describing how the National Security Agency intercepts international communications, processes them, and forwards them to other government agencies).

[89] *See* 3 TÄTIGKEITSBERICHT DES BUNDESBEAUFTRAGTER FÜR DEN DATENSCHUTZ 50-51 (1981) [hereinafter TB BFD] (examining the use of automated files by the West German federal criminal office, "Bundeskriminalamt"); 7 TB BFD 60 (1985) (discussing risks of new computer investigative techniques); J. SIMON & J. TAEGER, RASTERFAHNDUNG 25 (1981) (analyzing the matching of data from gas, power, and water companies in several West German cities against consumption patterns of a list of wanted persons established by the Bundeskriminalamt).

[90] *See* Herold, *supra* note 88, at 214, 221; Krückeberg, *Informationstechnologie der Zukunft*, in POLIZEILICHE DATENVERARBEITUNG, *supra* note 88, at 47-49.

[91] *See* 12 TB HDSB 58, 63 (1983); 4 TB BFD 30-32 (1982) (discussing the collection of data by the German federal border guard, "Bundesgrenzschutz").

tematically matched against the information contained in police data banks. The outcome was fit into individual criminal profiles indicating the habitual means of transport and the usual destinations, as well as the preferred lodging, and describing thus both the degree and the details of mobility of criminals. In the meantime, credit card companies adopted a comparable procedure in order to uncover fraudulent use of cards as quickly as possible.[92] The profiles are created by combining customer spending and travelling customs. All further uses of the particular credit card are matched against the individual's profile. Deviations from the recorded and computer-affirmed "normality" result in an additional, more thorough check before the charge to the card is accepted.

The close connection between the advances in retrieval techniques and the intensification of surveillance is probably best illustrated by the videotex experiences.[93] Interactive cable television services are already offered for catalog shopping, burglary and fire protection, electronic funds transfers, home monitoring of children and the elderly, energy management, and emergency medical assistance.[94] In each of these

---

[92] *See Unbeantwortete Datenschutzfragen,* Blick durch die Wirtschaft, Nov. 27, 1985, at 1, col. 2.

[93] For a general appreciation, see CNIL, 5ÈME RAPPORT D'ACTIVITÉ, 15 OCTOBRE 1983 - 31 DÉCEMBRE 1984, at 145 (1984) (describing related changes in information processing and notions of freedom); 7 TB BFD 24 (1985) (describing introduction and problems with German videotex system "Bildschirmtext" (Btx)); 12 TB HDSB 102-03 (1983) (discussing prevention of abuse of personal data in videotex processing); Nash & Bollier, *supra* note 62, at 67-72 (discussing the threat posed to individual privacy by interactive home-media because hometech information could be compiled to create an individual activity profile usable by other private and public agencies); Wachtel, *Videotex: A Welcome New Technology or an Orwellian Threat to Privacy?,* 2 CARDOZO ARTS & ENT. L.J. 287, 290 (1983) ("[Videotex] systems operators will be collecting massive amounts of personal data from subscribers. Whether the subscriber is ordering goods and services, answering inquiries, retrieving information, or utilizing the security services, he will be conveying his interests, choices, and views to the central computer."); Westin, *Home Information Systems: The Privacy Debate,* 28 DATAMATION 100 (July 1982) (describing ways cable television and telephone-based systems can be utilized by consumers, the dangers of private and public agencies gaining access to the personal information collected by the cable companies, and the need for individual protection through adoption of an industry code regulating information use); Comment, *Cable Television Privacy Act: Protecting Privacy Interest from Emerging Cable TV Technology,* 35 FED. COMM. L.J. 71, 79 (1983) (describing the danger of unauthorized access to private communications of consumers in the cable television industry).

[94] *See* 13 TB HDSB 60 (1984) (describing German TEMEX service which allows control of almost entire household); Nash & Smith, *supra* note 61, at 33-37 (describing Qube system, which uses interactive communication to assess viewer responses, bill for pay-TV services, and monitor home security); Westin, *supra* note 93, at 100, 103 (categorizing uses of cable television and telephone-based systems into eight groups: home banking, shop-at-home services, information services, home and personal security services, instant opinion polling, home study courses, special entertainment op-

cases, the subscriber's everyday life is painstakingly recorded.[95] A home modem, for instance, collects information from meters, hot water heaters, television sets, or any other major appliance by scanning the household up to every six seconds in order not only to control energy consumption but also to develop, if necessary, alternative patterns. The same mechanism applies to the monitoring services. The system conducts continuous sweeps of the subscriber's house and can thus constantly locate the persons to be surveyed. Where, therefore, anonymity was once the rule, complete transparency now dominates. It is little wonder that security agencies, advertisers, and direct-mail marketers have repeatedly underlined their interest in getting access to individual "home profiles."[96] Videotex is, therefore, further proof of the steady, but often imperceptible, transition in social control from physical coercion to observation and surveillance.[97] Automated processing paves the way to conformity by constantly improving the opportunities to follow and to retrace the individual's activities.[98]

III. Reviewing Privacy

A. *Privacy—A Refuge for the Individual*

The implications of automated processing can be viewed as merely

---

tions, and organizational fund raising).

[95] *See, e.g.,* 13 TB HDSB 60-61 (1984); Nash & Bollier, *supra* note 62, at 70 (household information that advertisers, direct-mail marketers, and cable television operators assemble can form a "psychographic" profile of an individual's activities); Wachtel, *supra* note 93, at 295 (describing how home media systems can put together a "home profile" of an individual's activities by compiling the massive amount of personal data acquired from a subscriber); Westin, *supra* note 93, at 103 (system operator can collect almost unlimited information about the subscriber's activities).

[96] *See* 13 TB HDSB 59-60 (1984); Nash & Smith, *supra* note 61, at 8-9; Nash & Bollier, *supra* note 62, at 70 (discussing the interest of private enterprises in "home profiles"); Westin, *supra* note 93, at 103, 111.

[97] In the 19th century, the prison system arose as the dominant form of punishment particularly because it provided a place to observe punished individuals. The prison system made it possible "to substitute for force or other violent constraints the gentle efficiency of total surveillance." M. Foucault, Discipline and Punish: The Birth of the Prison 249 (A. Sheridan trans. 1977).

[98] *See, e.g.,* Marx & Reichman, *supra* note 50, at 442.

> Rather than having to rely on what citizens happen to report or police accidentally discover, [social] control agents are taking greater initiative. . . . With a skeptical and scientific ethos and a broad data base that can be inexpensively screened, it becomes prudent to consider everyone a possible suspect initially. Analysis rather than tradition becomes the basis for action.

Id.; Simitis, *Datenschutz: Voraussetzung oder Ende der Kommunikation,* in 2 Europäisches Rechtsdenken in Geschichte und Gegenwart 513-14 (1982) (Festschrift für Helmut Coing).

a personal problem for the individuals concerned, because it is their data that are stored and retrieved and their activities and habits that are recorded. Indeed, until recently, most courts and legislators have seen no need for another approach. Consequently, as both the history and the text of the West German Federal Data Protection Act[99] and the Swiss draft[100] show, legislators and courts have legitimated data protection regulation by simple reference to traditional privacy concepts.

Processing problems are thus largely dealt with in terms already suggested in the course of the French Revolution and confirmed nearly 170 years later by article nine of the Code Civil: Everyone has the right to the protection of her private life.[101] Saint-Just's famous statement—"La liberté du people est dans sa vie privée; ne la troublez point. Que le gouvernement . . . ne soit une force que pour protéger cet état de simplicité contre la force même"[102]—not only rejects an autocratic political order but also expresses the conviction that a society that considers the freedom of individuals to act as its paramount regulatory principle must distinguish clearly between private and public life and preserve the intimacy of the former.[103]

The same view is found again in Warren and Brandeis's passionate pleading for the individual's right to be let alone.[104] Faced with

---

[99] *See* BDSG, § 1, ¶ 1. Section 1(1) describes the task of the law in rather unusual terms that are not easily understandable: to secure the "interests worthy of protection" of those concerned by data processing against its misuse. The meaning is nevertheless clear as the legislative materials show: to protect the personal interests of the individuals affected by the storage and retrieval of their data and thus to ensure the free development of their personality. *See* ENTWURF DES BDSG, BUNDESTAGS-DRUCKSACHE 7/1027, at 22; S. SIMITIS, U. DAMMANN, O. MALLMANN & H.J. REH, KOMMENTAR ZUM BUNDESDATENSCHUTZGESETZ 94 (3d ed. 1981) [hereinafter KOMMENTAR ZUM BDSG].

[100] EIDGENÖSSISCHES JUSTIZ- UND POLIZEIDEPARTMENT, BUNDESGESETZ ÜBER DEN SCHUTZ VON PERSONENDATEN: ENTWURF arts. 8-12, 36 (Dec. 5, 1983) [hereinafter Swiss draft data protection law); EIDGENÖSSISCHES JUSTIZ- UND POLIZEIDEPARTMENT, ERLÄUTERNDER BERICHT ZUM ENTWURF EINES BUNDESGESETZES ÜBER DEN SCHUTZ VON PERSONENDATEN 11, 30, 63 (Dec. 1983) (legislative comments on Swiss draft).

[101] C. CIV. art. 9 ("Chacun a droit au respect de sa vie privée.").

[102] A. DE SAINT-JUST, *Fragments sur les institutions républicaines,* in 2 OEUVRES COMPLÈTES 492, 507 (C. Vellay ed. 1908) ("The liberty of the people lies in their private lives; do not disturb it. Let the government . . . be a force only to protect this state of simplicity against force itself . . . .").

[103] *See also* J. BONNECASE, LA PHILOSOPHIE DU CODE NAPOLÉON APPLIQUÉE AU DROIT DE FAMILLE 84-85 (1928) (stating that examples such as the purely contractual view of marriage, establishing its free dissolubility, emphasize the sharp distinction between private and public life brought about by the French Constitution of 1791).

[104] *See* Warren & Brandeis, *supra* note 1, at 205. They state:

> [T]he protection afforded to thoughts, sentiments, and emotions, expressed through the medium of writing or of the arts . . . is merely an instance of

changes in the means of communication, they upheld and defended the right to an undisturbed private life.[105] Behind the claim for legally guaranteed privacy lies the expectation of all those who supported industrial expansion, advocated political and economic structures eliminating all obstacles to entrepreneurial initiative, and who regarded success, not birth, as the sole criterion legitimating social distinctions. Their desire was to enjoy, strictly for themselves and under conditions they determined, the fruits of their economic and social activity.[106] The right to be let alone was therefore increasingly hypostatized: privacy was considered a natural right binding courts and legislators. It permits and secures withdrawal from society. The *citoyen*'s access to information ends where the *bourgeois'* claim for privacy begins.

The more, therefore, that privacy is equated with a deliberate and legally protected seclusion of the individual, the more the right to be let alone develops into an impediment to the transparency necessary for a democratic decisionmaking process. As long as the data required to understand and evaluate the political and economic process are withheld, suppressed, or falsified, participation remains a pure fiction. Hence, publicity, and not secrecy, has been the outstanding feature of all efforts to secure participation in all aspects of decisionmaking.

Because the existence of a democratic society depends essentially on an uninhibited proliferation of information, privacy very quickly became one of the main objects of debate. In fact, free speech has been

---

the enforcement of the more general right of the individual to be let alone. It is like the right not to be assaulted or beaten, the right not to be imprisoned, the right not to be maliciously prosecuted, the right not to be defamed.

[105] *See id.* at 195. Additionally, they state:

> Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual . . . the right 'to be let alone.' Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life . . . . [O]f the desirability—indeed of the necessity—of some such protection, there can, it is believed, be no doubt.

[106] For a discussion of the political and social background of the period during which the need for a right of privacy became explicitly recognized, see G. BLODGETT, THE GENTLE REFORMERS: MASSACHUSETTS DEMOCRATS IN THE CLEVELAND ERA (1966) (detailing the roots and development of the Mugwumps, a group of nineteenth-century political independents); A. WESTIN, PRIVACY AND FREEDOM 348-49 (1967) (stating that the privacy movement was "essentially a protest by spokesmen for patrician values against the rise of the political and cultural values of 'mass society' "); Barron, *Warren and Brandeis,* The Right to Privacy, 4 Harv. L. Rev. 193 (1890): *Demystifying a Landmark Citation,* 13 SUFFOLK U.L. REV. 875 (1979) (criticizing the frequently cited Warren and Brandeis article as merely espousing the minority view of newsworthiness of the Mugwumps and attempting to create and romanticize a new legal right of privacy based on this view).

seen, to a substantial extent, as a product of the constant adjustment of the boundary between the individual's right to be let alone and the public's need to be informed. The standard remarks on the relative nature of privacy or on the necessity of a careful balancing of interests[107] are more than significant. Far from being considered a constitutive element of a democratic society, privacy appears as a tolerated contradiction, the implications of which must be continuously reconsidered. The *New York Times Co. v. Sullivan,*[108] *Lebach,*[109] *Curtis Publishing Co. v. Butts,* [110] and *Kohl/Biedenkopf*[111] cases all illustrate the constant to and fro between the effort to improve transparency and the tendency to preserve some degree of inaccessibility.

B. *Privacy—A Condition of Participation*

Both the quest for greater transparency and the defense of free speech are legitimated by the goal of allowing the individual to under-

---

[107] Examples can be easily found in the decisions of most courts. For West Germany, *see, e.g.,* Soraya case, 34 BVerfGE 269, 280-82 (1973) (stating that even where the conflict at stake concerns at first only the relationship between purely private parties, the need to respect and ensure the freedom of the press may restrict the individual's right to the free development of her personality); Panorama, 66 BGHZ 183, 186-87 (1976) (describing interests to be balanced in evaluating critical comments made on German public television); M. F.-Bank case, 36 BGHZ 80 (1961) (advocating restrictions of privacy protection in cases of publications concerning business activities). For Switzerland, *see, e.g.,* Judgment of Sept. 23, 1982, 108 BGE II at 344, 344 (stating that a person who intentionally and repeatedly disturbs the family life of a married couple by claiming to be the father of their children violates the privacy right of the couple); Judgment of July 3, 1975, 101 BGE II at 177, 197 (stating that a violation of the privacy right is not illegal when mandated by superior interests and that the decision on illegality depends on the balancing of the competing interests); *see also* M. PEDRAZZINI & N. OBERHOLZER, GRUNDRISS DES PERSONENRECHTS 134-35 (2d ed. 1985) (discussing balancing of interests in application of ZGB art. 28, para. 1 (Switz.). For an overview of the various interests directly connected to retrieval problems, see Morand, *Problèmes constitutionnels relatifs à la protection de la personnalité à l'égard des banques de données électroniques,* in INFORMATIQUE ET PROTECTION DE LA PERSONNALITÉ 15, 19-33 (1981) (assessing the individual interest in privacy and effective functioning of government).

[108] 376 U.S. 254 (1964) (holding that mere factual error in a defamation case is insufficient to warrant an award of damages).

[109] Judgment of June 5, 1973, 35 BVerfGE 202 (The constitution's protection of privacy does not allow television to invade the private sphere of a criminal offender beyond normal reporting. Later reporting, e.g., in the form of a documentary film, is impermissible when it harms the individual, particularly if her rehabilitation is put at risk.).

[110] 388 U.S. 130 (1967) (refusing to extend the *Sullivan* rule to require actual knowledge of falsehood in a defamation action brought by a "public figure").

[111] Judgment of Dec. 19, 1978, 73 BGHZ 120, 129 (In discussing a case involving the publication of a private telephone call between two high-ranking German politicians, the court stated that only a very serious need on the part of the public for information could justify such exposure of the individual's private sphere.).

stand social reality better and thus to form a personal opinion on its decisive factors as well as on possible changes. The citizen's right to be "a participator in the government of affairs," to use Jefferson's terms,[112] reflects a profoundly rational process. It presupposes individuals who not only disperse the necessary information but also have the capacity to transform the accessible data into policy expectations. Transparency is, in other words, a basic element of competent communicative action[113] and consequently remains indispensible as long as social discourse is to be promoted, not inhibited.

Inhibition, however, tends to be the rule once automated processing of personal data becomes a normal tool of both government and private enterprises. The price for an undoubted improvement in transparency is a no less evident loss in competence of communication. Habits, activities, and preferences are compiled, registered, and retrieved to facilitate better adjustment, *not* to improve the individual's capacity to act and to decide. Whatever the original incentive for computerization may have been, processing increasingly appears as the ideal means to adapt an individual to a predetermined, standardized behavior that aims at the highest possible degree of compliance with the model patient, consumer, taxpayer, employee, or citizen. Furthermore, interactive systems do not, despite all contrary assertions,[114] restore a long lost individuality by correcting the effects of mass production in a mass society. On the contrary, the telematic integration forces the individual once more into a preset scheme. The media supplier dictates the conditions under which communication takes place, fixes the possible subjects of the dialogue, and, due to the personal data collected, is in an increasingly better position to influence the subscriber's behavior. Interactive systems, therefore, suggest individual activity where in fact no more than stereotyped reactions occur.[115]

In short, the transparency achieved through automated processing

---

[112] Letter from Thomas Jefferson to Joseph C. Cabell (February 2, 1816), in 14 THE WRITINGS OF THOMAS JEFFERSON 417, 422 (Monticello ed. 1904).

[113] For the concept and the premises of a competent theory of communicative action, see J. HABERMAS, 1 THE THEORY OF COMMUNICATIVE ACTION 75-102, 273-338 (1983).

[114] *See, e.g.*, E. FEIGENBAUM & P. MCCORDUCK, THE FIFTH GENERATION (1983) (suggesting that the development of computer technology or artificial intelligence is the means of acquiring power and pre-eminence); A. TOFFLER, THE THIRD WAVE 200-02 (1980) (suggesting that individuals will not be dominated by technology and that technological processes will be "increasingly under the direct control of the consumer" because changes in technology and information storage and collection are moving manufacturing beyond traditional mass production).

[115] *See* Rodotà, *supra* note 11, at 201; S. GARDNER & R. WHITE, NEW TECHNOLOGY AND THE RIGHT TO PRIVACY: STATE RESPONSES TO FEDERAL INACTION, A REPORT TO THE NEW YORK STATE CONSUMER PROTECTION BOARD (1983).

creates possibly the best conditions for colonization of the individual's lifeworld.[116] Accurate, constantly updated knowledge of her personal history is systematically incorporated into policies that deliberately structure her behavior. The more routinized automated processing augments the transparency, however, the more privacy proves to be a prerequisite to the capacity to participate in social discourse. Where privacy is dismantled, both the chance for personal assessment of the political and societal process and the opportunity to develop and maintain a particular style of life fade.

For precisely this reason the West German Federal Constitutional Court, in the *National Census Case ("Volkszählungsurteil")*—its landmark decision on the census law—spoke of the individual's right to an "informational self-determination".[117] According to the court, unrestricted access to personal data imperils virtually every constitutionally guaranteed right. Neither freedom of speech nor freedom of association nor freedom of assembly can be fully exercized as long as it remains uncertain whether, under what circumstances, and for what purposes, personal information is collected and processed. In view of these implications of automated data processing, considerations of privacy protection involve more than any one particular right: they determine the choice between a democratic and an authoritarian society.[118]

If, as Jefferson suggests, democratic participation presupposes con-

---

[116] For both the colonization process and the impact of the individual's lifeworld on communicative action, *see* J. HABERMAS, *supra* note 113, at 70-71 (defining "lifeworld" as shared understandings about what will be treated as a fact, valid norms, and subjective experience); J. HABERMAS, 2 THEORIE DES KOMMUNIKATIVEN HANDELNS: ZUR KRITIK DER FUNKTIONALISTISCHEN VERNUNFT 173 (1981).

[117] Volkszählungsurteil, 65 BVerfGE 1, 68-69 (1983). The National Census Statute, Gesetz über eine Volks-, Berufs-, Wohnungs- und Arbeitsstättenzählung (Volkszählungsgesetz), Mar. 25, 1982, BGBl.I 369 (1982) ordered West German citizens to disclose personal data and foresaw a transmission of the information to the various branches of government. The Court held major portions of the statute to be unconstitutional especially because it did not explicitly exclude uses of the data other than those for exclusively statistical purposes.

[118] *See* Maisl & Vitalis, *Les libertés: enjeu d'une société informatisée,* 1985 ETUDES 471 (examining the general effects of an information society on individual and collective liberties and advocating greater public participation at earlier stages of decisionmaking about information use); Rodotà, *supra* note 11, 196-198 (referring to a 1968 U.N. resolution regarding use of electronics as an interference with citizens' rights). Significantly enough, the French legislature deliberately avoided the term "data protection" and spoke instead of "informatique et libertés"—automated processing and liberties—thus stressing the necessity of a broader view and clearly underscoring the structural importance of efficient privacy protection for the existence of a democratic society, *see* CNIL, RAPPORT DE LA COMMISSION INFORMATIQUE ET LIBERTÉS 16-23, 83-85 (1975) (indicating the necessity of enabling individuals to be aware of and to discuss the various uses of automated processing).

stant interaction between public and private life,[119] the protection of privacy must be accompanied by an equally efficient, guaranteed access to the information necessary to follow and evaluate social processes. Indeed, the very first step to cope with the implications of automated retrieval, the 1970 Hessian Data Protection Act, included a series of access rules.[120] Fourteen years later, the Quebec Act addressed both data protection and freedom of information in a single statute.[121] Each of these laws has a clearly limited scope, covering access in only a few selected instances.[122] They nonetheless reveal that social discourse depends on an information allocation policy that, through a mix of withholding and access, reflects a precise analysis and understanding of the consequences of automated processing for both the individual and society.[123] The contrary result is achieved, however, when privacy protection is more or less equated with an individual's right to decide when and which data are to be accessible. The regulation thus reverts to well-known property schemes and leads to the division and monopoli-

---

[119] *See* Letter from Thomas Jefferson to Joseph C. Cabell, *supra* note 112, at 422-23; *see also* Letter from Thomas Jefferson to James Monroe (May 20, 1782), in 4 THE WRITINGS OF THOMAS JEFFERSON 193, 196 (Monticello ed. 1904) ("Nothing could so completely divest us of . . . liberty as the establishment of the opinion, that the State has a perpetual right to the services of all its members.").

[120] *See* Datenschutzgesetz, Oct. 7, 1970, § 6, 1 Gesetz- und Verordnungsblatt für das Land Hessen 625 (1970) (West German state of Hesse data protection act). For the history and development of the law, see Simitis, *Datenschutzrecht,* in HESSISCHES STAATS- UND VERWALTUNGSRECHT 111-114 (H. Meyer & M. Stolleis eds. 1983).

[121] An Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information (as last amended on July 4, 1984), QUÉ. REV. STAT. ch. A-2.1 (1984); *see also* QUEBEC MINISTRY OF COMMUNICATIONS, INFORMATION ET LIBERTÉ: RAPPORT DE LA COMMISSION D'ÉTUDE SUR L'ACCÈS DU CITOYEN À L'INFORMATION GOUVERNEMENTALE ET SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS 14-18 (1981) (discussing the need for comprehensive legislation that would result from public debate over and consensual resolution of the issues surrounding the regulation of information).

[122] The access to personal data for research purposes, *see* Datenschutzgesetz, Nov. 11, 1986, § 33, 1 Gesetz- und Verordnungsblatt für das Land Hessen 309 (1986) [hereinafter 3d Hessian Data Protection Act], the openness of documents held by public bodies, *see* An Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information (as last amended on July 4, 1984), QUE. REV. STAT. ch. A-2.1 (1984), and the balance of information between Parliament and government, *see* 3d Hessian Data Protection Act, §§ 1(2), 24(2), are probably the most typical examples. *See also* Lov. nr. 293 om private registre m.v. (Private Registers Act), June 8, 1978, § 2(2), 2 Karnovs Lovsamling 2859 (1978) (Den.), *reprinted in* 5 Computer Law Serv. (Callaghan) app. 9-5.2a, no. 6 (1979) (protection does not apply to data collected for scientific, statistical, or biographical research).

[123] *See* CNIL, 3ÈME RAPPORT D'ACTIVITÉ, 15 OCTOBRE 1981 - 15 OCTOBRE 1982, at 65 (1983) (specifying that freedom of access law extends access to noncomputerized files not protected by the privacy law); Maisl & Vitalis, *supra* note 118, at 477 (urging an aggressive and comprehensive approach to organizing and planning the processing of technological information).

zation of personal information.[124] Public and private life are irrevocably disconnected. Open or hidden "sanctifications" of property sacrifice the *citoyen*[125] and reduce the *constitutio libertatis* to a mere guarantee of the *bourgeois'* refuge.

The reports of the West German Data Protection Agencies, especially on retrieval practices in the insurance, credit, and medical sector[126] and the remarks of the United States Privacy Protection Study Commission on access to data of "captive populations"[127] demonstrate the chimerical nature of the assumption that effective protection of privacy can be accomplished by simply entrusting the processing decision to the persons concerned. Whether or not the details of the intended retrieval are explained to them, hospital patients, bank customers, and employees cannot determine the proper data processing conditions, even though their consent to disclosure of information is required.[128] The

---

[124] *See* H. MEISTER, DATENSCHUTZ IM ZIVILRECHT 111, 113 (1977). For a critical appreciation, see A. MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS 211-16 (1971) (criticizing use of property notions as means of regulation on grounds that they are irrelevant and inappropriate); KOMMENTAR ZUM BDSG, *supra* note 99, at 272. Therefore, as appropriate as it may appear to define privacy as the individual's claim to determine the conditions under which personal information can be disseminated, *see* A. MILLER, *supra,* at 25; A. WESTIN, *supra* note 106, at 7, this definition encourages the widespread tendency to disregard the indissoluble connection between data protection and freedom of information. As a consequence, inconsistencies and contradictions burden the attempts to establish rules governing the allocation of information. For a detailed discussion, see, for example, Kronman, *The Privacy Exemption to the Freedom of Information Act,* 9 J. LEG. STUDIES 727 (1980) (discussing the balance of data protection and access from the perspective of maximizing economic efficiency).

[125] *See* H. ARENDT, ON REVOLUTION 255-56 (1965).

[126] *See, e.g.,* 7 TB BFD 83 (1985); 5 TB BFD 75 (1983); 2 TB BFD 55 (1980) (all discussing data protection in insurance and banking fields); 13 TB HDSB 115 (1984); 12 TB HDSB 82 (1983); 11 TB HDSB 22 (1982) (all discussing data banks in medical and psychiatric fields).

[127] *See* PRIVACY PROTECTION STUDY COMM'N, *supra* note 35, at 85-87, 196-198, 314-316.

[128] Consider the debate on the need for specific privacy protection regulation in view of the implications of videotex. Not only has the individual's right to choose what should be revealed been repeatedly stressed, but, as the Warner Amex Cable Communications Code of Privacy (1981) or the Model Privacy Guidelines for Videotex Systems released in 1983 by the Videotex Industry Association show, the proposals for self-regulation that were developed were clearly intended to preempt attempts at state intervention. *See* Neustadt & Swanson, *Privacy and Videotex Systems,* 8 BYTE 98, 98 (July 1983), *reprinted in 1984: Civil Liberties and the National Security State, Hearings Before the Subcomm. on Courts, Civil Liberties, and the Administration of Justice of the House Comm. on the Judiciary,* 98th Cong., 1st & 2d Sess. 103-04 (1983-84). Both the experience with retrieval of subscriber data and a close study of the various rules reveal, however, that the assumed control and interference opportunities are fictitious, due to the deliberately vague formulation of the policies and the subtleties of the disclaimers. Additionally, self-regulation can at best, even if it functions well, secure partial protection. None of the provisions proposed is an effective access shield against the government's retrieval expectations. It is therefore quite correct but still an under-

process of consent is no more than a "mystification" that ignores the long-standing experience that the value of a regulatory doctrine such as "informed consent" depends entirely on the social and economic context of the individual activity.[129]

An allocation of information that secures the necessary degree of proliferation without invading privacy can only be achieved through a mandatory framework for the processing of personal data. It should be clear, however, that while such rules may provide convincing answers to the specific questions arising out of the retrieval of personal information, they will never respond satisfactorily to all the problems assembled under the privacy rubric.[130] Both the claim for and content of any regulation are legitimated by the awareness of the implications of constantly perfected information processing. The commitment to privacy reflects specific experiences, concerns, and expectations. The more particular, therefore, the reaction to the peculiar aspects of intensified data processing, the better the chances of successful regulatory intervention.

C. *Data Processing—Basic Elements of a Regulation*

Despite their different approaches to the problem,[131] statutes, drafts, administrative procedures, court decisions, and reports of control agencies now offer a solid basis for identifying at least four essentials of an efficient processing regulation. First, the unique nature of the personal data processing must be recognized. Second, requests for personal information must specify the purpose for which the data will be used, thereby excluding all attempts at multifunctional processing. Third, data protection regulations must be reviewed and updated constantly to

---

statement, to conclude that "the moment has been reached at which industry pleas of *laissez innover* are not persuasive." Westin, *supra* note 93, at 112. For a discussion of the regulatory principles, see 13 TB HDSB 53 (1984).

[129] For an illustration of the difficulties and circumventing techniques in a typical sector—medical treatment—see J. KATZ, THE SILENT WORLD OF DOCTOR AND PATIENT 48-84 (1984).

[130] Although this idea may indeed appear to be a "reductionist" approach, *see* Gavison, *supra* note 10, at 422, 460-67, it is the only way to replace meaningless abstract commitments with precise and legally binding privacy policies.

[131] For an overview of the development of data protection regulations, see F. HONDIUS, EMERGING DATA PROTECTION IN EUROPE (1975); KOMMENTAR ZUM BDSG, *supra* note 99, at 77 (discussing developments in West Germany, Sweden, USA, and England); STUDY ON DATA SECURITY AND CONFIDENTIALITY, FREEDOM OF INFORMATION AND DATA PROTECTION, DRAFT FINAL REPORT TO THE COMMISSION FOR THE EUROPEAN COMMUNITIES AND NATIONAL GOVERNMENTS (1983); Hondius, *Data Law in Europe*, 16 STAN. J. INT'L L. 87 (1980). The annual reports of the West German Federal Data Protection Comissioner ("BfD") and the French Data Protection Commission ("CNIL") also provide overviews of recent developments in their respective countries. For a detailed bibliography on the subject, see D. FLAHERTY, PRIVACY AND DATA PROTECTION, AN INTERNATIONAL BIBLIOGRAPHY (1984).

reflect changes in technology. Finally, there must be an independent authority to enforce data regulations.

1. The Unique Nature of Personal Data Processing

The collection and retrieval of personal data must be viewed and treated as an exceptional means to obtain information. Government as well as private enterprises have, for far too long, considered the use of personal data to be the norm. Instead of asking how to perform their task without resorting to personal information, their interest has concentrated on developing new and better retrieval methods. Advances in processing have become synonymous with easier and quicker access to a steadily growing amount of data usable for more and more purposes.[132] Consequently, where a "convenient" use of computers appears to be the sole concern, purely technocratic considerations have held sway over all others.

Hence, despite the importance of the content of rules governing the collection and retrieval of personal data, the primary aim must be a radical revision of the information *methods.* Yet, as the ongoing census debate in West Germany shows,[133] what in theory appears clearly necessary is in practice not at all easy to accomplish.[134] When, during the proceedings in front of the West German Federal Constitutional Court,[135] the Federal Statistical Office was asked whether the entire population really had to provide such personal data, the Office replied by reminding the judges of the Office's duty to keep all data secret and pointing to the fact that the census had always been conducted in that manner. It obviously never occurred to the Office that the increased demand for and accelerated proliferation of personal data should induce some thought about future comprehensive collections. The Court's reac-

---

[132] *See* A. MILLER, *supra* note 124, at 20-23 (Increased access to automatically processed data increases demand for such data.).

[133] For a discussion of the background and main area of conflict, see 12 TB HDSB 7 (1983) (discussing the present state of affairs following the German Constitutional Court's invalidation of major sections of the National Census Statute).

[134] For the experience in other countries, see CNIL, 2ÈME RAPPORT, *supra* note 30, at 21-22; D. FLAHERTY, *supra* note 82, at 39-47; T. Dalenius, *Finding a Needle in a Haystack,* 2 J. OFFICIAL STATISTICS 329 (1986); F. Rapaport, *Legal and Technical Means for Protecting Data in the Production of Statistics,* 2 STATISTICAL J. U.N. 21 (1984).

For a review of the United States' experience in this area, see D. BURNHAM, *supra* note 35, at 18-117; Burnham, *Census Bureau Fighting Plan to Share its Personal Data,* N.Y. Times, Nov. 20, 1983, at A1, col. 1; *White House Kills Plan to Force Census Bureau to Share Data,* N.Y. Times, Nov. 24, 1983, at A16, col. 1.

[135] On the constitutionality of the census law enacted in 1982 by the West German Federal Parliament, BGBl.I 369 (1982), see Volkszählungsurteil, 65 BVerfGE 1, 55 (1983), discussed *supra* note 117.

tion was brief and precise: statistical offices, like any other part of government, must constantly review their information methods in order to minimize citizens' involvement.[136] Two years later, the West German Federal Parliament, in an opinion accompanying the enactment of a series of new statistic laws, explicitly advocated a change from coercive to voluntary participation.[137] Similarly, both the Council of Europe and the European Science Foundation stressed the importance of dialogue with the persons concerned, advocating the use of personal data only as an auxiliary source of information and urged the development of new research methods relying on anonymized or aggregated data.[138]

None of these efforts ultimately can eliminate the processing of personal information, which in a great number of situations in the public as well as the private sector serves both the user and the individual under scrutiny. Nevertheless, once priorities on information use are clearly set, the burden of proof will be reversed. Whoever asks for personal data will be obliged to explain why and to what extent her particular purposes cannot be fullfilled by using other information. The result should be a substantial reduction in the use of personal data.[139]

In order to achieve this goal, however, more than a purely normative approach is needed. Technical resources also must be mobilized. Instead of a simple focus on the convenience of the potential user, the safeguarding of privacy must become an equally powerful consideration in all further development of information technology.[140] Hardware and software should, like motor vehicles or medicine, meet certain safety

---

[136] Volkszählungsurteil, 65 BVerfGE 1, 55-56 (1983).

[137] BUNDESTAGS-DRUCKSACHE 10/3328, at 3 (May 14, 1985) (legislative material on new West German national census statute passed in reaction to the invalidation of the previous statute by the German Constitutional Court).

[138] COUNCIL OF EUROPE, PROTECTION OF PERSONAL DATA USED FOR SCIENTIFIC RESEARCH AND STATISTICS 2.1 to 2.2 (1984) (Recommendation No. R (83) 10, adopted by the Committee of Ministers of the Council of Europe on Sept. 23, 1983) (calling for respect of individual privacy and use of anonymous data in research projects using personal data); European Science Foundation, *Statement Concerning the Protection of Privacy and the Use of Personal Data for Research,* § 1.5 (1980) (adopted by the Assembly on the European Science Foundation on Nov. 12, 1980) ("[R]esearch should, wherever possible, be undertaken with anonymised data."); *see also* Simitis, *Data Protection and Research: A Case Study of Control,* 29 AM. J. COMP. L. 583, 600-04 (1981) (discussing minimization of personal data use).

[139] *See* PRIVACY PROTECTION STUDY COMM'N, *supra* note 35, at 513 (Even the relatively modest specificity requirements of the U.S. Privacy Act "seem[] to have resulted in a modest . . . reduction in data collection itself.").

[140] Even the most efficient technical means can, however, never replace normative barriers. Whether, and under what circumstances, the collection as well as the retrieval of certain data should be accepted is not a technical but a normative question. Only a legally binding provision can therefore provide a satisfactory answer. For a discussion of the relationship between normative and technical instruments in the history of data protection, see Simitis, *supra* note 40, at 46.

requirements before being put on the market. They should have a minimum of built-in protective devices. This requirement is by no means a utopian expectation. Smart cards and videotex can, at least for payment purposes, be designed in a way that demands almost no collection of personal data.

2. The Clearly Specified Purpose of Processing Requests

Personal information should only be processed for unequivocally specified purposes. Both government and private institutions should abstain from collecting and retrieving data merely for possible future uses for still unknown purposes. Both national[141] and international[142] organizations have in fact rejected the unlimited build-up of data files. In order to be retrieved, data must be necessary to a precise goal that is within the legally acknowledged activities of the organization interested in the information. A normative barrier thus prevents the technically possible multifunctional use of the data.

Yet, attempts to elude this restriction have never ceased because most government branches and private enterprises still consider multifunctionality as the decisive advantage of automated processing. The considerable amount of skill invested in exploiting loopholes in the 1974 United States Privacy Act provides a significant example.[143] Provisions reducing or even eliminating the otherwise mandatory standards of justification in cases of "routine" use are a standing invitation to circumvent the obligation to connect every processing with a clearly discernable purpose. Therefore, massive data transfers are legitimated simply by qualifying them as purely routine "housekeeping" measures.[144] Similarly, difficulties with regard to matching programs can

---

[141] *See supra* notes 133-36 and accompanying text (the example of the invalidation of the West German census statute).

[142] *See* Convention for the Protection of the Individual with regard to Automatic Processing of Personal Data, *opened for signature* Jan. 28, 1981, art. 5(b), Europ. T.S. No. 108 ("Personal data undergoing automatic processing shall be . . . stored for specified and legitimate purposes and not used in a way incompatible with those purposes . . . ."), *quoted in* COUNCIL OF EUROPE, EXPLANATORY REPORT ON THE CONVENTION FOR THE PROTECTION OF THE INDIVIDUAL WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA 32 (1981); Guidelines on the Protections of Privacy and Transborder Flows of Personal Data, *adopted and applicable* Sept. 23, 1980, art. 9 ("The purposes for which personal data are collected should be specified not later than at the time of data collection . . . ."), *quoted in* ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT, GUIDELINES ON THE PROTECTIONS OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA 10 (1981).

[143] *See* PRIVACY PROTECTION STUDY COMM'N, *supra* note 35, at 515-16.

[144] *Privacy Act Guidelines,* 40 Fed. Reg. 28,949, 28,953 (1975) (issued by United States Office of Management and Budget).

be avoided by pointing to their "routine" character.[145]

The limitation of purpose-bound processing not only affects the actual handling of the data but also has far-reaching organizational consequences. The purpose delineates both the internal and the external use. Whether the user is an insider or an outsider, the specific aim legitimating the collection restricts any further processing. Consequently, government in particular no longer can be treated as a single information unit, justifying a free flow of data among all governmental units. An agency's specific functions and their relationship to the particular purpose that led to the collection of the data determine the access to the information, not the mere fact that the agency is part of the government. The internal structure of government, therefore, must be reshaped to meet the demands of functional separation that inhibits proliferation tendencies.[146]

3. The Continual Review of Regulations

The regulation of personal data collection and retrieval should be regarded as a constant learning process based on continual observation of both the changes in information techniques and the conflicts generated by systematic data use. Most legislators adopt a different attitude.[147] They restrict themselves to a few extremely abstract provisions that reflect both their hope of coping once and for all with the processing problems and their complete uneasiness in dealing with a technol-

---

[145] *See Supplemental Guidance For Matching Programs,* 44 Fed. Reg. 23,138, 23,141 (1979); *see also* UNITED STATES GEN'L ACCOUNTING OFFICE, PRIVACY ACT: FEDERAL AGENCIES' IMPLEMENTATIONS CAN BE IMPROVED 31-36 (Report to the Chairman, Subcomm. on Gov't Information, Justice, and Agriculture of the House Comm. on Gov't Operations, Aug. 1986, GAO/GGD-86-107) (discussing actual matching practices of federal agencies); Kirchner, *Privacy: A History of Computer Matching in Federal Government,* COMPUTERWORLD, Dec. 14, 1981, at 1, 2 (critical analysis of excessive use of matching programs).

[146] *See, e.g.,* Volkszählungsurteil, 65 BVerfGE 1, 68-69 (1983) (holding that governmental agencies, especially on the county level, must be organized to guarantee that data is used only for purpose for which it is collected); 10 TB HDSB 66-68 (1981) (For purposes of data use, a municipality cannot be considered a single unit: data protection provisions must apply when one municipal office transfers data to another office.). The concept of a "functional separation" was first developed in connection with the processing of personal data for research purposes. The inaccessibility of the data was and is seen as the primary condition for establishing a regulation allowing processing based on the particular research needs. *See* COUNCIL OF EUROPE, *supra* note 138, at 4.1; PRIVACY PROTECTION STUDY COMM'N, *supra* note 35, at 572-74; European Science Foundation, *supra* note 138, at §2.5 ("Personal Data obtained for research should not be used for any purpose other than research."); Simitis, *supra* note 138, at 597.

[147] For an analysis of the various legislative concepts, *see* KOMMENTAR ZUM BDSG, *supra* note 99, at 77.

ogy the further developments of which are as difficult to foresee as their exact implications.

None of the early laws, therefore, reacted effectively to the evolution of information procedures.[148] Contrary, for instance, to early assumptions, the structure of processing has not been determined by the establishment of huge data banks nor has access to information systems proven to be a privilege reserved to an elite of specialists.[149] Furthermore, the conditions justifying a retrieval can only be defined by carefully considering the particular characteristics of the area in which the data are to be used. For example, a retrieval for social security purposes should be premised on a careful analysis of the welfare system involved. The same applies to electronic banking. Whether the solutions to the problems in this area really work depends on the ability to integrate the conflict structures characteristic of the credit sector into the applicable regulatory scheme.[150]

Efficient protection thus begins when the quest for abstract, generally applicable provisions is abandoned. The emphasis must shift to a context-bound allocation of information embodied in a complex system of both specific and substantive regulations.[151] Yet, no matter how precise the rules, they nevertheless remain provisional measures because of the incessant advances in technology. Regulations on the collection and retrieval of personal data thus present a classic case of sunset legislation.[152] If the legislator wants to master processing issues, she must commit herself explicitly to a constant reappraisal of the various rules.

4. An Independent Data Control Authority

Efficient regulation presupposes the establishment of an independent control authority. Experience confirms what was argued in the earliest debates: a mandatory framework for data processing is not suf-

---

[148] *See* Simitis, *General Report,* in BEYOND 1984, *supra* note 27, at 109, 113-14.

[149] *See* Soma & Wehmhoefer, *A Legal and Technical Assessment of the Effect of Computers on Privacy,* 60 DEN. L.J. 449, 450-54 (1983) (describing growth and availability of relatively inexpensive computers).

[150] *See id.* at 463-65 (discussing the balancing of interests embodied in the Fair Credit Reporting Act).

[151] This is a tendency which is becoming more and more obvious, particularly in connection with the processing of personal data for social security, police, or videotex purposes. *See* Rodotà, *supra* note 11, at 222, 234 (recommending flexible instead of strict rules); Simitis, *supra* note 40, at 44.

[152] For example, art. 31 of the 1985 Icelandic Law on the Systematic Recording of Personal Data explicitly requires that the existing provisions be replaced by a new regulation by December 31, 1989. *See* COUNCIL OF EUROPE, COMMITTEE OF EXPERTS ON DATA PROTECTION, REPORT OF ICELANDIC ACT NO. 39/1955 ON SYSTEMATIC RECORDING OF PERSONAL DATA (1986).

ficient.[153] The legislator must also provide a control to monitor collection and retrieval conditions. Neither intervention by the data subject nor any of the traditional control mechanisms guarantees adequate supervision. Even if the persons concerned are entrusted with control rights, they remain, as a rule, outsiders, deprived of the knowledge necessary to understand and evaluate the activities of the various government agencies and private institutions. The obvious conflict of interest discredits all attempts to reduce the supervision to purely internal procedures. Finally, both the technical knowledge essential for effective monitoring and the necessary intensity of the supervision exclude supervision by any of the other existing control authorities.[154]

Despite the growing readiness to combine substantive regulatory provisions on information processing with the establishment of a particular control institution, the difficulties in implementing efficient monitoring are still considerable. Although it is undisputed that the control authority must be clearly separated from all the potential data users, this "independence" of the control authority, generally considered the crucial element of true supervision, remains hard to define. Certainly, an equidistance from both the public and the private sector constitutes the first and foremost condition of independent supervision. It is precisely for this reason that the Hessian Data Protection Act links the control authority to the Hessian Parliament.[155]

The West German solution—the establishment of a Data Protection Commissioner—indicates the insufficiency of traditional monitoring mechanisms in highly industrialized societies marked by rapid advances in information technology. The existence of a separate control authority reflects, to a large extent, Parliament's difficulties in exercising its own control tasks in an area vital to the structure and development of society. In other words, because Parliament cannot by itself adequately oversee the consequences of automated processing, a paraparliamentary institution takes over a genuine parliamentary activity.

The integration into the parliamentary organization also underlies the essential difference between the Data Protection Commissioner and

---

[153] *See, e.g.*, ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, POLICY ISSUES IN DATA PROTECTION AND PRIVACY 13-19, 56-103 (1976) (Proceedings of the OECD Seminar, June 24-26, 1974); PRIVACY PROTECTION STUDY COMM'N, *supra* note 35, at 34-35; U. DAMMANN, DIE KONTROLLE DES DATENSCHUTZES 11-13 (1977).

[154] The question whether the control tasks could be assigned to one of the existing control authorities is discussed extensively in U. DAMMANN, *supra* note 153, at 101-114, 131-185.

[155] 3d Hessian Data Protection Act, §§ 21-31; Simitis, *supra* note 120, at 128-29.

nearly every other state agency created during the last decades. Its task consists not of helping government enforce its policies but of preventing both government and private institutions from overstepping the boundaries guaranteeing the democratic structure of society. Therefore, the possibility of conflict with state agencies and private enterprises is ever present. The potential for a clash, especially with the government, has induced some legislatures to entrust the control task to a commission.[156] All conflicts over the collection and retrieval of personal data are handled by a group of carefully selected persons representing the major political and societal interests. The need for continuously renewed compromise thus governs control activities. In addition, commissions including representatives of government branches and of private organizations processing personal data tend to internalize all controversies and therefore to inhibit genuine public debate or at least to reduce substantially its topics. Hence, the control authority runs the risk of becoming an agency that legitimates processing practices and new information-gathering methods, rather than an agency that monitors and, if necessary, openly condemns them.

Another no less noteworthy obstacle to true supervision results from the often sharply restricted jurisdiction of the control authorities. West German law, for instance, prescribes independent commissioners only for the public sector.[157] Private institutions are also monitored, but by agencies fully integrated into government.[158] Unlike the commissioners, none of these agencies is under the obligation to report its activities

---

[156] *See, e.g.* Loi relative à l'informatique, aux fichiers et aux libertés, Loi No. 78-17 of 6 January 1978, arts. 6-13, 1978 J.O. 227, 1978 B.L.D. 77 (French data protection law); Lov. nr. 48 om personen registre (Personal Data Registers Act), June 9, 1978, § 2 (Nor.), NORGER LOVER 1685-1985, at 2180 (Oslo 1986) [hereinafter Norwegian personal data registers law], *reprinted in* 5 Computer Law Serv. (Callaghan) app. 9-5.2a, no. 5 (1979); Landesgesetz zum Schutze des Bürgers bei der Verarbeitung personenbezogener Daten, Dec. 21, 1978, §§ 17-22, Gesetz- und Verordnungsblatt für das Land Rheinland-Pfalz 749 (1978) (West German state of Rheinland-Pfalz data protection act); Swiss draft data protection law, *supra* note 100, at arts. 44-56; *see also* CNIL, BILAN ET PERSPECTIVES, *supra* note 32, at 15-23 (1980) and CNIL, 2ÈME RAPPORT, *supra* note 30, at 9-11 (1982) (discussing the nature, mission, and organization of the CNIL); Selmer, *Norwegian Privacy Legislation,* in J. BING & K. SELMER, A DECADE OF COMPUTERS AND LAW 45 (1980) (discussing the Norwegian Data Inspectorate, established by the Personal Data Registers Act as a monitoring body).

[157] *See, e.g.* BDSG §§ 17-21; Bayerisches Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der Datenverarbeitung (Bayerisches Datenschutzgesetz), Apr. 28, 1978, §§ 27-28, Bayerisches Gesetz- und Verordnungsblatt 165 (1978) (West German state of Bavaria data protection act); 3d Hessian Data Protection Act §§ 3, 24(1); *see also* KOMMENTAR ZUM BDSG, *supra* note 99, at 590 (discussing commissioners' rights and control difficulties).

[158] *See* BDSG §§ 30, 40; KOMMENTAR ZUM BDSG, *supra* note 99, at 917, 1089 (discussing the role of the state agencies controlling the application of the data protection rules in the private sector).

regularly and in public. The consequence is an increasingly one-dimensional discussion of processing problems. Because the practices of private institutions remain largely unknown, government appears to be the only source of practices necessitating regulatory intervention.[159]

There are also striking differences in the rights granted to the control authorities. Both the Norwegian[160] and the Austrian[161] data protection laws, for example, provide the data protection agencies with executive powers. Conflicts with the demands of the processing regulations are thus solved directly. Conversely, the West German law relies on the impact of public discussion. The commissioners must, of course, receive all the necessary information[162] and almost certainly will demand the immediate correction of collection or retrieval practices violating the data protection acts.[163] If their action is ignored, however, they can do no more than immediately inform parliament and the general public.

In this situation, the threat of public controversy replaces coercive intervention. At first this result seems to be a rather surprising choice; but, where, as in the case of the Hessian Commissioner, the control authority is fully integrated into the parliamentary organization, the denial of executive powers is the price for the close connection between Parliament and the supervision of the processing activities.[164] Neither Parliament nor any of its subordinate parts can directly interfere with the Executive and impose administrative measures.

There are other, far more general, reasons for the deliberate restraint of the commissioners' powers. The reverse of executive rights is judicial control.[165] Where, as with data protection, the success of the regulation depends on an open system of rules, constantly adapted to the increasing knowledge of processing practices and changing information techniques, recourse to judicial intervention in the conflicts may quickly reduce the flexibility of the law and thereby inhibit the guiding

---

[159] For a detailed discussion, see 10 TB HDSB 7, 18 (1981).

[160] *See* Norwegian personal data registers law, *supra* note 156, §§ 3, 8.

[161] *See* Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz), Oct. 18, 1978, §§ 36, 37, Bundesgesetzblatt für die Republik Österreich 565 (1978), as last amended *id.* at 370 (1986) [hereinafter Austrian data protection law]; *see* M. MATZKA, DATENSCHUTZRECHT FÜR DIE PRAXIS §§ 36, 37 (1986).

[162] *See, e.g.,* BDSG, § 19(3); 3d Hessian Data Protection Act, § 29; KOMMENTAR ZUM BDSG, *supra* note 99, at 589.

[163] *See, e.g.,* 7 TB BFD 17, 32, 41, 71, 74 (1985); 13 TB HDSB 21, 27, 45 (1984).

[164] *See* Simitis, *supra* note 120, at 131.

[165] This is an implication explicitly mentioned by art. 56 of the Swiss draft data protection act, *supra* note 100; *see also* art. 36 para. 4 of the Austrian data protection law, *supra* note 161 (foreseeing an appeal to the Austrian Verwaltungsgerichtshof (administrative court)).

effect of the legal requirements.

As efficient a corrective instrument as public controversy may be in certain situations, an appeal to the general public loses its potency if used too often. Consequently, the lack of executive powers, especially for the control of the private sector, has been increasingly criticized.[166] The more the monitoring of processing practices loses its exceptional character, the less convincing it becomes not to allow direct protection by the control authority. Procedures reflecting hesitations inherent in a new regulation dealing with still unknown implications of collection and processing must give way to better formulations once the conflicts grow familiar and experience is gained in dealing with them. Both the credibility and efficiency of control depend largely on the ability to secure a strict as well as a quick adaptation of processing practices to the expectations of the law.

CONCLUSION

The processing of personal data is not unique to a particular society. On the contrary, the attractiveness of information technology transcends political boundaries, particularly because of the opportunity to guide the individual's behavior. For a democratic society, however, the risks are high: labeling of individuals, manipulative tendencies, magnification of errors, and strengthening of social control threaten the very fabric of democracy. Yet, despite the incontestable importance of its technical aspects, informatization, like industrialization, is primarily a political and social challenge. When the relationship between information processing and democracy is understood, it becomes clear that the protection of privacy is the price necessary to secure the individual's ability to communicate and participate. Regulations that create precisely specified conditions for personal data processing are the decisive test for discerning whether society is aware of this price and willing to pay it. If the signs of experience are correct, this payment can be delayed no further. There is, in fact, no alternative to the advice of Horace: Seize the day, put not trust in the morrow.[167]

---

[166] *See* 10 TB HDSB 29 (1981); KOMMENTAR ZUM BDSG, *supra* note 99, at 920.

[167] "Carpe diem quam minimum credula postero." HORACE, ODES, 1.11.