PAUL SCHWARTZ

The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination

In 1890 Warren and Brandeis announced a "right to privacy" in an article in the *Harvard Law Review*.[1] Since this article drew its famous phrase, "the right to be let alone," from a tort treatise published a few years earlier,[2] the festivities celebrating the centennial of the right to privacy need not wait until 1990. Before the festivities can begin, however, we must decide if they are merited. The privacy article of Warren and Brandeis protests against the yellow press and attempts to provide a legal basis for protecting the individual from abusive journalistic practices.[3] Another privacy issue of that era was the attempt by the government to compel production of private books and papers. This activity led to the first great Fourth Amendment case of the Supreme Court, *Boyd v. United States*.[4] Over the next decades, a new tort, a privacy tort, was created in most states and some constitutional protection was given to letters, personal papers and other personal effects.

In their article, Warren and Brandeis declared that "[t]he intensity and complexity of life, attendant upon advanced civilization"

PAUL SCHWARTZ is Assistant Professor of Law, University of Arkansas, Fayetteville.
I wish to thank Spiros Simitis, Ludwig Salgo, Jutta Körbel, Joseph Goldstein, Owen Fiss, and Robert Burt for their suggestions and assistance. The Alexander von Humboldt Foundation provided a generous grant that made this work possible. Finally, I wish to acknowledge the superb secretarial help of Terri Snavely and the outstanding bibliographical assistance of Anne-Elise Arendt of the Goethe-Universität, Frankfurt-am-Main, West Germany. Unless otherwise noted, I am responsible for all translations.

1. Warren & Brandeis, "The Right of Privacy," 4 *Harv. L. Rev.* 193 (1890).

2. Thomas Cooley, *Torts* 29 (2d ed. 1888). See Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting) (the makers of our Constitution "conferred as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized man.").

3. See Warren & Brandeis, supra n. 1 at 196 ("The press is overstepping in every direction the obvious bounds of propriety and decency."). A generation earlier, Charles Dickens made even less favorable observations about the American press, see *The Life and Adventures of Martin Chuzzlewit*, Chapter 16 (orig. ed. 1843-44) (newspapers for sale in New York called *The Sewer, The Stabber, The Family Spy, The Private Listener, The Peeper, The Plunderer, The Keyhole Reporter*); *American Notes*, Chapter 6 (orig. ed. 1842) (newspapers in New York described as "pulling off the roofs of private houses").

4. 116 U.S. 616 (1886).

and "modern enterprise and invention" subject the individual to "mental pain and distress, far greater than could be inflicted by mere bodily injury."[5] Due to the continuing development of societal organization and of modern enterprise and invention, there are now more dangerous threats to the individual than at the time that Warren and Brandeis wrote. Today the enormous amounts of personal data available in computers threaten the individual in a way that renders obsolete much of the previous legal protection. The danger that the computer poses is to human autonomy. The more that is known about a person, the easier it is to control him. Insuring the liberty that nourishes democracy requires a structuring of societal use of information and even permitting some concealment of information.

This article examines the constitutional responses of two legal systems to the fashion in which the computer processes personal information and to the use that society makes of this capability. This examination of American and West German constitutional law will be carried out as an exercise in "functional comparative law."[6] As Max Rheinstein defined this term, it is a "problem related" attempt to analyze the "adequacy of legal regulation."[7] A comparison of certain legal norms of the United States and West Germany will be made in order to gain insights and ideas about constitutional principles for protecting human autonomy from the destructive effects of unbridled processing of personal information. This comparison will demonstrate the inadequacy of the current American constitutional standard. Although the U.S. Supreme Court has found two constitutional interests to be affected by governmental collection and processing of personal data, these interests do not provide sufficient legal protection for the individual.[8] In contrast, the Federal Constitutional Court of West Germany has met the challenge of new technology by adapting the idea of personality rights to create a "right of informational self-determination."[9] This German constitutional standard is part of a significant legal commitment in the Federal Republic to structuring the use of personal data.

German law shows that the regulation of personal information in computers cannot depend on the legal idea of privacy. Attempts to define a basis for a privacy right based on the borders of the "private" domain or the "secrecy" of personal information will not succeed. Rather, attention must be paid to the likely effect of information processing on human autonomy. The law must examine

5. Warren & Brandeis, supra n. 1 at 196.
6. Max Rheinstein, *Einführung in die Rechtsvergleichung* 27-28 (1974).
7. Id. at 28.
8. See infra Part I.
9. See infra Part II.

the dangers of specific data processing constellations in which individual information is employed. An American constitutional right of informational self-determination should be articulated that obliges government to organize its data processing systems in a fashion consistent with individual liberty. This interest should be protected by federal courts.

I. INFORMATIONAL SELF-DETERMINATION IN AMERICAN CONSTITUTIONAL LAW

Similar developments in data use have taken place in the United States and the Federal Republic of Germany.[10] Up to the start of this century, the amount of personal data recorded about any one person was small.[11] In the information society[12] in which we now live, ever more precise knowledge about individuals is required. This need for personal information results from the complex process of managing industrial production and consumer demand and from the complex services that must be provided in an accurate and effective fashion. The State itself must gather information because it has assumed responsibility for the well-being of citizens in an enlarged "social sphere," that is the field of political choice and social experimentation.[13] There are now records of our medical treatments, educational achievements, credit histories, tax bills, and the government benefits or services that we receive.[14] Not

10. See, e.g., Reese, Lange, Derricks et al., "Die Entwicklung der Informationsgesellschaft aus der Sicht der Bundesrepublik Deutschland" at 81 in *Informationsgesellschaft oder Uberwachungsstaat* (Symposium der Hessischen Landesregierung, 1984) (after the United States, the Federal Republic of Germany has more computers per employed person than any other country).

11. See *Personal Privacy in an Information Society: the Report of the Privacy Protection Study Commission* (1977) (hereinafter cited as *Privacy Report*) at 2 ("The records of a hundred years ago tell little about the average American, except when he died, perhaps when and where he was born, and if he owned land, how he got his title to it.").

12. See, e.g., Reese, et al., supra n. 10 at 17, 19 ("Information society means above all nothing other than that the majority of employed person earn their income in the information sector rather than the industrial sector."); *Privacy Report*, supra n. 11 at 3-6 (discussion of changes in use of information in American society). In 1987, an estimated $3,262 billion will be spent in America on data banks of information. "Beliebte Datenbank," *Frankfurter Allgemeine Zeitung*, 21 (8 September 1987). The United States government has an average of fifteen files on every citizen, Peck, "Extending the Constitutional Right to Privacy in the New Technological Age," 12 *Hofstra L. Rev.* 893, 894 (1984), and is the world's largest single user of computers, House of Rep., Rept. 100-153, Pt. 1, 6 (1987).

13. Cf. Jürgen Habermas, *Strukturwandel der Öffentlichkeit* (1962) ("Out of the middle of the publicly relevant private sphere of bourgeois society, a repoliticized social sphere formed in which state and societal institutions combined into a single continuity of function."); Bruce Ackerman, *Reconstructing American Law* 31 (1984) ("The activist legal task is to design a better form of accommodation between competing activities than the one thrown up by the invisible hand" of the market).

14. See Miller, "Personal Privacy in the Computer Age: The Challenge of New

only is this information extremely detailed, it can be stored indefinitely and combined endlessly with other information. The computer makes data multi-functional; once data are in digital, electronic form, they are available for a variety of processing purposes.[15]

Participation in modern life generates records that are critical in determining how we are treated and how power is allocated in our country.[16] The processing of this information is not a technological fate to be accepted, but a decision that is fraught with political consequences and subject to constitutional imperatives. Yet the nature of these constitutional commands is different in America and West Germany.

The German constitutional document, the *Grundgesetz*, sets both limitations on the State and positive goals for it to accomplish.[17] These goals oblige State activity in the areas of "public" and "private" law. In comparison, the American Constitution's protection of individual rights comes through definition of the limits of

---

Technology in an Information-Oriented Society," 67 *Mich. L. Rev.* 1089, 1103 (1969) ("Ever since the federal government's entry into the taxation and social welfare spheres, increasing quantities of information have been elicited from citizens and recorded. Moreover, in recent years access to government largess—at all levels—has depended increasingly upon a willingness to divulge private information."); Erickson & Gilbertson, "Case Records in the Mental Hospital," in *On Record: Files and Dossiers in American Life* 389 (S. Wheeler ed., 1969) ("If a stranger were to notice how many of the hospital's resources were devoted to the task of recording information about patients, he might well conclude that the main objective of the institution was to generate information and keep systematic files rather than treat illness.").

15. Simitis, "Les garanties générales quant à la qualité des données à caractère personnel faisant l'objet d'un traitement automatisé," in *Informatique et Droit en Europe* 305, 306 (Université libre de Bruxelles, ed. 1986). See Arthur Miller, *The Assault on Privacy: Computers, Data Banks and Dossiers* 202 (1971) ("Computers facilitate the composition of lists of people connected with various types of activities and institutions from widely scattered data that probably could not be brought together manually, enabling previously unknown relationships to be revealed or inferred from seemingly disparate information."). Cf. Kenneth Laudon, *Dossier Society* 15 (1986) (half of the uses of the FBI's Computerized Criminal History Records are for employment screening).

16. To offer one example: the use of computerized criminal history records affects both the chances for employment of ex-convicts and the balance of power between defense attorney and prosecution, Laudon, supra n. 15 at 4. For a further example, see Stauffer, "Tenant Blacklisting: Tenant Screening Services and the Right to Privacy," 24 *Harv. J. Legis.* 238 (1987) (description of computerized national tenant screening services).

17. See Art. 20(1): "The Federal Republic of Germany is a democratic and social federal state," *Basic Law in Federal Republic in Germany* (Gisbert Flanz. ed. 1985) (hereinafter cited as *Basic Law*) in *Constitutions of the Countries of the World* (Albert Blaustein & Gisbert Flanz, eds.); Art. 28(1): "The constitutional order in the Länder must conform to the principles of the republican, democratic and social legal state based on the rule of law (*Rechtstaat*) within the meaning of this Basic Law." Id. See also Dieter Grimm, *Recht und Staat der bürgerlichen Gesellschaft* 160 (1987) (social state principle obliges the state to care for life of citizens and strive for social justice).

State power.[18] Constitutional rights in the United States are, to use a term from German law, *Abwehrrechte*, or "rights of defense" against State activity.[19] As a result, no constitutional rights are implicated when private companies process personal data. These companies are unlikely to meet the threshold requirement of "state action" that is required to trigger constitutional protection.[20] Legal control of the data processing of private organizations can only be accomplished through federal and state statutes. The American Constitution creates no rights for the individual when personal information is processed by private companies.

The American Constitution is, however, of more help when it comes to personal information in the control of the government. In *Whalen v. Roe*,[21] the Supreme Court began to formulate a constitutional right for the computer age. This case concerned the creation of a centralized state computer file containing the names and addresses of all persons who obtained certain drugs pursuant to a doctor's prescription.[22] While upholding the state's exercise of its power, the Supreme Court did find two interests to be affected by this governmental gathering of information. One was an "individual interest in avoiding disclosure of personal matters," the other, "the interest in independence in making certain kinds of important decisions."[23]

A. *The Need for a New Start*

The *Whalen* Court did not discuss the interests that it found to be at stake, the interests in avoiding disclosure and in independence of decisionmaking, in terms of privacy. In fact, the *Whalen* Court appeared to distance itself from this concept by stating that the two

18. See Blum v. Yaretsky, 457 U.S. 991, 1004 (1982) ("a state normally can be held responsible for a private decision only when it has exercised coercive power or has provided . . . significant encouragement"); Evans v. Newtown, 382 U.S. 296, 299 (1966) ("Conduct that is formally 'private' may become so entwined with governmental policies or so impregnated with a governmental character as to become subject to the constitutional limitations placed on state action.").

19. See 39 Bundesverfassungsgericht [hereinafter cited as BVerfGE] 1, 41 (Abortion) (1975) ("the norms of the basic rights contain not only subjective rights of defense (*Abwehrrechte*) for the individual against the state, but embody, at the same time, an objective order of worth, which is valid for all domains of law and gives guiding rules and impulses for lawmaking, administration and judicial decisions.").

20. See Jackson v. Metropolitan Edison Co., 419 U.S. 345, 352 (1975) ("The fact that defendant's credit reporting operations are regulated by federal and state law is not sufficient to create state action.").

21. 429 U.S. 589 (1977) (unanimous opinion).

22. The contested New York law classified potentially harmful drugs in various schedules. Drugs with no recognized medical use were grouped under Schedule I and could not be prescribed. Id. at 592. Schedule II drugs were prescribable only with a special triplicate form, one copy of which was logged on to magnetic tapes for processing by a computer. Id. at 592-93.

23. Id. at 598-600.

interests at stake in this case were also found in "[t]he cases *sometimes characterized* as protecting 'privacy.' "[24] According to the Court, the proper characterization for the rights protected in these cases and in *Whalen v. Roe* was not privacy, but the rights and liberties protected by the Fourteenth Amendment.[25] By locating a textual basis for the two *Whalen* interests in the Fourteenth Amendment, the Court was able, at least in principle, to start developing a right that would be independent of two kinds of privacy law: sexual privacy and Fourth Amendment privacy.

There were, in fact, good reasons for the Court to distance itself from these two privacy rights. The immediate difficulty with the use of "sexual privacy" in *Whalen v. Roe* was that this case did not involve legal restrictions on access to abortions or contraceptives.[26] Yet Fourth Amendment privacy was even more problematic due to the Supreme Court's methodology for deciding when searches or seizures are subject to the protection of the Fourth Amendment. When deciding whether governmental conduct impinges upon a Fourth Amendment privacy interest, the Supreme Court evaluates the expectations of the individual and of society. A search is subject to the safeguards of the Fourth Amendment only if the object of the search has an actual, subjective expectation of privacy and society is prepared to recognize this expectation as reasonable.[27] There are a number of shortcomings with this approach,[28] but the most important in this context are those that follow from two of the Supreme Court's glosses on its testing of expectations.

According to the first of these glosses, a reasonable expectation

24. Id. at 598-599 (emphasis added).

25. Id. at 598.

26. See, e.g., Roe v. Wade, 410 U.S. 113, 153 (1973) (right of privacy has "some extension" to activities relating to marriage, procreation, contraception, abortion).

27. Oliver v. United States, 466 U.S. 170, 177-181 (1984); Smith v. State of Maryland, 442 U.S. 735, 740-41 (1979); United States v. White, 401 U.S. 745 (1975). The test of expectations was first suggested in Justice Harlan's concurrence to Katz v. United States, 389 U.S. 347, 361-62 (1967).

28. For criticism of the Supreme Court's approach, see Comment, "A Taxonomy of Privacy," 64 *Calif. L. Rev.* 1447, 1462 (1976) ("People learn to expect privacy in certain situations because courts give notice that in such situations the privacy interest is protected. For the courts then to say that privacy will be protected only where people expect such protection is a circular avoidance of responsibility."); Amsterdam, "Perspectives on the Fourth Amendment," 58 *Minn. L. Rev.* 349, 384 (1974) (expectation test "can neither add to, nor can its absence detract from, an individual's claim to fourth amendment protection. If it could, the government could diminish each person's subjective expectation of privacy" merely by announcing on television that nation was placed under electronic surveillance.); United States v. Taborda, 635 F.2d 131, 137 (2d Cir. 1980) ("The use of a subjective test as to expectations of privacy has been criticized by some courts and commentators on Orwellian grounds, that is, that it would be possible for the government by edict or by known systematic practice to condition the expectations of the populace in such a way that no one would have any real hope of privacy").

of privacy usually attaches to activities that take place within the "private sphere" or objects that are within our personal control.[29] Neither activities that take place in "public" nor objects that are in the control of a third party are considered "private" for purposes of the Fourth Amendment. If the naked eye of the State can see the activity or find evidence of it in the hands of another party, the Fourth Amendment offers no shield for the individual.[30] Governmental data use involves activities that take place outside of a private sphere and information that is outside of the control of the individual. Thus, the Fourth Amendment's protection of only a restricted "private domain" means that it has little value when the government has personal information in its computers.

The second relevant gloss to the Fourth Amendment is that reasonable expectations of privacy attach only to activities that the individual treats as secret.[31] Knowledge of the activity or of the information must be extremely limited if there is to be any protection by the Fourth Amendment. Personal information obtained by the government cannot be expected to remain secret in this sense; indeed, it will sometimes not even be treated as especially confidential. We know that these data will be used to make decisions about us and that these decisions can only be reached if someone examines the information. Within the crabbed confines of these two glosses of the Fourth Amendment, the *Whalen* Court could not protect informational privacy.

Faced with a Fourth Amendment made unsuitable for the informational age, the *Whalen* Court turned to the right of "sexual privacy" and engaged in some redefinition. The Court linked some of its sexual privacy cases to the Fourteenth Amendment and declared that the interests present in *Whalen v. Roe* were also such rights and liberties.[32] This reliance on the Fourteenth Amendment raises the specter of application of a substantive due process standard.[33]

---

29. This personal control can be in the sense of either possession or ownership, Couch v. United States, 409 U.S. 322 (1973).

30. For a recent extension of the "naked eye" limitation to Fourth Amendment privacy, see Florida v. Riley, 488 U.S. — (1989), 109 S. Ct. 693, 696 (1989) (plurality opinion) ("Riley could not reasonably have expected the contents of his greenhouse to be immune from examination by an officer seated in a fixed-wing aircraft flying in navigable airspace" or in a helicopter flying at 400 feet).

31. Smith v. State of Maryland, 442 U.S. 735, 743-46 (1979); United States v. Miller, 425 U.S. 435, 440-43 (1976).

32. *Whalen*, 429 U.S. at 594.

33. See Whalen v. Roe (Brennan, J., concurring) (emphasis added) (broad dissemination of personal matters is "presumably . . . justified only by *compelling* state interests"). This language referring to a need for a compelling state interest would bring the opinion into the realm of substantive due process, see, e.g., Moore v. East Cleveland, 431 U.S. 494, 499-507 (1977) (plurality opinion) (application of substantive due process analysis).

This difficulty is not insoluble.[34] But wherever the Court finds a textual basis for the new rights, it should make an explicit commitment to its prior decisions that set limits on governmental use of personal information.

B. The Path Not Taken

There have been times in both Fourth Amendment cases and sexual privacy cases when the Court saw its goal as preventing coercion of the individual through the State's gathering of information.[35] In these cases, the Court sets limits on State activity because of its "respect for the inviolability of the human personality."[36] This respect is the consequence of the protection of the individual from governmental domination contained in the Bill of Rights.[37] Perhaps the first clear expression of this value in the Supreme Court's jurisprudence appears in *Boyd v. United States*. The *Boyd* Court said: "It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offence; but it is the invasion of his indefeasible right of personal security, personal liberty and

34. The standard of substantive due process rights will most likely discourage courts from protecting individual interests of informational self-determination. The identification of a new substantive due process right of informational privacy would appear to withdraw sensitive information and important decisions from the expanded sphere in which the State seeks the well-being of society. Cf. Gunther, "The Supreme Court, 1971 Term," 86 *Harv. L. Rev.* 1, 8 (1972) (review of interests that compete with substantive due process right is "fatal in fact" for competing interest.). The solution lies in the process of developing a scale of values with which to evaluate informational self-determination and government's information interests. See infra Part II, B-C.

35. See, e.g., United States v. United States District Court, 407 U.S. 297 (1972) (Fourth Amendment's requirement of judicial judgment limits power of President to authorize electronic surveillance in internal security matters); Stanley v. Georgia, 394 U.S. 557, 565 (1969) ("right to be free from state inquiry into contents of [personal] library"); Griswold v. Connecticut, 381 U.S. 479 (1965) (a law that forbids the use of contraceptives "seeks to achieve its goals by means having a maximum destructive impact" upon marital relationship—for example, police searches of "sacred precients of marital bedrooms for telltale signs of the use of contraceptives"); Marcus v. Search Warrant, 367 U.S. 717, 733 (1961) (mass seizure of books under "general" warrant authorizing "search and seizure of obscene publications" violates Due Process Clause of Fourteenth Amendment). There is, unfortunately, little doubt that at present the Supreme Court does not care much about the protection of individual autonomy, see, e.g., Florida v. Riley, 488 U.S. — (1989), 109 S. Ct. 693, 704 (1989) (Brennan, J., dissenting) ("I find considerable cause for concern that a plurality of four Justices would remove virtually all constitutional barriers to police surveillance from the vantage point of helicopters. . . . I hope it will be a method of concern to my colleagues that the police surveillance methods they would sanction were among those described forty years ago in George Orwell's dread vision of life in the 1980's. . . .").

36. Murphy v. Waterfront Commissioner, 378 U.S. 52, 55 (1964).

37. Cf. Ely, "The Wages of Crying Wolf," 82 *Yale L.J.* 920, 929 (1973) (Bill of Rights limits the ways in which the government can go about gathering information about citizens).

personal property."[38] The Court has since found the rights of personal security and liberty to be of special constitutional significance[39] because they encourage the self-determination of the American people.[40]

Limits on governmental use of information that can coerce citizens, which are found in the First, Fourth, and Fifth Amendments, reach a high point in the Due Process Clause of the Fourteenth Amendment. The *Whalen* Court did not go astray in using this provision. The government's utilization of computers provides an excellent means for increasing the efficiency of the State; the Fourteenth Amendment indicates the importance of other values. As the Supreme Court noted in *Stanley v. Illinois*: "[O]ne might fairly say of the Bill of Rights in general, and the Due Process Clause in particular, that they were designed to protect the fragile values of a vulnerable citizenry from the overbearing concern for efficiency and efficacy that may characterize praiseworthy government officials no less, and, perhaps more, than mediocre ones."[41]

The *Whalen* Court should have developed the American constitutional tradition of protecting self-determination into a right that responded to the dangers of the State's processing of personal information. Individual autonomy depends on a mixture of concealment and exposure of the self. The mixture is made because a differentiation between ourself and others depends on limits to the knowledge that people have of us.[42] If everyone knew everything about us, we would be unable to act freely—an independent existence and a dem-

38. 116 U.S. 616, 630 (1885).

39. See Wayden v. Hayden, 387 U.S. 294, 304 (1967) ("premise that property interests control the right of the government to search and seize" is discredited); ICC v. Brimson, 154 U.S. 447, 479 (1894) ("Of all the rights of the citizen, few are of greater importance or more essential to his peace and happiness than the right of personal security.").

40. See cases cited in supra nn. 35, 36, 39. Cf. Tomkovicz, "Beyond Secrecy for Secrecy's Sake," 36 *Hastings L.J.* 645, 674-75 (1985) ("The confidentiality assured by our homes is valuable not just because it closes actual doors to the government, but because it opens figurative doors for those who dwell within.").

41. 405 U.S. 645, 656 (1971). See supra n. 35.

42. The first such differentiation is between our self and that of our parents, Freud, "Der Familienroman der Neurotiker" (orig. ed. 1909), in *Studienausgabe*, Bd. IV (1970). See Erik Erikson, *Childhood and Society* 254 (2d ed. 1963) ("the sense of autonomy fostered in the child and modified as life progresses, serves (and is served by) the preservation in economic and political life of a sense of justice."). For a description of why and how humans control discrediting and discreditable personal information, see Erving Goffman, *Stigma* (1963). See also Fried, "Privacy," 74 *Yale L.J.* 475 (1968) (noting human need for some control over information as necessary for "the relationships of love, friendship and trust"); Gavison, "Privacy and the Limits of Law," 89 *Yale L.J.* 421, 454 (1980) ("We always give partial descriptions of ourselves and no one expects anything else. The question is not whether we should edit, but how and by whom the editing should be done."); Tomkovicz, supra n. 40 at 693, fn. 194 (noting "inhibitory pressure generated by the prospect of unregulated government awareness").

ocratically ordered State would be impossible.[43] The *Whalen* Court should have applied a constitutional right of informational self-determination in judging the State's planned use of personal data. Citizens must be aware of where personal information relating to them is processed and how it is being used. Furthermore, there must be a prohibition of that processing of personal information that would make impossible the individual choices on which a democratic consensus depends.

In *Whalen v. Roe*, the Court should have applied the right of informational self-determination by first asking if the State had decided what it planned to do with the data. Although New York had recorded 100,000 prescriptions each month during the twenty months that the law had been in effect, it had used this information in investigations of exactly two persons.[44] To be sure, the Supreme Court's job is not to stop state legislatures from wasting money on foolish projects that are decided upon after orderly deliberation. But the protection of human autonomy does require judicial inquiry into the influence on the individual of having his personal information used in a specific system or indefinitely stored for future application. The Court should have searched for statutory barriers that would prevent New York from using this information for other purposes. The Court should have examined the kind of data processing involved and its likely impact on the individual.

C. *The Path Taken: Privacy Redux*

Instead of creating such an American right of informational autonomy, the *Whalen* Court identified two interests that rely on regrettable aspects of privacy law. The Court distanced itself from privacy only on a superficial level: the two interests that it established have undeniable ties to notions of privacy as secrecy and to the law of sexual privacy.

The first interest that it identified was "avoiding disclosure of

43. John Stuart Mill made this connection between human autonomy and civil liberty explicit in his discussion of the importance of the ability to carry on "civil" and "public business" with "intelligence and order and decision:" "This is what every free people ought to be: and a people capable of this is certain to be free; it will never let itself be enslaved by any man or body of men because these are able to seize and pull the reins of the central administration." J. Mill, *On Liberty*, Chapter V (1859). Mill specifically praises the autonomous behavior of the American people: "What the French are in military affairs, the Americans are in every kind of civil business; let them be left without a government, every body of Americans is able to improvise one, and to carry on that or any other public business with a sufficient amount of intelligence, order and decision." Id. *Sic transit gloria mundi.* For further discussion of the need for self-determination in a democratic order, see Simitis, "Selbstbestimmung: Illusorisches Projekt oder reale Chance?," 21 *Krit. Justiz* 32 (1988).

44. *Whalen*, 429 U.S. at 595.

personal matters." The *Whalen* Court recognized an interest that prohibits the public disclosure of personal information that is in the government's control. This interest modifies the Fourth Amendment's notion of privacy-as-secrecy by recognizing a privacy interest in personal data outside of the control of the individual to whom the information relates. Yet the emphasis on secrecy remains: here, the protection is granted to insure that the government keeps knowledge of the personal information hidden from the public. So long as the information is so concealed, there is no violation of the first *Whalen* interest.

Within the boundaries of this right, the Supreme Court did all that it could: the Court examined the data security provisions of New York,[45] and it found that there had been no public disclosure of the personal information.[46] But there are issues other than whether the public would find out details of the drug use of some citizens. Of equal importance are the plans that the State of New York had for this information and the impact on the individual of this use. In the computer age, constitutional protection must be given to more than a narrow interest in avoiding public disclosure; it must be given to an interest in being free from state coercion through data use.

Just as there was no disclosure, the *Whalen* Court found no violation of the second interest, that of independence in making "certain decisions."[47] This interest is derived from the protection of certain choices by the right of sexual privacy. One might describe that privacy right as protecting the freedom to engage in sexual activities without governmental determination of the procreative consequences. A different sort of decisionmaking was at stake in *Whalen*; according to the Court, it is coextensive with acquiring and using needed medication. This interest was not considered to be threatened because "the decision to prescribe, or to use, is left entirely to the physician and the patient."[48] The Court did admit that the "record supports the conclusion" that some use of the drugs in question had been discouraged by the record-keeping requirement.[49]

45. Id. at 593.

46. The Court noted that associated with "many facets of health care" were "disclosures of private medical information to doctors, to hospital personnel, to insurance companies, and to public health agencies." Id. But see United States Department of Justice v. Reporters Committee, 489 U.S. — (1989), 109 S. Ct. 1468, 1476-79 (1989) (applying *Whalen* interest against disclosure and noting privacy interest under Freedom of Information Act in single computerized summary even if data is available in various public records). Compare Zimmerman, "Requiem for A Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort," 68 *Cornell L. Rev.* 291, 363 (1983) ("current, capricious course" of privacy tort law is to impose "liability only if the material is ultimately disseminated to the public at large").

47. *Whalen*, 429 U.S. at 602-603.

48. Id at 603.

49. Id.

But in light of the 100,000 prescriptions that were filled for these drugs every month, the Court found that the statute did not deprive the public of access to these substances.[50]

Like the interest in "avoiding disclosure," the second right at stake in *Whalen*, independence in making "certain decisions," is of less help than protection of decisionmaking would be. The second *Whalen* right also fails to protect the individual from the pressure of state data use. More important than the abstract availability of certain choices is whether a decision will be free or whether it will be lost because of the coercion of the government's data gathering. A given activity that is still permitted may be refused by people who know that the government is collecting and processing information about them. The choice of some patients not to use the drugs in question rather than have their data stored in the computers of the New York Health Department shows such concern. The Supreme Court needs to protect not a right to make certain decisions or a right against public disclosure but a right of informational self-determination. Such a right, anchored in the Due Process Clause of the Fourteenth Amendment, would protect human autonomy through judicial attention to the effect of governmental data use.

II. THE GERMAN CONSTITUTION'S RESPONSE TO THE COMPUTER

The American Supreme Court's deficient idea of constitutional data protection law can be contrasted with the more successful principles articulated by the German Constitutional Court. The first outstanding expression of this jurisprudence came in the Court's *Census* decision of 1983, which established constitutional standards for the processing of personal information. An examination of the *Census* opinion will show both improvement on the work of the *Whalen* Court and the most difficult task for judges in evaluating the impact of governmental data processing systems.

As has been noted, American constitutional rights set limits on certain aspects of the State's power, but the German Constitution explicitly commands State activism. The *Grundgesetz* obliges the State to recognize and enforce fundamental norms that will affect the relations among private actors. As part of this constitutionally commanded activism, the first two articles of the German Constitution compel the State to take positive action to protect human dignity (Article 1) and the development of human personality (Article 2).[51] These provisions form the basis of a "right of personality."[52]

50. Id.

51. Art. 1(1): "The dignity of man shall be inviolable. To respect and protect it shall be the duty of all state authority." Basic Law, supra n. 17. Article 2(1): "Everyone shall have the right to free development of his personality in so far as he does

Protection of an interest in individual autonomy is carried out under a sub-division of this personality right that is called "the right of self-determination."[53] This right provided the foundation for a constitutionally mandated judicial role in safeguarding human autonomy from the pressure of modern information use. In its *Census* decision, the Constitutional Court created an additional component of this part of the right of personality, which it termed "the right of informational self-determination."[54]

A. The Census Decision: the Legal and Social Background

In March 1982, the *Bundestag*, the German Parliament, promulgated a law for a census of the population and its professions, dwellings and workplaces.[55] The first eight sections of this law regulated the contents of the census questionnaire and the way that the census was to be executed; the ninth section contained special provisions for the application and transmission of the collected data.[56] Among the questions set out in the first eight sections were inquiries about: religion; occupation; chief sources of income; the means of transportation used to go to work or to the place of education; and the nature of living quarters and place of work.[57] Paragraph 9 allowed information obtained through the census to be compared to the inhabitant register and to be used to correct it.[58]

---

not violate the rights of others or offend against the constitutional order or the moral code." Id. See Art. 1(3): "The following basic rights shall bind the legislature, the executive, and the judiciary as directly binding law," Basic law, supra n. 17. See also *Bundesgerichtshof Entscheidungen für Zivilsachen* [BGHZ], *Neue Juristische Wochenschrift* [hereinafter cited as *NJW*) 1593 (1959) (citing v. Mangoldt & Klein, *Grundgesetz* 147 (2ed)) (The inalienability of human worth protected by Art. 1 of the *Grundgesetz* "is no simple non-binding proposition, but rather a 'directly effective norm of the objective (constitutional) law in the form of a generally valid general clause' ").

52. 30 BGHZ 7, 11 (Valente) (1959); 26 BGHZ 349, 354-55 (Herrenreiter) (1958); 24 BGHZ 72, 77 (Krankenpapiere) (1957); 14 BGHZ 334 (1954).

53. See 54 BVerfGE 148, 155 (Eppler) (1980) (an idea of self-determination follows from and underlies the general right of personality); 34 BVerfGE 269, 281 (Soraya) (1973) ("the value system of the basic rights" protects the "private sphere" where one is to make "decisions in individual responsibility"); 27 BVerfGE 1, 6-7 (Mikrozensus) (1969) (a menace to the right of self-determination would be posed by a statistical inquiry into the inner domain of human life).

54. 65 BVerfGE 1, 41-52 (1983). The term was not new at the time of the *Census* decision. It had already been used in discussions during the preparation of the federal data protection law and in the articles of a number of professors. At least one mention of the term came as early as 1971, see Podlech, "Das Recht auf Privatheit," in *Grundrechte als Fundament der Demokratie* 55 (Perels, ed. 1979); Denninger, "Die Trennung von Verfassungsschutz und Polizei und das Grundrecht auf informationelle Selbstbestimmung," *Z. RPol.* 231 (1981).

55. Gesetz über eine Volks-, Berufs-, Wohnungs-, und Arbeitsstättenzählung, 1982 Bundesgesetzblatt [BGB1] I 369.

56. Id. at Paras. 1-9.

57. Id. at Paras. 1-8.

58. Id. at Para. 9. According to this paragraph, the knowledge gained through

Although passed by the Parliament with little debate, this law led to an unexpected storm of protest.[59] In a few weeks, hundreds of new citizen initiative groups called for a boycott of the census.[60] On the doors of apartments and houses appeared stickers proclaiming, "Beggars, peddlers and census numerators forbidden."[61] In a debate in Hamburg, Günter Grass called the census "a monster" and asked for it to be discontinued.[62] In his defense of the Census, the Federal Data Protection Commissioner, Hans Peter Bull, admitted that the questionnaire was written in an exceedingly authoritative style and frightfully unclear language.[63] State Data Protection Commissioners not only objected to the census, but expressed their criticisms in testimony before the Constitutional Court.[64]

These activities by federal and state officials indicate that at the time of the census law's promulgation, West Germany already had established some sophisticated institutional arrangements for observing and shaping data use. The *Census* decision did not occur in a legal vacuum, but at a time when West Germany had begun to establish measures that respond to the threat of the computer. These legal measures had started on the state level, where the first data protection law was passed in 1970.[65] State laws, which now exist in all eleven *Bundesländer*, set up provisions for the processing and transmission of data and establish the post of data protection commissioner. These state officials are to observe the application of data protection law, report to the state parliament, and assist citizens by providing the resources and technical expertise to help them understand the structure of information processing and the extent of their rights.[66] A federal data protection law was passed in 1977.[67] Much like the state laws, the federal law gives individuals a general right to be informed about the existence of data banks and to correct false

---

this comparison was not to be used in measures against the individual who was under a legal obligation to answer the questions (*Benachteilungsverbot*). Id. at Para. 9(1). The Constitutional Court made the pithy observation that this measure promised more than it could achieve. 65 BVerfGE 1, 65 (1983).

59. Muckenberger, "Datenschutz als Verfassungsgebot," 18 *Krit. Justiz* 1 (1984).

60. For a sampling of the public reaction, see "Volkszählung: Lasst 1000 Fragebogen glühen," *Spiegel* Nr. 13, 28 (1983).

61. Id.

62. Grass & Bull, "Ein Streitgespräch," 43-44, in *Die Volkszählung* (J. Tager, ed., 1983).

63. Id. at 45, 58.

64. 65 BVerfGE 1, 34-35 (1983).

65. Simitis, "Bundesdatenschutzgesetz—Ende der Diskussion oder Neubeginn?," 30 *NJW* 729 (1977).

66. See, e.g., Hessisches Datenschutzgesetz vom 11.11.1986 (1986 BGBl I 309) (hereinafter cited as "Hessian Data Protection Law").

67. Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz) v.27.1.1977, BGBl I, 201. For discussion of this law, see Simitis, supra n. 65.

information that refers to them. It also establishes a Federal Data Protection Commissioner. The next round of German legislative activity has occurred on both federal and state levels.[68] Laws have been promulgated to govern the processing of data according to the type of information and its planned use. These "domain-specific" laws exist for such activities as the granting of credit and the utilization of medical information by hospitals and insurance companies.[69]

The protest against the census took place in a legal culture that had already devoted considerable ingenuity to developing a law of data protection. Broad public disapproval of the planned poll and an already significant tradition of legal attention to the dangers of the processing of personal information provided a supportive context for the *Census* decision.[70] The projected inquiry had become a symbol for the dangers of data gathering and processing. The Constitutional Court responded by raising to the level of constitutional command an obligation to protect citizens and the democratic order from these dangers.[71]

B. Informational Self-Determination

The German right of informational self-determination protects the individual from borderless collection, storage, application and

68. Gola, "Zur Entwicklung des Datenschutzrechts im Jahre 1985," 1986 *NJW* 1913, 1916.

69. Id. at 1916-1919.

70. For an excellent discussion of the Court's opinion and a chronology of the events before and after it, see 12 *Tätigkeitsbericht des Hessischen Datenschutzbeauftragten*, 73-82 (1983).

71. The Constitutional Court did not, however, find that the population census as a whole violated the right of informational self-determination. 65 BVerfGE 1, 52-53 (1983). Yet the Court did declare a number of individual provisions of the census to be unconstitutional. The comparison of the census data with the inhabitant register, as provided for in Sect. 9, was found unacceptable. Id. at 63. The concrete purposes to which the authorities would apply the individualized data that they received were not foreseeable. Id. at 62, 63. For this same reason, the Court also struck down provisions that allowed data to be transmitted to federal, state and community officials. Id. at 65.

The Court went on to order specific protective measures to be instituted as part of the census. In order to avoid dangers that arise through the inspection of the formula by the numerator, the Court ordered that surveys could be returned through the mail at the cost of the government. Id. at 60. Attributes which served to identify a respondent were to be deleted as soon as possible and until then were to be maintained under lock and key. Id. Finally, census numerators were not to be employed in the immediate area in which they lived. Id. These requirements were taken into account when the next Census Law was drafted, see Mallman, "Das Volkszählungsgesetz 1987," *NJW* 1850 (1987). But see Rottmann, "Volkszählung 1987—wieder verfassungswidrig?" *Krit. Justiz* 72, 82-87 (1987) (anything but free of doubts about the constitutionality of the 1987 Census). In a series of decisions, the Constitutional Court upheld the 1987 Census as constitutional, BVerfGE, *NJW* 2805 (1987); BVerfG, *Computer und Recht* 147 (1988); BVerfG, *Computer und Recht* 872 (1988); BVerfG, *Computer und Recht* 877 (1988); BVerfG, *NJW* 707 (1989).

transmission of personal data.[72] It prevents any processing of personal data that leads to an inspection of or an influence upon a person that is capable of destroying an individual capacity for self-governance.[73] Yet the right of informational self-determination is not intended to be a right of control over personal data. It also creates no individual property interest in this information. The Constitutional Court stated: "The individual does not have a right in the sense of an absolute, unlimitable mastery over 'his' data; he is rather a personality that develops within a social community and is dependent upon communication."[74] Information relating to a person depicts "an image of social reality that the concerned party cannot exclusively coordinate."[75] Rather than giving exclusive control or a property interest to the data subject, the right of informational self-determination compels the State to organize data processing so that personal autonomy will be respected. Thus, the right both limits certain actions and obliges other activities on the part of the State.

In contrast to the U.S. Supreme Court's decision in *Whalen v. Roe*, the Constitutional Court did not rely on any legal notion of privacy in its *Census* opinion. It neither searched for data security measures to insure the "secrecy" of the information within the government nor checked to see if "certain decisions" would still be open. Instead, the Court accepted the social nature of information and called for measures to structure the handling of personal data. These measures must allow the person affected to anticipate who will use his personal data and the purpose to which this information will be put.[76] Without this knowledge, the "psychic pressure" of uncertainty about whether information about "deviating modes of behavior" is stored or transmitted can impede a citizen's freedom of action and cause the renouncement of rights guaranteed by the German constitution.[77] The Court declared: "Inconsistent with the right of informational self-determination would be a societal order and assisting legal order in which the citizen no longer knew the who, what, when and how of knowledge about him."[78] The Court called for a legislative setting of precise goals before any collection of individual data.[79] The informational activities of the State and

72. 65 BVerfGE 1, at 42.
73. Id.
74. Id. at 44.
75. Id.
76. Id. at 43-45.
77. Id. at 42-43.
78. Id.
79. Although the legislature had the job of drafting the laws that authorize the gathering of personal information, the Court made clear that the only data that may be collected is that which is "suitable as well as necessary" to attain the legislative goals. Id. at 46. Indeed, the Court stated that a stockpiling of personal data for indeterminate purposes would be unconstitutional. Id. at 46. The Court established

private industry alike require these organizational and procedural regulations for the processing of personal data. Like the general right of personality, the right of informational self-determination is applicable to organizations governed by private law.[80]

The Constitutional Court is committed to a law of data protection in which various actors play a part. The legislature is to pass laws that set provisions for every constellation of data use and transmission.[81] The individual citizen is placed at the center of the data collection process to insure his awareness of the fate of his information and to encourage his participation in the discussion and debate regarding the use of personal data. The independent monitoring and criticism of federal and state data protection commissioners are to assist the public in gaining knowledge of data processing practices.[82] Such institutional figures are needed, according to the Court, because of the unfathomable nature of data processing for the citizen and the need for timely legal measures that will protect the right to informational self-determination.[83] The final institution involved, the judiciary, will hear constitutional objections to data processing laws or data processing practices.

The *Census* decision establishes a power of judicial review of all legislation that authorizes or regulates data collection or processing.[84] Such laws must be checked for a valid legislative basis; clearness of norms; and observance of the "principle of proportionality."[85] Judges can also hear constitutional complaints about practices of data processing—whether the government or a private company is involved. By allowing judicial review of the constitution-

other rules for statistical data. It is in the nature of statistics that they be applied for various tasks after their preparation—there is a need here for stockpiling of data. Id. at 47. Although a concrete binding to a goal cannot be requested of a data inquiry for statistical purposes, limits were to be set within the information system. Id. at 48. During the initial stages of a statistical inquiry, collected data will still be in individual form. Therefore, the lawmaker must check whether the collection of certain details carries the danger of a "social labeling" of the individual and whether the goal of the inquiry cannot also be reached by an anonymous inquiry. Id. at 48-49. In addition, individual data raised for statistical purposes must be maintained in secrecy; must be made anonymous as soon as possible; and must be protected against deanonymization. Id. at 49-52.

80. The Court does not merely discuss a right against governmental action, but speaks of a "societal order" and a "legal order" in which the right of informational self-determination must be respected. Id. at 43. See Simitis, "Die informationelle Selbstbestimmung," 1984 *NJW* 398, 400-401 (when the individual's capacity to act depends on the possibility to have influence on the processing of personal data, protection cannot depend on who seeks the information); Ehmann, "Zur Zweckbindung privater Datennutzung," 1988 *Recht der Datenverarbeitung* 221 (attempt to define scope of constitutional limits on private data processing).

81. 65 BVerfGE at 46.

82. Id. at 46. See 67 BVerfGE 157, 185 (1985); 49 BVerfGE 89 (1962).

83. 65 BVerfGE at 46.

84. See, e.g., cases cited supra n. 71.

85. 65 BVerfGE at 44.

ality of the processing of personal information, the right of informational self-determination grants German courts a great deal of power. Wise use of this authority depends on further definition of the values involved in specific conflicts between informational self-determination and information processing.

C. *Informational Self-Determination as a Judicial Tool*

As we have seen, the *Census* Court was primarily concerned with establishing the requirements for a constitutional structure of data use. The government and private enterprises alike can only process personal data once certain procedures are in place. Yet even a processing of personal data that is made in a procedurally adequate fashion might still impinge upon the right of informational self-determination. Judges have a difficult task in deciding whether there has been such a substantive infringement of the right. The Constitutional Court proposed that these conflicts be solved with that classic tool of jurisprudence, a weighing of interests.[86] Unfortunately, the Court did not discuss the way that this balancing was to be carried out. This lack of discussion suggests that the right of informational self-determination will undergo the same development as a tool of judicial decisionmaking as the right of personality, of which it is, after all, a part.

When the Constitutional Court weighs competing interests in cases that concern personality rights, it evaluates the personality rights of the individual and the interests of the State or of the community. The weakness often present in these decisions is the mechanical nature of the weighing. The Court allows anything that it identifies as a significant public interest to triumph over any interest that it identifies as a private one. By doing so, the Constitutional Court relies on trickery with the categories of public and private interests. The *Lebach* decision[87] is an example of this sleight of hand.

In this opinion, the Constitutional Court decided whether a television drama depicting a notorious crime could be broadcast before one of the participants was to be released from jail.[88] The *Lebach* Court weighed the competing constitutional values of the plaintiff's right of personality and the freedom of reporting through broadcasting.[89] It identified the right of personality at stake as the convict's interest in controlling the representation in public of his life.[90] The Constitutional Court decided that this private interest was accompa-

86. Id.
87. 35 BVerfGE 202 (1973).
88. The details of the crime and punishment are given id. at 204-209.
89. Id. at 220-224.
90. Id. at 220.

nied by a public one: the interest of the community in the resocialization of the individual.[91] The Court also found that the broadcast was without any significant worth because the "informational interest" of the public regarding the crime was already adequately satisfied.[92] There was no need for more deliberation. The verdict of the Court was that the *private interest* (the personality right) and a *public interest* (resocialization of criminals) outweighed the *public interest* in the information (the public's need to know had been satisfied to an appropriate extent).[93] The Court prohibited the broadcast of the drama.

The *Lebach* Court's attention to the plaintiff's social existence is justified. While isolated in prison, the offender had both a lack of freedom and a formal legal status of reduced rights. Now the prison bars would be gone, but the television drama was capable of making him remain an outsider with a diminished social identity.[94] Yet the decisive factor in the Court's decision, its belief that the plaintiff's reintegration into society was not just a personal concern[95] but an important social interest, is actually less than determinative. All individual interests that are worthy of State protection benefit both the right bearer and the community.[96] By identifying the interest in rehabilitation as a public value and denigrating the significance of the contested broadcast, the Court fails to engage in the needed evaluation of why one interest is more important than another in

91. Id. at 238.

92. Id. at 240.

93. Id.

94. In its decision, the Constitutional Court noted that the broadcast in dispute would probably have an audience of 23 million viewers. Id. at 228. The Court stated that this television program would strengthen the already existing tendency of the public not to accept these "social outsiders" and would thereby seriously harm any chances that the plaintiff had of rejoining society. Id. at 230. Compare Posner, "Privacy, Secrecy and Reputation," 28 *Buffalo L. Rev.* 1, 12 (1978) ("If ex-convicts have on average poor employment records, if the cost of correcting this average judgment for the individual ex-convict applying for a job is high, and if substitute employees without criminal records are available at not much higher wages, it may be rational for an employer to adopt a flat rule of not employing anyone who has a criminal record.").

95. Among the personal concerns that the Court discussed was the plaintiff's interest in finding a wife. 35 BVerfGE at 242. The broadcast, which emphasized the homosexual relations among the band of murderers, would pose a special impediment to the resocialization of the plaintiff, whose interest in rejoining society included being able to marry. 35 BVerfGE at 242. The Court explained: "In the situation of the complainant, the union for life with a female can form a determinative factor for the success of his reintegration." Id. The broadcast could prevent the formation of such a union. Id.

96. See Alenikoff, "Constitutional Law in the Age of Balancing," 96 *Yale L.J.* 943, 973 (1987) (characterization of interests in balancing cases is often arbitrary as some interests can be conceived of in both public and private terms); Pound, "Interests of Personality," 28 *Harv. L. Rev.* 243, 253 (1915) (social interests can be identified in "free belief and free expression as guarantees of political efficiency and instruments of social progress" as well as in securing individual interests of personality).

terms of the values protected by the German Constitution. The Court makes it too easy for itself in its exploration of the constitutional values that are implicated by the reintegration of ex-convicts.

The *Lebach* decision may foreshadow the development of the right of informational self-determination. In cases involving this right, courts must judge the constitutionality of personal information processing that threaten individual autonomy. If they follow the *Lebach* model, German courts will first decide whether the processing of information or the interest in self-determination at stake is more important and then justify their decision by aligning the decisive interest of the public with the interest they only believe to be more significant.[97] Public interests can be found in either a data processing system or an individual's complaint against this system—a democratic order requires both a relatively free flow of information and limits to knowledge of the individual. An alternative to the mechanical balancing of *Lebach* is for German courts to develop the right of informational self-determination through study and elaboration of the fundamental values of the German constitution. There would be no magical process involved—just analysis of constitutional principles, explication of social values and study of precedent. German courts must start on the difficult task of developing a scale of values with which to evaluate the right of self-determination and the informational interests of society.

III. Recent Developments in American and German Law

A. *American Deficiencies*

American developments on the judicial level have been particularly discouraging since the *Whalen* decision. There is still no constitutional right adequate to protect the individual in the information age. Federal courts have not even stopped the undercutting of the Privacy Act's protection against sharing of personal data within the government.[98] This weakening of the Privacy Act

97. For a recent case that applies the right of informational self-determination with some trickery with categories, see BVerfG, 1987 *Computer und Recht* 12, 872, 875 (the risk of re-identification of personal data must be accepted by the individual as part of "a statistical survey ordered in the prepondent general interest"). For a sampling of decisions of lower courts that uphold limitations of the right of informational self-determination because of a weightier public interest, see Gola, "Das Recht auf informationelle Selbstbestimmung in der aktuellen Rechtsprechung", *Recht der Datenverarbeitung* 109, 110-112 (1988).

98. The Privacy Act states that information collected for one purpose should not be used for another purpose without the data subject's permission. Yet it also creates an exemption if the information will be put to a "routine use"—that is, one that is compatible with the purpose for which it is collected. Privacy Act, Sec. 5b.1(j), Public Law 93-579, 88 Stat. 1897 (1974), as amended by Pub. L. No. 94-183, 89 Stat. 1057 (1975) (codified as amended at 5 U.S.C. Sec. 552a (1982)). For cases that find routine uses in interagency sharing of data, see, e.g., United States v. Miller, 643 F.2d

has come through an overbroad reading of its exemption for "routine use" of information by federal agencies.[99] Some order has been imposed on federal data sharing by the Computer Matching and Protection Act of 1988, but this law is at best a housekeeping measure that still grants enormous discretionary power to governmental agencies.[100] The judicial role in enforcing this law will, most likely, be on the scale of procedural attention to its notification provisions.[101]

The nature of government processing of personal information is decided in America in a low profile, ad hoc fashion by a variety of government bodies. The agencies with the most important roles are the Office of Management and Budget, which is part of the Executive Office;[102] the General Accounting Office;[103] the Office of the Inspector General of the Department of Health and Human Services;[104] the National Bureau of Standards, which is a division of

713 (10th Cir. 1981); Windsor v. Federal Executive Agency, 614 F. Supp. 1255, aff'd without op., 767 F.2d 923 (6th Cir. 1985); Andrews v. Veterans Admin., 613 F. Sup. 1404 (Wyo. 1985); United States v. Collins, 596 F.2d 166, 169 (6th Cir. 1979); but see Howard v. Marsh, 785 F.2d 645 (8th Cir. 1988), cert. den., 479 U.S. 988 (1987); Tigerina v. Walters, 821 F.2d 789 (D.C. Cir. 1987). See also Office of Technology Assessment, Congress of the United States, *Electronic Record Systems and Individual Privacy* 57 (1986) (hereinafter cited as "Record Systems") ("The Privacy Act as presently interpreted by the Courts and OMB guidelines offers little protection to individuals who are the subjects of computer matching.").

99. See Record Systems, supra n. 98 at 105 ("routine use" exemption of Privacy Act "has become a catchall exemption").

100. The Computer Matching and Privacy Protection Act of 1988, Public Law 100-503 (codified at 5 U.S.C. 552a (1988)), prohibits matching agreements without written agreements between the source agency and recipient agency and establishes data integrity boards within each agency that participates in a matching program. Federal matching programs permit data from various agencies and private sources to be compared. See Record Systems, supra n. 98 at 50 ("no firm evidence is available to determine the costs and benefits of computer matching," but some evidence suggests most waste in federal programs is due to factors other than "client fraud").

101. The Computer Matching and Privacy Act does require matching agreements to be in writing, but it provides no guidelines as to when these agreements are not acceptable. See supra n. 100 at Sec. 2. To allow federal matching programs simply because the agencies make a written agreement arguably violates the letter and spirit of the Privacy Act. See Privacy Act, supra n. 98 at Sec. 2(b)(1) (purpose of Act is to "permit an individual to determine what records pertaining to him are collected, maintained, used or disseminated by" federal agencies).

102. The Office of Management and Budget has been given responsibilities by the Privacy Act "to provide continuing assistance to and oversight of the (A)ct's implementation by the agencies." General Accounting Office, *Report to the Chairman, Subcommittee on Government Information, Justice, and Agriculture, Committee on Government Operations, House of Representatives*, 11 (August 1987). Its oversight of the Privacy Act has been criticized by Congress and the General Accounting Office, id. at 11, 47.

103. The General Accounting Office has issued important studies of implementation of the Privacy Act, *see* General Accounting Office, supra n. 102, and of the federal government's computer security, see Committee on Science, Space and Technology, *Hearing*, 100-15 (First Session, 19 May 1987).

104. The Office of the Inspector General has prepared important studies of data

the Department of Commerce[105]; and the Computer Systems Security and Privacy Advisory Board, which is also part of the Department of Commerce.[106] As far as the Privacy Act is concerned, the Office of the Management and Budget should play a critical role in its enforcement. Yet, this agency has merely encouraged individual federal agencies to police themselves while allowing generous funds for the installation of new computer facilities.[107] Neither the Computer Matching Act of 1988 nor the Computer Security Act of 1987 has established coherent legal standards for the processing of personal data.[108]

---

use by four major benefit programs: Aid to Families with Dependent Children, Food Stamps, Medicaid and Unemployment Insurance. See, e.g., Office of Inspector General, Department of Health and Human Services, *Catalog of Automated Front-End Eligibility Verification Techniques* (1985). It has attempted "to promote the sharing of money-saving computer technology," id. at i, and to set up controls to limit computer-related fraud and abuse, see Richard Kusserow, *Computer-Related Fraud and Abuse in Governmental Agencies* (1983) (report of Inspector General of the Department of Health and Human Services).

105. The National Bureau of Standards is required by the Computer Security Act of 1987, Pub. L. No. 100-235, 101 Stat. 1724 (1988) (codified as amended at 15 U.S.C. Sec. 272 (1988), 40 U.S.C. 759(d) (1988)) to develop a "computer standards program" that will "assure the cost-effective security and privacy of sensitive information in Federal computer systems."

106. The Computer Security Act, id. at Sec. 21, establishes this Board, whose duties are "to identify emerging managerial, technical, administrative, and physical safeguard issues relative to computer systems security and privacy; . . . to advise the Bureau of Standards and the Secretary of Commerce on security and privacy issues pertaining to Federal computer systems; and . . . to report its findings to the Secretary of Commerce, the Director of the Office of Management and Budget, the Director of the National Security Agency, and the appropriate Committees of the Congress."

107. OMB's "general policy framework for management of Federal information resources" is expressed in its Circular No. A-130 (12 December 1985). Section 8 of this document gives enormous power to agencies to determine their systems of data processing and admonishes them to "(s)eek to satisfy new information needs through legally authorized interagency or intergovernmental sharing of information, or through commercial sources, where appropriate, before creating or collecting new information." Id. at Sect. 8(2). See United States General Account Office, *Report to the Chairman, Subcommittee on Government Information, Justice, and Agriculture, Committee on Government Operations, House of Representatives* 47 (August 1986) ("Privacy Act Operations need a cohesive, articulated program aimed at assuring that such activities are conducted in full compliance with OMB guidance and the act's provisions. In our opinion, without more active involvement and monitoring by both OMB and agencies, there will be less than full assurance that Privacy Act functions are carried out in a manner that protects the privacy rights of individuals and balances these rights with the information needs of federal agencies."). See also Record Systems, supra n. 98 at 105 ("There is serious question as to the efficiency of the current institutional arrangements for oversights of Federal agency compliance with the Privacy Act and related OMB guidelines").

108. The Computer Security Act of 1987 sets up a Computer Systems Security and Privacy Advisory Board within the Department of Commerce and provides for a computer standards program to be established within the National Bureau of Standards. The President is the ultimate judge of how these standards that "improve the efficiency of operation or security and privacy of Federal computer systems" should be set. Id. at Sec. 4; 40 U.S.C. 759(d)(1).

Perhaps even more disturbing than this lack of legal standards is the Federal government's habit of establishing computer programs without attention as to how a discrete system will add to the overall computer surveillance of citizens. An example of such inattention came this year when the Health Care Financing Administration proposed to outfit 52,000 pharmacies with computer terminals. The goal of the networking is to allow the rapid determination of whether patients qualify for drug benefits.[109] Although no legislation authorized this measure, the Health Care Financing Administration claimed that it was necessary to fulfill the objectives of the Medicare Catastrophic Protection Act of 1988.[110] The creation of this new data base will affect at least 32 million Americans and provide ninety-five percent of our nation's pharmacies with computers;[111] nevertheless, it appears to be occurring without intensive congressional oversight or public debate.[112]

Another such initiative with overlooked implications is the Family Support Act of 1988.[113] This law, which has changed much of the system of American welfare, contains a number of provisions that affect data protection. The Family Support Act makes mandatory the use of computers to track and monitor the distribution of welfare benefits.[114] It provides generous federal funds to establish the required electronic systems. The law also orders state agencies and the federal government to share "wage and unemployment compensation claims information (including *any information that might be useful in locating an absent parent or such parent's employer*)."[115] This authorization of federal and state data sharing is extremely broad; in addition, the law goes on to create a new data

109. See Health Care Financing Administration, Department of Health and Human Services, *Information Kit for Medicare Catastrophic Coverage Act* (description of plan for a "highly automated drug bill processing system").

110. Tolchin, "System to Track Medicare Drugs," *New York Times*, col. A1 (13 July 1988).

111. Id.

112. There has, however, been some Congressional involvement. In particular, the Subcommittee on Civil Constitutional Rights of the House Committee on the Judiciary has attempted to monitor the Health Care Financing Administration's plan. Letter from Rep. Don Edwards, Chairman, Subcommittee on Civil and Constitutional Rights, U.S. House of Representatives Judiciary Committee to Paul Schwartz (13 April 1989). Meanwhile, the Health Care Financing Administration appears not to have accepted the proposal of the American Civil Liberties Union to set up a working group with oversight responsibility for the electronic point-of-sale technology. Letter from Frank Derviller, Deputy Director, Bureau of Program Operations, Health Care Financing Administration to Paul Schwartz (27 April 1989). This agency has hired several private consulting firms with expertise in the design of point-of-sale systems and plans to publish notice of the new system of records in the Federal Register, as required by the Privacy Act. Id.

113. Pub. L. 100-485, 102 Stat. 2353, codified at Sec. 402, 42 U.S.C. (1988).

114. Id. at Sec. 121-124.

115. Id. at Sec. 124 (emphasis added).

bank that has an even greater potential for misuse. The Family Support Act requires that when children are born, the parents' social security numbers be recorded and stored along with the name of the children.[116] The Act authorizes use of this information to enforce child support laws. This new data bank contains sensitive information that will be open to misuse by many governmental agencies. Whether or not this information is likely to reduce the poverty of single mothers and their children or the burden on the taxpayers is debatable.[117]

B. German Developments

The five years since the *Census* decision have seen both successes and failures in German data protection law. The *Census* decision has inspired an impressive legal and legislative attempt to meet its challenges and commands.[118] The German judiciary has invalidated some treatment of personal data as unconstitutional;[119] but its most significant use of the *Census* decision has come in cases where it exerts pressure on federal and state legislatures to pass laws that will conform data use to constitutional standards.

In one of the more noteworthy of these decisions, the Bavarian Constitutional Court of Justice required the replacement of the "general clauses" of the regulations for processing criminal denunciations.[120] The Court saw a need for "more specific and more de-

116. Id. at Sec. 125.

117. Hacker, "Getting Rough on the Poor," *New York Review of Books*, 12, 13 (13 October 1988).

118. The decision has also inspired an outpouring of academic analysis of the right of informational self-determination. See Klaus Vogelsang, *Grundrecht auf informationelle Selbstbestimmung* 84 (1987) (narrow reading of *Census* decision that criticizes "global acceptance of all deliberations in the grounds of the judgment"); Denninger, "Das Recht auf informationelle Selbstbestimmung und Innere Sicherheit," 19 *Krit. Justiz*, 215, 230-240 (1985) (discussion of conflicts between information processing activities of the police and informational self-determination); Gola, supra n. 68 at 1913 (since the *Census* decision of the Constitutional Court, data protection has constitutional rank); Simitis, "Die informationelle Selbstbestimmung-Grundbedingung einer verfassungskonformen Informationsordnung," 1984 *NJW* 398, 402 (German constitution guarantees not freedom of data processing, but orders barriers to data processing); Schneider, "Anmerkung," *Die Öffentliche Verwaltung*, 161-63 (February 1984) (criticism of the *Census* decision as overly expansive and unclearly written); Krause, "Das Recht auf informationelle Selbstbestimmung," 1984 *Jurist. Schul.* 268 (narrow interpretation of the *Census* decision); Muckenberger, supra n. 59 at 4 (*Census* decision orders "informational separation of powers").

119. See, e.g., BVfG (decision of 9 March 1988) *Recht der Datenverarbeitung* 194 (1988) (public notification of legal incapacitation because of prodigality or alcoholism is incompatible with the right of informational self-determination); SG Hildesheim (decision of 6 May 1985), *Computer und Recht* 161 (1985) (only expert medical opinion's final judgment regarding ability of petitioner to work may be kept in documents of State Labor Bureau).

120. BayVerfGH (decision of 9 July 1985), *Computer und Recht* 101 (1986).

tailed" rules in this area of police law.[121] It did, however, admit the necessity of a "certain transition period" to allow the legislature to enact the necessary measures.[122] This so-called "transition bonus," a period of time allowed the legislature to respond to the *Census* decision, is now coming to an end. In July 1988, the Higher Regional Court of Frankfurt allowed such a "transition period" only in conjuncture with setting an unmistakable date when it would end.[123] The *Oberlandesgericht* permitted the Hessian District Attorney's Office to continue to use its central register only until the end of the current federal legislature period.[124] By that time, the court demanded the passage of a law that would provide "constitutional legitimation" for the storage of personal data in the register.[125]

Even without this judicial pressure, some German states have themselves taken initiatives to renew their data protection laws. One of the most noteworthy of the new German laws is the Hessian Data Protection Act of 1986.[126] As a general rule, the Hessian law provides that personal data must be collected from the data subject, who will be informed of the purpose of the planned use of the data and whether there is a legal requirement that the data be supplied. The law expands the right to inspect personal records and provides for written notification to the data subject when his data are stored for the first time.[127] These changes respond to the *Census* decision's call for greater involvement of the citizen in his role as data subject.

The Hessian Act also strengthens the role of the State Data Protection Commissioner in several valuable ways. Data subjects who have not been permitted to examine their records may request that the Hessian Data Protection Commissioner examine the circumstances of the denial as well as their records.[128] The Hessian Act also states that no one shall suffer retribution on account of having complained to the Data Protection Commissioner.[129] By strengthening access to the Commissioner, this law facilitates the dialogue between administration and data subject in a way that comports with the *Census* decision.

Apart from the statutory changes and the vigorous judicial role, another success in German data protection law is the accomplish-

121. Id. at 104.
122. Id. at 105.
123. OLG Frankfurt, (decision of 14 July 1988), *NJW* 47 (1989).
124. Id. at 50-51.
125. Id. at 51. *See* Simitis, "Konsequenzen des Volkszählungsurteils: Ende der Übergangsfrist," *NJW* 21 (1989) (discussion of end to period of the so-called "transition bonus").
126. GVBl.I 1986, 309.
127. Id.
128. Id. at Part II.
129. Id. at Section 28.

ment of this work with relatively modest expenditures by government and industry. There is no probably no other area of governmental activity in West Germany where similarly small staffs have accomplished as much.[130] In some instances, data protection has even reduced administrative costs.[131] A less expensive organization of data can be more efficient and more respectful of the data subjects.

The failures of this area of German law include the lack of sufficient legal regulation of the use of personal information by the police and anti-terrorist agencies.[132] Helmut Kohl's administration has tried to polarize the data protection discussion by suggesting that such legal measures are incompatible with fighting crime and terrorism. Another data protection failure is the Federal Government's introduction of a machine-readable national identification card and passport.[133] Despite the criticism of this measure by numerous data protection experts, the Minister of the Interior insisted on its necessity as part of the fight against terrorists.[134]

Another less than glorious moment for German law was provided by the census that succeeded the ill-fated one of 1983. After the *Census* decision found part of the planned inquiry to be unconstitutional, the government decided to cancel the undertaking and not to carry out a modified poll at that time. The next census bill of the Parliament was upheld by the Constitutional Court.[135] Although the institutions of German data protection provided forums for observation and criticism of the 1987 census, this poll was hardly more popular than the earlier one.[136] The German legal order responded to this opposition with repressive measures that revealed a strong intolerance for actions that appear to limit the efficiency of the State or to show disrespect for its decisions.[137] The

130. For one example, see 15 *Tätigkeitsbericht des Hessischen Datenschutzbeauftragten* 56-57 (1986) (hereinafter cited as 15 *Tätigkeitsbericht*).

131. Id.

132. Gola, supra n. 68 at 1916-1918; Denninger, supra n. 118 at 230-240; 15 *Tätigkeitsbereich*, supra n. 130 at 64, 117; Schoreit, "Datenschutz und Informationsrecht im Bereich der Strafverfolgung unter Berücksichtigung der Dateien des Bundeskriminalamts," 2 *Z. RPol.* 73 (1981).

133. 15 *Tätigkeitsbericht*, supra n. 130 at 119-120; 13 *Tätigkeitsbericht des Hessischen Datenschutzbeauftragten* 93-99 (1984).

134. See, e.g., Harold, "Fahndung nach Terroristen braucht eigene Methoden," *Frankfurter Allgemeine Zeitung*, 8 (29 November 1986) (objecting to proposal by data protection experts to set limits on computers of Federal Criminal Bureau (*Bundeskriminalamt*)). For analysis of how this bureau used computers to search for terrorists when Harold was its president, see Stefan Aust, *Der Baader-Meinhof Komplex* 196-204 (1985).

135. See supra n. 71. But for legal objections to the law, see Rottman, supra n. 71.

136. See "Datenschrott für eine Milliarde?," *Spiegel*, Nr. 12, 30 (1987) (discussing movement to boycott 1987 Census); H.v. Ditfurth, "Warum ich nicht gezählt zu werden wünsche," *Spiegel*, No. 21, 34 (1987) (arguments against the 1987 Census).

137. See *Spiegel*, "Datenschrott," supra n. 136 (noting threats of Interior Minister

prosecution of the opponents of the census included prior restraints on their speech and an order to disconnect one organization's telephone.[138] These measures suggest that the future health of data protection in Germany is tied to the country's political climate.

CONCLUSION

The German Constitutional Court has responded to the information society by enunciating a "right of informational self-determination." This constitutional right obliges the State to organize societal use of personal information in a fashion that will respect personal autonomy. It grants to the judiciary the power to strike down laws that fail to regulate data use or data processing practices in a constitutional manner. The German judiciary is committed to assessing informational self-determination by balancing it against other interests. While this approach allows judges to make perceptive choices to resolve conflicts, it fails to provide a scale of values for the identifying of interests and assigning of weight to them.

The U.S. Supreme Court has begun to develop a "right of informational privacy" that applies to use of personal information by the government. It has, however, yet to define this right so that it responds to the risk of data processing. A right of informational self-determination must be developed in America. This interest should be grounded in provisions of the Bill of Rights—in particular, in the Due Process Clause. The establishment of this right will give judges a role in making the difficult choices typical of data protection law. Democracy depends on the flow of information among the people. The activist state requires personal information about those whom it is expected to serve and assist. The economy of the information society relies upon banks of personal data. Yet the autonomy of the individual requires the law to give shape and to set limits to the information flow.

Zimmerman against opponents of 1987 Census); "Boykotteure in Polizeidateien," *Frankfurter Allgemeine Zeitung*, 29 (12 January 1988) (police in Hessen, as well as in at least two other German states, registered the names of opponents of the 1987 Census in their computers as possible "opponents of the state" (*Staatsfeinde*)).

138. These cases are printed and discussed in "Dokumentation: Die Volkszählung auf dem Rechtsweg," 21 *Krit. Justiz* 206 (1988).